USA PATRIOT ACT: A REVIEW FOR THE PURPOSE OF REAUTHORIZATION

HEARING

BEFORE THE

COMMITTEE ON THE JUDICIARY
HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

APRIL 6, 2005

Serial No. 109–12

Printed for the use of the Committee on the Judiciary

Available via the World Wide Web: http://www.house.gov/judiciary

U.S. GOVERNMENT PRINTING OFFICE

20–390 PDF WASHINGTON : 2005

For sale by the Superintendent of Documents, U.S. Government Printing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2250 Mail: Stop SSOP, Washington, DC 20402–0001

COMMITTEE ON THE JUDICIARY

F. JAMES SENSENBRENNER, JR., Wisconsin, *Chairman*

HENRY J. HYDE, Illinois
HOWARD COBLE, North Carolina
LAMAR SMITH, Texas
ELTON GALLEGLY, California
BOB GOODLATTE, Virginia
STEVE CHABOT, Ohio
DANIEL E. LUNGREN, California
WILLIAM L. JENKINS, Tennessee
CHRIS CANNON, Utah
SPENCER BACHUS, Alabama
BOB INGLIS, South Carolina
JOHN N. HOSTETTLER, Indiana
MARK GREEN, Wisconsin
RIC KELLER, Florida
DARRELL ISSA, California
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
STEVE KING, Iowa
TOM FEENEY, Florida
TRENT FRANKS, Arizona
LOUIE GOHMERT, Texas

JOHN CONYERS, JR., Michigan
HOWARD L. BERMAN, California
RICK BOUCHER, Virginia
JERROLD NADLER, New York
ROBERT C. SCOTT, Virginia
MELVIN L. WATT, North Carolina
ZOE LOFGREN, California
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ROBERT WEXLER, Florida
ANTHONY D. WEINER, New York
ADAM B. SCHIFF, California
LINDA T. SÁNCHEZ, California
ADAM SMITH, Washington
CHRIS VAN HOLLEN, Maryland

PHILIP G. KIKO, *Chief of Staff-General Counsel*
PERRY H. APELBAUM, *Minority Chief Counsel*

CONTENTS

APRIL 6, 2005

OPENING STATEMENT

WITNESSES

LETTERS, STATEMENTS, ETC., SUBMITTED FOR THE HEARING

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

USA PATRIOT ACT: A REVIEW FOR THE PURPOSE OF REAUTHORIZATION

WEDNESDAY, APRIL 6, 2005

HOUSE OF REPRESENTATIVES,
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Committee met, pursuant to notice, at 1:01 p.m., in Room 2141, Rayburn House Office Building, Hon. F. James Sensenbrenner, Jr. (Chairman of the Committee) presiding.

Chairman SENSENBRENNER. The Committee will be in order. A quorum for the taking of testimony is present.

On September 11, 2001, 19 terrorists turned four planes into guided missiles that killed more than 3,000 innocent men, women, and children, caused approximately $100 billion in economic losses, and triggered U.S. military action in Afghanistan. In response to the failure of the Nation's law enforcement and intelligence communities to discover and prevent these attacks, Congress passed the USA PATRIOT Act. The objective of this bill was to modernize both Federal law enforcement and intelligence investigative tools and to ensure that the information collected was shared between the law enforcement and intelligence communities.

September 11 also led to the passage of several other key pieces of legislation to assist law enforcement and the Intelligence Community with their efforts in the war on terrorism. Such accomplishments included creating a Department of Homeland Security to better coordinate agency efforts for a secure homeland; further improvements to information sharing; efforts to enhance border and visa security; and heightened penalties for terrorist acts and criminal activities which assist in their furtherance.

The PATRIOT Act is an important part of the overall framework to protect our Nation. In passing the PATRIOT Act, Congress established standards and oversight for the use of the Act's provision. For example, section 1001 of the PATRIOT Act requires the Inspector General of the Department of Justice to determine and report to Congress civil liberties violations. I would note that this includes any violations of civil liberties by DOJ, not just those alleged to have occurred under the provisions of the PATRIOT Act. To date, the Inspector General has issued six reports and not found a single example of a civil liberties violation relating to authority granted under the PATRIOT Act.

To further address concerns that enhanced law enforcement tools could lead to civil liberties violations, Congress included a sunset provision for 16 sections of the PATRIOT Act. These 16 sections, set to expire this year on December 31, are aimed at updating in-

vestigative tools and improving information sharing and go to the very heart of our Nation's response to a changed world in which terrorists plot to destroy our very way of life.

As we consider the reauthorization of these provisions, we must consider whether allowing them to expire will once again saddle law enforcement and the Intelligence Community with the restrictions that will render intelligence unreliable and prosecutions unattainable against criminals and terrorists who increasingly utilize advanced technology and countersurveillance methods to improve their efforts to harm and to kill.

As we learned from the 9/11 attacks, procedures needed to be streamlined for law enforcement and the Intelligence Community to react in real time. In this war on terrorism, we are racing against the clock. Terrorist cells operate throughout the world, including within our own borders, and actively plan attacks against U.S. citizens. Law enforcement and the Intelligence Community must be able to quickly protect the public from future attacks.

That is why I believe that one of the most important tasks Congress faces this year is to consider the reauthorization of these provisions. Lawmakers must focus on how the PATRIOT Act has been implemented, what improvements, if any, are needed, and whether the provisions set to expire deserve to be made permanent.

Accordingly, the Committee plans an ambitious hearing and oversight schedule beginning with today's full Committee hearing with Attorney General Alberto Gonzales. After this hearing, the Committee will hold eight Subcommittee hearings through April and May on the PATRIOT Act provisions that are set to expire on December 31. Finally, I anticipate the Deputy Attorney General and the Inspector General will testify before the full Committee soon after the Subcommittee hearings are completed. These hearings reflect this Committee's continued commitment to monitor the implementation of anti-terrorism legislation, to conduct active oversight over the Department of Justice, and to ensure that law enforcement has the tools necessary to fight and to win the war on terrorism and to fight crime in general.

I look forward to hearing the testimony of the Attorney General, and congratulations, General Gonzales, on your recent confirmation.

Now I recognize the gentleman from Michigan, Mr. Conyers.

Mr. CONYERS. Thank you, Mr. Chairman. Good afternoon, Mr. Attorney General. We are delighted to have you here.

As we begin our review of the PATRIOT Act, let me start at this very important point. Those who oppose the passage of any parts of the PATRIOT Act, want changes, who question its utility, who are concerned about the Government's demand for new and unnecessary powers after September 11 are not those who do that because they have any sympathy with terrorists or those that support them. I personally resent on the part of all Americans any one, particularly in the Government, that takes that point of view.

In the Congress and in the Judiciary Committee, that's even more important because we make the laws. We pass the laws. These are our responsibilities. This is what we took the oath for. So we have a historic and legitimate concern regarding the misuse and the abuse of Government power, any Government power, but

particularly coming from the Department of Justice, not only under the PATRIOT Act, but under the entire array of authority unilaterally assumed in many instances by the Administration since September 11.

This includes the mistreatment of detainees, the condoning of torture, the designation of enemy combatants, the immigration sweeps, hundreds of them, the excessive collection of personnel data, the closing of immigration proceedings, the unchecked military tribunals, and the abuse of our material witness statutes.

When our own Government detains and verbally and physically abuses thousands of immigrants for unknown and unspecified reasons with no time limits, targets tens of thousands of Arab Americans for intensive interrogation, I, sir, see a Department of Justice that has institutionalized racial and ethnic profiling without the benefit of a single terrorism conviction.

When our President takes upon himself to label United States citizens as enemy combatants without a trial, without charges, without access to the outside world, I see an executive branch that has placed itself in the constitutionally untenable position of prosecutor, judge, and jury, and is ignoring, to my shock and dismay, the principles of the separation of powers.

When our Justice Department condones the torture of prisoners at home and abroad, authorizes the monitoring of mosques and religious sites without any indication of criminal activity, I see a course of conduct that makes our citizens less safe, not more safe, and undermines our role as a beacon of democracy and freedom in the world.

When the FBI can arrest an innocent American citizen, a Muslim, Brandon Mayfield, based on a botched fingerprint exam, blame him for blowing up a train in Spain and he's never been in the country, has no known connection to al-Qaeda or any terrorist group, I hope you can understand why so many Americans are distrustful about the tactics and standards being applied in our war against terror.

When the PATRIOT Act can be misused to tap Mr. Mayfield's phones, seize his property, copy his computer, spy on his children, take his DNA, all without his knowledge, please, sir, appreciate why I am today calling on the Inspector General to review the manner in which this American citizen and his family have been treated by our Government.

In the past, your predecessor has stated that those who would criticize this Administration are aiding the terrorists and giving ammunition to America's enemies and chastise us as searching for phantoms of lost liberty. Well, I'm here to say that these incidents are not phantoms, thousands of them. They involve real people with real families whose civil liberties have been abused in the war on terror.

This Member will not be bullied or intimidated or rushed into backing down from my legislative and oversight responsibilities. Many of us remember a time when the powers of the FBI and the CIA were horribly abused. We know what it means to face racial profiling and religious persecution. Many of us know that our Nation has too frequently overreacted to threats of violence in the past by clamping down on legitimate protests and law-abiding citi-

zens and immigrants. To me, the lessons of September 11 are that if we allow law enforcement to do their work free of political interference, if we give them adequate resources and modern technologies, we can protect our citizens without intruding on our liberties.

We all fight terrorism, but we want to work with you to fight it the right way, consistent with our Constitution and in a manner that serves as a model for the rest of the world.

Chairman SENSENBRENNER. Thank you, Mr. Conyers.

[The letter from Ms. Clash-Drexler follows:]

LETTER SUBMITTED FOR THE RECORD BY THE HONORABLE JOHN CONYERS, JR. FROM MS. CLASH-DREXLER

U.S. Department of Justice

Civil Division, *Federal Programs Branch*

Via U.S. Mail:
P.O. Box 883, Rm. 6132
Washington D.C. 20044

Via Special Delivery:
20 Massachusetts Ave, NW
Rm. 6132
Washington D.C. 20001

Sara W. Clash-Drexler
Trial Attorney

Tel: (202) 514-3481
Fax: (202) 616-8460

March 24, 2005

BY FACSIMILE AND U.S. MAIL

Elden Rosenthal
Rosenthal & Greene
1001 Southwest Fifth Avenue
Suite 1907
Portland, OR 97204

Dear Elden:

As our forthcoming response to plaintiffs' motion to compel will make clear, the government believes that the Court may not compel the Attorney General to make a disclosure under Title 50 of the United States Code Section 1825(b). Nevertheless, the government has decided voluntarily to provide the following notice to Mr. Brandon Mayfield. Please advise Mr. Mayfield of the following, which I have been authorized to provide on behalf of the Acting Attorney General of the United States.

As authorized by the Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, 50 U.S.C. §§ 1801 *et seq*, Brandon Mayfield was the target of physical searches of his residence, and pursuant to 50 U.S.C. § 1825(b), Mr. Mayfield is hereby notified that the following property was seized, altered or reproduced during FISA searches of his residence: three hard drives of three desk top computers and one loose hard drive were copied; several documents in the residence were digitally-photographed; ten DNA samples were taken and preserved on cotton swabs and six cigarette butts were seized for DNA analysis; and approximately 335 digital photographs were taken of the residence and property therein.

In addition, although 50 U.S.C. § 1825 (b) is limited by its terms to circumstances involving search of a residence of a U.S. person, Mr. Mayfield is also hereby notified that he was the target of electronic surveillance and other physical searches authorized pursuant to FISA.

Sincerely,

Sara W. Clash-Drexler

ARTICLE SUBMITTED BY THE HONORABLE JOHN CONYERS, JR. ENTITLED "SEEKING THE TRUTH FROM JUSTICE," BY LAURA MURPHY, FORMER DIRECTOR, AMERICAN CIVIL LIBERTIES UNION

Seeking Truth From Justice

Volume One

PATRIOT Propaganda:

The Justice Department's Campaign to Mislead
The Public About the USA PATRIOT Act

July 2003

www.aclu.org

Seeking Truth From Justice

PATRIOT Propaganda:
The Justice Department's Campaign to Mislead
The Public About the USA PATRIOT Act

Published July 2003

THE AMERICAN CIVIL LIBERTIES UNION is the nation's premier guardian of liberty, working daily in courts, legislatures and communities to defend and preserve the individual rights and freedoms guaranteed by the Constitution and the laws of the United States.

National Office
125 Broad Street, 18th Fl.
New York, NY 10004
(212) 549-2500
www.aclu.org

Washington Legislative Office
1333 H St., NW, 10th Fl.
Washington, DC 20005
(202) 544-1681

Foreword

In April of this year, Maine's *Bangor Daily News* entered the national spotlight when it reported on a small-town librarian's drive to keep the Justice Department from obtaining the borrowing records of her patrons under the increasingly controversial USA PATRIOT Act.

It was a regional human interest story, yet it spurred a high-level spokesman for Attorney General John Ashcroft to call the Bangor paper and claim that a grassroots backlash against parts of the PATRIOT Act amounted to nothing more than a "propaganda campaign," which had consistently got the facts "wrong."

Interestingly, though, when the spokesman, Mark Corallo, berated the paper's editors, *he* misrepresented the scope and impact of the relevant provision in the PATRIOT Act, prompting the editorial board to write a piece complaining that Corallo's characterization "completely overstates the Department's limitations."

The editorial went on to support the librarian's position.

If this was just an isolated incident, it could easily be chalked up to human error or an understandable lapse by a spokesperson at the Justice Department. Unfortunately, the same pattern of behavior – where the Justice Department's critics are answered not with substantive counter arguments, but with often-inaccurate dismissals – is evident in numerous instances, going back almost 20 months.

The following report, titled "Seeking Truth From Justice," is the first volume in a series of ACLU special reports that will catalogue and detail the Justice Department's seeming inability to get its facts straight. This report is part of a series of ACLU special publications examining government policies since September 11. Each of the reports – *The Dangers of Domestic Spying By Federal Law Enforcement* (January 2002), *Insatiable Appetite* (April 2002), *Civil Liberties After 9/11* (September 2002), *Bigger Monster, Weaker Chains* (January 2003), *Freedom Under Fire: Dissent in Post-9/11 America* (May 2003) and *Independence Day 2003: Main Street America Fights the Government's Insatiable Appetite for New Powers* (July 2003) – is available on our website at http://www.aclu.org/safeandfree.

As you will see, the errors documented in this report go beyond mere legal hair splitting; rather, they deal with core constitutional values like due process or Fourth Amendment protections against unreasonable search and seizure. They also raise serious questions about whether our leaders in Washington are intentionally misrepresenting the facts of a debate to deflect public or political criticism.

Take, for instance, the U.S. Attorney for Alaska's testimony in front of a state Senate Committee: "I think, for instance, there is concern that under the PATRIOT Act, federal agents are now able to review library records and books checked out by U.S. citizens," he said. "If you read the Act, that's absolutely not true…. It can't be for U.S. citizens."

In fact, the U.S. Attorney was wrong. Section 215 of the USA PATRIOT Act – reproduced in the first section of this report – makes it clear that "U.S. persons," a term referring to citizens and certain types of non-citizens alike, can have their records seized.

That is but one example of the misleading statements that Justice Department officials and supporters of the USA PATRIOT Act have made in recent months. Our report details others and we plan future reports looking at other ways the government is misleading the American public.

Is the Justice Department telling the truth? You decide.

LAURA W. MURPHY
DIRECTOR, ACLU WASHINGTON
LEGISLATIVE OFFICE

July 9, 2003

Seeking Truth From Justice

PATRIOT Propaganda: The Justice Department's Campaign to Mislead The Public About the USA Patriot Act

In recent months, citizen concern about the USA PATRIOT Act has continued to climb to new highs. More than 130 communities across the country – and state legislatures in Alaska, Hawaii and Vermont have passed resolutions opposing provisions of the PATRIOT Act and other government actions that compromise civil liberties. And librarians have begun taking steps to warn patrons about and protect them from the Act's dangerously overbroad powers.

Unfortunately, the Department of Justice under Attorney General John Ashcroft has responded to this movement by trying to mislead the American people about the Act's new powers. Department spokespersons have consistently made statements to the media and local officials that are either half-truths or are plainly and demonstrably false – and which are recognized as false by the Justice Department in its own documents.

Primarily at issue is Section 215 of the PATRIOT Act, the so-called "business records" or "tangible things" provision. Section 215 allows the government to obtain without an ordinary criminal subpoena or search warrant and without probable cause an order from a court giving them records on clients or customers from libraries, bookstores, doctors, universities, Internet service providers and other public entities and private sector businesses. The Act also imposes a gag order prohibiting an organization forced to turn over records from disclosing the search to their clients, customers or anyone else. The result is vastly expanded government power to rifle through individuals' finances, medical histories, Internet usage, bookstore purchases, library usage, school records, travel patterns or through records of any other activity.

The debate over the PATRIOT Act comes at a time when the Justice Department is not only pushing Congress to remove "sunset" or expiration provisions that apply to some portions of the Act, but is also planning to ask Congress for passage of new legislation – dubbed "PATRIOT II" that would give federal law enforcement authorities even more expansive powers. In testimony before the House Judiciary Committee on June 5, Attorney General Ashcroft testified that the new powers would include expansions of the offense of "material support" for terrorism, which under overbroad definitions of terrorism in the original PATRIOT Act could be applied to political protesters, and an expansion of presumptive, pre-trial detention even after the Department's own Inspector General found widespread mistreatment of detainees wrongly classified as terror suspects.

It is troubling that in its eagerness to prepare a foundation for new surveillance and other powers, the Justice Department has resorted to spreading falsehoods and half-truths about the powers it already has.

The following report lays out a series of "falsehoods" and "half-truths" that Justice Department officials have consistently made in the media as well as in letters to lawmakers and provides the facts to counter each.

FALSEHOOD: The PATRIOT Act does not apply to Americans.

What the government has been saying:

> "This is limited only to foreign intelligence," said Mark Corallo, a spokesman with the Department of Justice. "U.S. citizens cannot be investigated under this act."
>
> *– Florida Today*
> *Sept. 23, 2002*

> Mark Corallo, Justice Department spokesman, said Wednesday that critics of the USA Patriot Act were "completely wrong" and denied that the act targeted Americans. ...
>
> "I don't know why they are misleading the public, but they are," he said of the act's critics Thursday. "The fact is the FBI can't get your records."
>
> *– Bangor [ME] Daily News*
> *April 4, 2003*

> "And I have prepared ... this handy chart that takes the actual text of section 215 and explains the requirement for court authorization, the requirement that it not – it is not directed at US Persons, the requirement that it cannot be directed solely at First Amendment activities. ..."
>
> "The public has I think been misled, and this is the myth versus the reality of section 215."
>
> *— Viet Dinh, Assistant Attorney General, primary author of the PATRIOT Act, speaking at the National Press Club, Washington D.C., April 24, 2003*[1]

> "I think, for instance, there is concern that under the PATRIOT Act, federal agents are now able to review library records and books checked out by U.S. citizens. If you read the Act, that's absolutely not true.... It can't be for U.S. citizens."
>
> *– Testimony of Timothy Burgess, U.S. Attorney for Alaska, before the Alaska Senate State Affairs Committee on May 13, 2003*

TRUTH: Section 215 of the PATRIOT Act <u>can</u> be used against American citizens.

Claims that Section 215 of the PATRIOT Act cannot be used against American citizens are simply wrong. According to the text of the Foreign Intelligence Surveillance Act as it was amended by Section 215:

> (a)(1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a *United States person* is not conducted solely upon the basis of activities protected by the First Amendment to the Constitution.

[1] Video of Dinh's remarks is available online at www.c-span.org. "Viet Dinh & Marc Rotenberg Debate Patriot Act," April 24, 2003.

Nowhere does this statute indicate that United States citizens cannot be targeted. In fact, the statute makes it clear that an "investigation of a United States person" *can* be conducted, so long as it is not based solely on activity protected by the First Amendment. (Of course, even this limit apparently applies only where the *investigation* is of a United States person, not where the investigation is of a foreign national but the records or other tangible things that the government seeks are of United States persons). The statute defines "United States persons" to include both citizens and permanent residents. (See 50 U.S.C. § 1801(i).)

FALSEHOOD: Under the PATRIOT Act, the FBI cannot obtain a person's records unless it has probable cause.

What the government has been saying:

> "I really don't understand what the concerns are with the act," [LaRae] Quy [spokeswoman for the San Francisco FBI office] said. "What it did was primarily streamline existing laws on the books. I know some people feel their privacy rights are being violated, but I think there's some hysteria out there. . . some misunderstanding.
>
> "We still have to show probable cause for any actions we take," she said.
>
> – *San Francisco Chronicle*
> *April 13, 2003*

> The Justice Department spokesman, Mark Corallo, says the assertions about the Act are completely wrong because, for the FBI to check on a citizen's reading habits, it must get a search warrant. And to get a warrant, it must convince a judge "there is probable cause that the person you are seeking the information for is a terrorist or a foreign spy."
>
> – *Bangor [ME] Daily News*
> *April 9, 2003*

> U.S. Department of Justice spokesman Mark C. Corallo said the FBI must present credible evidence in order to secure a warrant from the so-called spy court, which meets in secret.
>
> "The standard of proof before the court is the same as it's always been," Corallo said. "It's not been lessened."
>
> – *Springfield [MA] Union-News*
> *January 12, 2003*

TRUTH: Section 215 of the PATRIOT Act allows the government to obtain materials like library records without probable cause.

Under the PATRIOT Act, the FBI can obtain records – including library circulation records – merely by specifying to a court that the records are "sought for" an ongoing investigation. That standard (sometimes called a "relevance" standard) is much lower than the standard required by the Fourth Amendment, which ordinarily prohibits the government from conducting intrusive searches unless it has probable cause to believe that the target of

the investigation is engaged in criminal activity.

Although the Justice Department is assuring the public that it remains constrained by the standard of probable cause and that the standard "is the same as it's always been," the government has been telling a different story to its own attorneys. For example, an October 26, 2001 memo to "All Divisions" from the FBI's Office of General Counsel (and approved by FBI Director Robert S. Mueller III) included a section on "Changes in FISA Business Records Authority":

> The field may continue to request business records orders through FBIHQ in the established manner. However, such requests may now seek production of any relevant information, and need only contain information establishing such relevance.

Similarly, in a December 2002 letter to Congress responding to questions posed by the Senate Judiciary Committee, Deputy Attorney General Larry D. Thompson wrote:

> Under the old language, the FISA Court would issue an order compelling the production of certain defined categories of business records upon a showing of relevance and "specific and articuable facts" giving reason to believe that the person to whom the records related was an agent of a foreign power. The USA PATRIOT Act changed the standard to simple relevance.

Finally, at a hearing before the House Judiciary Committee on June 5, 2003, Attorney General Ashcroft conceded that the PATRIOT Act changed the FISA business records standard, saying the government "used to have [to allege] a reason to believe that the target is an agent of a foreign power" a standard he agreed was "lower than probable cause." Under the PATRIOT Act, he acknowledged, the standard has changed to allow the government may obtain all "relevant, tangible items" without such a showing [see below].

Ashcroft's testimony and these internal memoranda get the law exactly right. They acknowledge, as they must, that the FBI can now obtain sensitive business records merely by telling a court that the records are sought for an ongoing investigation; that is, the FBI can obtain the records even if they have no reason at all to believe that the person to whom the records pertain is a criminal or foreign spy. The Department's contention that Section 215 can't be used without probable cause misleads the public and ignores the government's own legal analysis.

HALF TRUTH: The government must "convince a judge" to obtain records under Section 215.

The Justice Department's repeated assertion that the authorities must "convince a judge" to win permission for a search also overstates the law's protections. Section 215 states:

> (c)(1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

This language suggests that the government must only certify to a judge – with no need for evidence or proof – that such a search meets the statute's broad criteria: "upon an application" the judge "shall enter" a surveillance order. Although the statute is not clear and has not yet been tested in court, it appears that the judge may not even have the authority to reject an application, unless the application fails to meet "the requirements of this section." What are those requirements?

FULL TRUTH: Judicial oversight is minimal.

As we have seen, the requirements are minimal. The FBI can obtain sensitive records merely by specifying that the records are "sought for" an on-going investigation. For Justice Department spokespersons to stress the need to "convince a judge" does not do justice to the true weakness of judicial oversight in this law.

FALSEHOOD: Section 215 applies only to terrorists and spies.

What the government has been saying:

> Justice Department spokesman Mark Corallo called [librarians' measures against the PATRIOT Act] "absurd." The legislation "doesn't apply to the average American," he said. "It's only for people who are spying or members of a terrorist organization."
>
> — *Journal News [NY] April 13, 2003*

> Before demanding records from a library or bookstore under the Patriot Act, he [Corallo] said, "one has to convince a judge that the person for whom you're seeking a warrant is a spy or a member of a terrorist organization."
>
> — *San Francisco Chronicle March 10, 2003*

> Corallo pointed out that the law only applies to agents of a foreign power or a member of a terrorist organization.
>
> - *Associated Press March 6, 2003*

> I think there are a lot of misconceptions being offered about what the PATRIOT Act does or doesn't do. …It has to be in regards to an international terrorism investigation after a court approves us seeking those records.
>
> — *Testimony of Timothy Burgess, U.S. Attorney for Alaska before the Alaska Senate State Affairs Committee, May 13, 2003*

TRUTH: Section 215 can be applied to anyone.

Once again, the spokesperson's statements are flat wrong. While some provisions of FISA do require a showing that a target is

an "agent of a foreign power," there is no such requirement in Section 215.

All the government needs to do to conduct a search under Section 215 is "specify" that the records are "sought for" an ongoing terrorism or foreign intelligence investigation. The government need not show that the target of the Section 215 order is engaged in terrorism or criminal activity of any kind.

Attorney General Ashcroft acknowledged as much in testimony before the House Judiciary Committee on June 5, 2003, under questioning by Rep. Tammy Baldwin (D-WI):

> BALDWIN: Prior to the enactment of the USA PATRIOT Act, a FISA order for business records related only to common carriers, accommodations, storage facilities and vehicle rentals. Is that correct?
>
> ASHCROFT: Yes, it is.
>
> BALDWIN: And what was the evidentiary standard for obtaining that court order?
>
> ASHCROFT: I don't think the evidentiary standard has changed. . . . [crosstalk] *OK, maybe it has. It used to have* [to show] *a reason to believe that the target is an agent of a foreign power* [emphasis added]...
>
> ***
>
> BALDWIN: OK. Now, under section 215 of the USA PATRIOT Act, now the government can obtain any relevant, tangible items. Is that correct?
>
> ASHCROFT: I think they are authorized to ask for relevant, tangible items.
>
> BALDWIN: And so that would include things like book purchase records?
>
> ASHCROFT: ... [I]n the narrow arena in which they are authorized to ask, yes.
>
> BALDWIN: A library book or computer records?
>
> ASHCROFT: I think it could include a library book or computer records.
>
> ***
>
> BALDWIN: Education records?
>
> ASHCROFT: I think there are some education records that would be susceptible to demand under the court supervision of FISA, yes.
>
> BALDWIN: Genetic information?
>
> ***
>
> ASHCROFT: . . . I think [we] probably could.
>
> BALDWIN: Under the PATRIOT Act, what is the evidentiary standard for the FISA court order to obtain these sorts of records?

> ASHCROFT: ... [I]f the judge finds that the investigation is for these [counter-intelligence or counter-terrorism] purposes, *he orders the FISA*. [emphasis supplied] ...

Exactly right. Before the USA PATRIOT Act, government agents could get *some* business records under FISA if they had "reason to believe" the person to whom the records related was an agent of a foreign power; now, as the Attorney General makes clear, they can get any record or other "tangible thing" that is allegedly relevant to an investigation regardless of whether the information pertains to an agent of a foreign power.

The implications of Section 215's weak evidentiary standard are frightening. The FBI can now conduct investigations using this power even when it has no particular individual in mind. For example, the FBI could demand the records of every person who has checked out a book on bridges based on no more than its investigation of a vague, unsubstantiated tip. The Department's suggestions that only spies or terrorists need worry about the PATRIOT Act couldn't be farther from the truth.

FALSEHOOD: The American people can trust the authorities not to abuse their powers.

What the government has been saying:

> "We don't have any interest in looking at the book preferences of Americans. We don't care, and it would be an incredible waste of our time," he [Corallo] said.
>
> — *Chicago Tribune*
> *April 4, 2003*

> The Justice Department "goes to great lengths to protect the privacy of every American unless you happen to be a foreign spy or member of a terrorism organization," said spokesman Mark Corallo. "The average American has nothing to fear."
>
> - *Newark Star-Ledger*
> *April 7, 2003*

> "We're not going after the average American," said Mark Corallo, a Justice Department spokesman. "We're only going after the bad guys. We respect the right to privacy. If you're not a terrorist or a spy, you have nothing to worry about."
>
> - *Washington Post*
> *April 10, 2003*

TRUTH: Democratic societies are based on checks and balances, not on blind faith in the good intentions of government officials.

With all due respect to the Justice Department, it is not enough for the government to *assure* us that they "go to great lengths to protect" privacy, "don't have any interest" in spying on innocent people, and are "not going after" the average American. The wisdom of the Founding Fathers, the historical record of abuses by the FBI, and common sense all point to the same conclusion: we can't rely on the FBI or any other federal law enforcement agency to police itself.

In June, for example, the Justice Department's own internal oversight unit released a report highly critical of what it

found to be the wholesale and long-term preventive detention of immigrants swept up in the months following 9/11. According to the report issued by the Justice Department's Inspector General, many immigrants who had no connection to the terrorist attacks of September 11 languished in federal lock-up for months at a time under an official "no bond policy" that effectively prohibited their release. The INS complained that the FBI had given them no evidence to justify their continued detention, yet some immigrants still spent up to eight months waiting for release.

Conclusion: A pattern of deceit

It is time for the Department of Justice to stop misleading the American people. The public cannot make informed decisions about the future of the police powers contained in the PATRIOT Act whether to let them expire, renew them, or expand them even more with PATRIOT Act II – if the government is not truthful about the extent of its current powers.

And the falsehoods are not limited to the PATRIOT Act. In a letter to the City Clerk of Ithaca, the FBI's Keith A. Devincentis, Special Agent in Charge of the Bureau's Albany office, misstates the FBI's powers under the Attorney General guidelines on domestic surveillance. "Contrary to popular television and theatrical portrayals, the FBI initiates cases predicted on facts, not suspicions or guesswork. 'Fishing expeditions' are clearly proscribed by FBI policy, Attorney General Guidelines, and other Federal statutes and regulations," Devincentis wrote.

In fact, in the aftermath of the passage of the USA PATRIOT Act, on May 30, 2002, Attorney General John Ashcroft announced that he had rewritten the guidelines that govern FBI surveillance. The Ashcroft guidelines sever the tie between the start of an investigative activities and evidence of a crime. Ashcroft's guidelines give the FBI a green light to send undercover agents or informants to spy on worship services, political demonstrations and other public gatherings and in the Internet chat rooms without even the slightest evidence that wrongdoing is afoot. Contrary to what Devincentis wrote, the FBI is now very much empowered to conduct investigative "fishing expeditions" on First Amendment protected activities even though there is no indication of criminal activity.

At this moment, the Justice Department has clear political incentives to soft-pedal the nature of the PATRIOT Act. But we can count on the fact that government investigators and prosecutors, when they appear before judges, will be making much bolder claims about what the Act lets them do.

Some Americans might have a hard time believing that a Justice Department spokesperson could be inaccurate about basic matters of law with such flagrancy. The ACLU has certainly found that from time to time it is possible to make occasional errors about matters of law, or to be misunderstood by a reporter when discussing the law. In this case, however, we are witnessing a pattern of inaccuracy spread out over a long period of time, over a wide variety of news outlets, by various staff members, on a central issue in a prominent national debate.

The Department's inaccuracies have to do not with subtle, debatable points of legal interpretation, but clear matters of law that are spelled out in black and white in the text of the PATRIOT Act.

There is no excuse for the Justice Department to get the PATRIOT Act wrong; the Department was behind the legislation from the beginning. The Justice Department drafted the Act (most of the Act's surveillance provisions were part of a longstanding wish list that had previously been sought by the Justice Department but rejected by Congress), and the Department was instrumental in forcing the bill through Congress with minimal discussion or debate in the panicked weeks after 9/11.

Considering the extent to which the USA PATRIOT Act is the Ashcroft Justice Department's "baby," one might expect department officials to be proud parents. Instead, they seem intent on denying the true nature of their creation.

Chairman SENSENBRENNER. Without objection, all Members may place opening statements in the record at this point.

[The prepared statement of Ms. Jackson Lee follows:]

SHEILA JACKSON LEE
18TH DISTRICT, TEXAS

COMMITTEES
SELECT COMMITTEE ON HOMELAND SECURITY
SUBCOMMITTEES:
INFRASTRUCTURE AND BORDER SECURITY
CYBERSECURITY, SCIENCE, AND RESEARCH & DEVELOPMENT
JUDICIARY
SUBCOMMITTEES
CRIME
RANKING MEMBER
INTELLECTUAL PROPERTY AND CLAIMS
SCIENCE
SUBCOMMITTEES:
SPACE AND AERONAUTICS
MEMBER
DEMOCRATIC CAUCUS POLICY AND STEERING COMMITTEE
CONGRESSIONAL BLACK CAUCUS

Congress of the United States
House of Representatives
Washington, DC 20515

WASHINGTON OFFICE
2435 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515
(202) 225-3816

DISTRICT OFFICE
1919 SMITH STREET, SUITE 1180
THE GEORGE "MICKEY" LELAND FEDERAL BUILDING
HOUSTON, TX 77002
(713) 655-0050

ACRS-CDW OFFICE
6719 WEST MONTGOMERY, SUITE 204
HOUSTON, TX 77019
(713) 691-4882

HEARTH OFFICE
420 WEST 19TH STREET
HOUSTON, TX 77008
(713) 861-4070

STATEMENT BY
CONGRESSWOMAN SHEILA JACKSON LEE

COMMITTEE ON THE JUDICIARY

FULL COMMITTEE OVERSIGHT HEARING,
THE USA PATRIOT ACT: A REVIEW FOR THE PURPOSE OF ITS REAUTHORIZATION

WEDNESDAY, APRIL 06, 2005

One of our Founding Fathers, John Quincy Adams, made the following statement regarding the importance of civil liberties:

> **Individual liberty is individual power, and as the power of a community is a mass compounded of individual powers, the nation which enjoys the most freedom must necessarily be in proportion to its numbers the most powerful nation.**

I have in my hand a copy of Chapter 1 of John Stuart Mill's

On Liberty, written in 1859. Selections of this chapter are quite fitting for today's proceeding:

> **Protection, therefore, against the tyranny of the magistrate is not enough;** ***there needs protection also against the tyranny of the prevailing opinion and feeling; against the tendency of society to impose, by other means than civil penalties, its own ideas and practices as rules of conduct on those who dissent from them*****; to fetter the development, and, if possible, prevent the formation, of any individuality not in harmony with its ways, and compel all characters to fashion themselves upon the model of its own.** ***There is a limit to the legitimate interference of collective opinion with individual independence; and to find that limit, and maintain it against encroachment, is as indispensable to a good condition of human affairs, as protection against political despotism.***

We passed the PATRIOT Act in 2001 six weeks after the terrorist attacks of September 11. While the actual bill passed by wide margins in both Chambers of Congress, I made the record clearly reflect my strong reservations about provisions that pose serious threats to fundamental freedoms and civil liberties.

In my capacity as member of the House Committee on the Judiciary, I joined a caucus of members in submitting letters to the Administration and to the Department of Justice requesting documentation and statements that speak to the protection of individual rights in light of the potentially dangerous provisions contained within the bill.

Congress included in the bill a "sunset clause" that provides an expiration date for over a dozen provisions on December 31, 2005 unless we act to renew them. This fact is the impetus behind this hearing in order to give us an opportunity to pose the serious questions relating to fundamental freedoms and civil liberties to Attorney General Alberto Gonzalez.

9/11 Commission Recommendations

It is vital that, in considering the re-authorization of the sunsetted provisions, we in Congress must ensure that the four-prong

recommendations of the bi-partisan 9/11 Commission[1]: First, Congress should re-examine the specific provisions that sunset, taking care not to renew any provision unless the government can show "(a) that the power actually materially enhance security and (b) that there is adequate supervision of the executive's use of the powers to ensure protection of civil liberties."[2] Second, "[i]f the power is granted, there must be adequate guidelines and oversight to properly confine its use."[3] Third, because the issues of national security and civil liberties posed by anti-terrorism powers that are not part of the Patriot Act sunset are at least as serious as any posed by those provisions that do sunset, Congress should undertake a broader review of anti-terrorism powers, both within and outside of the Patriot Act, using the same standard of review. Fourth, Congress should resist efforts by the Executive Branch to evade searching review of its existing powers, both under the Patriot Act and under other legal authorities, by shifting the debate to new anti-terrorism

[1] Letter from Tim Edgar, National Security Policy Counsel to the American Civil Liberties Union (ACLU) dated March 28, 2005 to all interested persons.
[2] Final Report of the National Commission on Terrorist Attacks Upon the United States ("The 9/11 Commission Report") 294-95 (2004) (boldfaced recommendation)
[3] *Id.*

legislation, such as proposals for administrative subpoenas or new death penalties.

In several hearings of the House Judiciary Committee that present opportunities to question witnesses about potential infringements upon civil liberties, I inquire as to the status of the Department of Justice's drafting of a "PATRIOT Act II" that is even more intrusive and more threatening than PATRIOT Act I; however, only nebulous response has been given to date.

As we approach the decision to reauthorize the sunsetted provisions, I will work with Amnesty and similar groups to ensure adequate examination of issues such as:

- Mass secret arrests of Arabs and Muslims followed by detention for extended periods without charges, denials of access to counsel, secret hearings and, in some cases, abuse by prison guards;
- Abuse of the material witness authority to detain citizens and others without charges;
- Discriminatory enforcement of the immigration laws, leading to arbitrary detentions and deportations;

- Detentions of Americans incommunicado as "enemy combatants" without access to lawyers or the courts;
- Expanded use of secret wiretaps and secret searches of Americans' homes and offices;
- Massive growth in surveillance technologies and authority (including the authority under the USA Patriot Act to seize library and medical records and all commercial databases) with inadequate legal protections against abuse;
- Spying on lawful political and religious activity; and
- Eavesdropping on attorney-client communications without judicial approval or oversight.

Taken together, these issues reflect a steady assault on fundamental liberties that has served only to make us less free, and not more secure. With few exceptions, Congress has failed to address these issues. To the contrary, it is continuing to consider legislation, such as the Real ID Act, that targets immigrants and asylum seekers unfairly without enhancing security. For Congress now to focus only on the concerns raised by the USA Patriot Act would be inappropriate.

Infringement Upon the Bill of Rights

The PATRIOT Act has directly infringed on many of the rights and freedoms granted by the Bill of Rights. This feature will overview the impact of the PATRIOT Act on some of our most cherished rights.

The First Amendment

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Violates the First Amendment by effectively authorizing the FBI to launch investigations of American citizens in part for exercising their freedom of speech.

Violates the First Amendment's guarantee of free speech by prohibiting the recipients of search orders from telling others about those orders, even where there is no real need for secrecy.

Creates a very serious risk that truly innocent individuals could be deported for association with political groups that the government later chooses to regard as terrorist organizations.

The Fourth Amendment

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized:

Violates the Fourth Amendment by allowing foreign intelligence searches for criminal purposes without probable cause of crime.

Violates the Fourth Amendment by failing to provide timely notice to persons whose home has been searched. Notice is also a key element of due process, which is guaranteed by the Fifth Amendment.

Violates the Fourth Amendment by allowing the government to seize records in intelligence and terrorism investigations without probable suspicion that the records pertain to a terrorist,

The Fifth Amendment

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

Allows indefinite incarceration of persons without judicial review thereby denying due process and equal protection of law.

Creates a very serious risk that individuals could be deported for association with political groups that the government later chooses to regard as terrorist organizations.

Immigration Provisions

The USA PATRIOT Act contains a number of immigration provisions that will improve our ability to identify and either exclude or prosecute aliens with terrorist ties. However, PATRIOT, as it relates to immigration law, is merely a first step in the immigration-policy reforms that are necessary to combat terrorism effectively and to protect Americans from future terrorist attacks. A detailed summary of the law's immigration-related provisions follows.

Racial Profiling

On June 17, 2003 President Bush publicly released a set of guidelines promulgated by the Civil Rights Division of the Department of Justice entitled, *Regarding the Use of Race by Federal Law*

Enforcement Agencies. The introduction to the guidelines alluded to the president's February 2001 address to Congress in which he declared that racial profiling is "wrong and we will end it in America."

The guidelines included several positive phrases such as:

- "racial profiling is wrong and will not be tolerated;"
- "America has a moral obligation to prohibit racial profiling;" and
- "stereotyping certain races as having a greater propensity to commit crimes is absolutely prohibited."

But the guidelines themselves fall far short of the Bush administration's rhetorical posturing. Since they are only a set of guidelines, rather than a law or an executive order, they have no teeth. They acknowledge racial profiling as a national concern, but they provide no enforcement mechanisms or methods for tracking whether or not federal law enforcement agencies are in compliance.

The guidelines' most serious flaw, however, is that they carve out a huge national security loophole. The guidelines specify "The above standards do not affect current Federal policy with respect to law enforcement activities and other efforts to defend and safeguard against threats to national security or the integrity of the Nation's borders..."

Since the 9/11 terrorist attacks, it has been the official policy of the United States government to stop, interrogate and detain individuals without criminal charge – often for long periods of time on the basis of their national origin, ethnicity and religion. In fact, the very inclusion of a national security exception in the guidelines is an admission by the Department of Justice that it relies upon racial and ethnic profiling in its domestic counterterrorism efforts.

In response to the severe shortcomings in the president's guidelines, I joined a bipartisan group of members in both the House of Representatives and the Senate to introduce the "End Racial Profiling

Act," a comprehensive package designed to track and provide steps toward eliminating racial, ethnic, religious and national origin profiling.

[The prepared statement of Ms. Sánchez follows:]

PREPARED STATEMENT OF THE HONORABLE LINDA T. SÁNCHEZ, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Thank you, Chairman Sensenbrenner and Ranking Member Conyers for convening this oversight hearing today to review the PATRIOT Act, and to consider its reauthorization.

Reauthorizing the PATRIOT Act raises many very deep concerns, and those concerns are just as deep as the opposition I feel to the first incarnation of the PATRIOT Act.

The PATRIOT Act signed in 2001 is a massive infringement on many civil liberties. It became law with little consideration of the consequences of giving law enforcement such broad surveillance powers—even going so far as granting them access to your library records.

Every Member of this Committee is fully aware of how quickly we advanced from the terrorist attacks on 9/11, to the concept of the PATRIOT Act, to the bill being passed by both chambers of Congress.

It only took 41 days.

Forty-one days is simply not enough time to fully develop a bill that impacts the Constitutionally protected privacy rights of every American citizen, and granted so much authority to law enforcement agencies.

Some of the new law enforcement powers the PATRIOT Act allows are shocking.

We now live in a country where the government can listen to conversations between attorneys and clients as they prepare their defense in certain cases.

We live in a country where the government has the power to indefinitely detain and even deport people who are part of certain associations, or simply exercise their right to free speech.

We live in a country where law enforcement agents have the power to detain aliens when the Attorney General merely suspects they have engaged in terrorist activity.

That doesn't sound like the United States to me, it sounds more like Communist China?

As troubling as the law enforcement provisions of this bill are, the restrictions on the ability of Judiciary and Legislative branches to oversee law enforcement's actions are equally troubling.

This Committee has tried in vain to exercise its oversight powers and get answers to our many questions about how the PATRIOT Act is being used, and more importantly, how it is being misused.

Far too often we have been met by a wall of secrecy or silence.

That is unacceptable. When every American's civil liberties and rights are at stake, we must have transparency to ensure that privacy rights are protected.

I fully recognize how monumental and important the task of protecting national security and preventing future terrorist attacks is.

I also recognize that law enforcement agents are working tirelessly to protect our country and will need every resource we can provide to keep another 9/11 from happening.

But we cannot trample on the Constitution in our effort to prevent terrorist attacks.

I thank the Attorney General for his testimony today, and I hope that he can inform the Committee how he plans to address the serious civil liberty concerns inherent in reauthorizing the PATRIOT Act.

I yield back.

[The prepared statement of Ms. Lofgren follows:]

PREPARED STATEMENT OF THE HONORABLE ZOE LOFGREN, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Following the attacks of 9/11, this Congress passed the USA PATRIOT Act to give our law enforcement and intelligence agencies new powers to fight terrorism. I voted for that law, but only after securing support for sunset provisions that allowed this Congress to revisit these issues under less trying circumstances.

Today, we begin that review in a very different atmosphere. This Nation is still fighting terrorism at home and abroad. But an increasing number of Americans are beginning to wonder whether the PATRIOT Act does more harm than good. In fact, over 370 communities and 4 states have passed resolutions opposing parts of the PATRIOT Act. These communities represent about 56 million Americans who have lost faith in their government's ability to protect civil liberties.

It's no surprise so many Americans have lost faith. Aside from the PATRIOT Act, Americans have had to deal with torture scandals that were at least implicitly authorized by their own government. They have had to grapple with the reality that their government detains its own citizens for indefinite periods of time without charge, access to counsel, or due process. And they have had to watch their government conduct racial profiling sweeps and secret tribunals.

Add to these realities the fact that this Administration has been so secretive about its use of the PATRIOT Act, and one can understand why the American public wants answers.

Every American, whether Democrat or Republican, wants to protect this country and all it stands for. But we cannot let our zeal for security destroy our fundamental freedoms. There must be a system of checks and balances to ensure that the goals of security and liberty both receive attention.

I question whether this Administration is succeeding in that challenge. I question this Administration's actions because I love this country too much to sit back and watch our fundamental freedoms give way to indefinite detentions and secret tribunals.

For several years now, this Congress has abrogated its responsibility to ask the tough questions. But today, we have an opportunity to change that. There are difficult decisions ahead of us. I am hopeful that the members of this committee will follow their conscience and not the prevailing political winds of the day. These issues are too important.

As we start this process, I for one plan to keep an open mind. But I cannot do my job unless this Administration starts to provide real answers. We have the time to give thoughtful consideration to whether particular powers actually advance security and adequately protect civil liberties. But we can't do that in a vacuum. We need to know the facts. We need to know whether these powers are actually helping protect this country from terrorism. And we need to know their effect on fundamental freedoms. These are not Republican issues, and they are not Democratic issues. They are American issues, and the public deserves answers. I hope we can get some starting today.

Chairman SENSENBRENNER. Now, I would like to welcome our witness today, Attorney General Alberto Gonzales. He was sworn in as our Nation's 80th Attorney General in February of this year. Prior to his appointment, he served as counsel to President George W. Bush throughout the President's first term. Before coming to Washington, he sat on the Supreme Court of Texas, served as Texas Secretary of State, and served as General Counsel to then-Governor Bush. Before joining the Governor's staff, he was a partner with the law firm of Vinson and Elkins. It is also noteworthy to mention that General Gonzales has served in the Air Force, which adds to his distinguished career.

Welcome, General. We are pleased to have you testify today, and if you will please rise and take the oath, you may proceed afterwards.

Do you solemnly swear that the testimony before this Committee will be the truth, the whole truth, and nothing but the truth, so help you, God?

Attorney General GONZALES. I do.

Chairman SENSENBRENNER. Thank you. Attorney General, you are now recognized.

TESTIMONY OF ALBERTO R. GONZALES, ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Attorney General GONZALES. Chairman Sensenbrenner, Congressman Conyers, and Members of the Committee, I am pleased to be here to discuss an issue relating to the security of the American people and the protection of our cherished freedoms.

Following the attacks of September 11, the Administration and Congress came together to prevent another tragedy from happening

again. One result of our collaboration was the USA PATRIOT Act, which was passed by Congress with overwhelming bipartisan support after carefully balancing security and civil liberties. And since then, this law has been integral to the Government's prosection of the war on terrorism. We have dismantled terrorist cells, disrupted terrorist plots, and captured terrorists before they could strike.

Many of the most important authorities in the Act are scheduled to expire on December 31 of this year. I believe it is important that they remain available. Al-Qaeda and other terrorist groups still pose a grave threat to the security of the American people and now is not the time to relinquish some of our most effective tools in the fight.

As Congress considers whether to renew these provisions, I am open to suggestions for clarifying and strengthening the Act and I look forward to meeting with those both inside and outside of Congress who have expressed concern about some of these provisions. But let me be clear that I cannot support any proposal that would undermine our ability to combat terrorism effectively.

All of us continue to have the same objective, ensuring the security of the American people while preserving our civil liberties. I, therefore, hope that we would consider reauthorization in a calm and thoughtful manner and with the understanding that while the tools of the PATRIOT Act are important, they are not extraordinary. Many of these authorities to deal with terrorists have long been available to prosecutors to deal with ordinary criminals, and actions under the Act often must occur with the approval of a Federal judge. Our dialogue should be based on these facts rather than exaggeration.

And because I believe that this discussion must be conducted in an open and honest fashion, I will begin my testimony today by presenting this Committee with relatively new information recently declassified about the use of certain PATRIOT Act provisions.

Of the 16 provisions scheduled to sunset, I understand that some Members of this Committee are most concerned about sections 206 and 215. Section 215 granted national security investigators authority to seek a court order requiring the production of records relevant to their investigation. Just as prosecutors use grand jury subpoenas as the building blocks of criminal investigations, investigators of international terrorism and espionage cases must have the ability, with appropriate safeguards, to request production of evidence that can be essential to the success of an intelligence investigation.

To be clear, a section 215 order, like a subpoena, does not authorize Government investigators to enter anyone's home or search anyone's property. It is a request for information. A Federal judge must approve every request for records under section 215, and the FISA court has granted the Department's request for a 215 order 35 times as of March 30, 2005.

Although prosecutors have long been able to obtain and have obtained library records in connection with a criminal investigation, I understand section 215 may be considered controversial because of fears concerning its theoretical use to obtain library records. However, I can report the Department has not sought a section 215 order to obtain library or book store records, medical records, or

gun sale records. Rather, the provision to date has been used only to obtain driver's license records, public accommodation records, apartment leasing records, credit card records, and subscriber information, such as names and addresses, for telephone numbers captured through court-authorized pen-register devices.

Going forward, the Department anticipates that our use of section 215 will increase as we continue to use the provision to obtain subscriber information for telephone numbers captured through court-authorized pen-register devices, just as such information is routinely obtained in criminal investigations.

Although some of the concerns expressed about section 215 have been based on inaccurate fears about its use, other criticisms have apparently been based on possible ambiguity in the law. The Department has already stated in litigation that the recipient of a section 215 order may consult with an attorney and may challenge that order in court. The Department has also stated that the Government may seek and a court may require only the production of records that are relevant to a national security investigation, a standard similar to the relevant standard that applied to grand jury subpoenas in criminal cases. The text of section 215, however, is not as clear as it could be in these respects. The Department, therefore, is willing to support amendments to section 215 to clarify these points.

We cannot, however, support elevating the relevant standard under section 215 to probable cause. According to our lawyers and agents, raising the standard would render section 215 a dead letter. As we all know, probable cause is the standard that law enforcement must meet to justify a search for electronic surveillance. It should not be applied to preliminary investigative tools, such as grand jury subpoenas or section 215 orders, which are used to determine whether more intrusive investigative techniques requiring probable cause are justified.

Section 206 also provides terrorism investigators with an authority long possessed by criminal investigators. In 1986, Congress authorized the use of multi-point or roving wiretaps in criminal investigations. Before the PATRIOT Act, however, these orders were not available for national security investigations under FISA. Therefore, when an international terrorist or spy switched telephones, investigators had to return to the FISA court for a new surveillance order and risk missing key conversations.

In a post-9/11 world, we cannot afford to take that risk. Section 206 fixed this problem by authorizing multi-point surveillance of an international terrorist or spy when a judge finds that the target may take action to thwart surveillance; and as of March 30, this provision had been used 49 times.

As in the case of multi-point wiretaps for traditional criminal investigations, section 206 contains ample safeguards to protect the privacy of innocent Americans. The target of roving surveillance must be identified or described specifically in the order. The Government cannot use a 206 roving wiretap order to move from target to target. If the Government wants to obtain a wiretap for a new target, it must go back to court.

Another important FISA-related PATRIOT Act provision is section 207. Prior to this law, the Justice Department invested consid-

erable time returning to court to renew existing orders. Section 207 substantially reduced this investment of time by increasing the maximum time duration for FISA electronic surveillance and physical search orders.

The Department estimates that section 207 has saved nearly 60,000 attorney hours. In other words, it has saved 30 lawyers a year's work, and this estimate does not account for the time saved by FBI agents, administrative staff, and the judiciary. Department personnel were able to spend that time pursuing other investigations and oversight matters.

And given section 207's success, I am today proposing additional amendments to increase the efficiency of the FISA process, copies of which will be presented to this Committee today. And had these proposals been included in the PATRIOT Act, the Department estimates that an additional 25,000 attorney hours would have been saved in the interim. Most of these ideas were specifically endorsed in the recent report of the WMD Commission, which said that these amendments would allow the Department both to "focus their attention where it is most needed," and to maintain the current level of oversight paid to cases implicating the civil liberties of Americans.

Finally, I would like to touch on another provision that has generated significant discussion. Section 213, which is not scheduled to sunset, established a nationwide standard for issuing delayed notice search warrants, which have been used by law enforcement and criminal investigations and approved by courts for decades. Under section 213, law enforcement must always provide notice to a person whose property is searched. A judge may allow that notice to be temporarily delayed, but that person will always receive notification.

The Department uses this tool only when necessary. For instance, from enactment of the PATRIOT Act through January 31 of this year, the Department used section 213 to request approximately 155 delayed notice search warrants, which have been issued in terrorism, drug, murder, and other criminal investigations. We estimate that this number represents less than one-fifth of 1 percent of all search warrants obtained by the Department during this time. In other words, in more than 499 of 500 cases, the Department provides immediate notice of the search. In appropriate cases, however, delayed notice search warrants are necessary, because if terrorists or other criminals are prematurely tipped off that they are under investigation, they may destroy evidence, harm witnesses, or flee prosecution.

I hope that this information will demystify these essential national security tools, eliminate some of the confusion surrounding their use, and enrich the debate about the Department's counterterrorism efforts.

I believe the authorities of the PATRIOT Act are critical to our Nation's success in the war against terrorism. I am, therefore, committed to providing the information that this Committee and the American public need to thoroughly evaluate its effectiveness. The Act has a proven record of success in protecting the security of the American people and we cannot afford to allow its most important provisions to sunset.

I look forward to working with the Committee closely in the weeks ahead, listening to your concerns, and joining together again to protect the security of the American people. Thank you, Mr. Chairman.

Chairman SENSENBRENNER. Thank you very much, Attorney General Gonzales.

[The prepared statement of Mr. Gonzales follows:]

PREPARED STATEMENT OF THE HONORABLE ALBERTO R. GONZALES

Chairman Sensenbrenner, Ranking Member Conyers, and Members of the Committee:

It is my pleasure to appear before you this afternoon to discuss the USA PATRIOT Act. Approximately three-and-a-half years ago, our Nation suffered a great tragedy. Thousands of our fellow citizens were murdered at the World Trade Center, the Pentagon, and a field in rural Pennsylvania. We will never forget that day or the heroes who perished on that hallowed ground. Forever in our Nation's collective memory are stories of the New York City firefighters who rushed into burning buildings so that others might live and of the brave passengers who brought down United Airlines Flight 93 before it could reach Washington, DC, and the messages from those trapped in the World Trade Center saying their last goodbyes to loved ones as they faced certain death will stay forever in our hearts.

In the wake of this horrific attack on American soil, we mourned our Nation's terrible loss. In addition, we came together in an effort to prevent such a tragedy from ever happening again. Members of both parties worked together on legislation to ensure that investigators and prosecutors would have the tools they need to uncover and disrupt terrorist plots. Additionally, members joined hands across the aisle to guarantee that our efforts to update and strengthen the laws governing the investigation and prosecution of terrorism remained firmly within the parameters of the Constitution and our fundamental national commitment to the protection of civil rights and civil liberties.

The result of this collaboration was the USA PATRIOT Act, which passed both Houses of the Congress with overwhelming bipartisan majorities and was signed into law by President Bush on October 26, 2001. In the past three-and-a-half years, the USA PATRIOT Act has been an integral part of the Federal Government's successful prosecution of the war against terrorism. Thanks to the Act, we have been able to identify terrorist operatives, dismantle terrorist cells, disrupt terrorist plots, and capture terrorists before they have been able to strike.

Many of the most important provisions of the USA PATRIOT Act, however, are scheduled to expire at the end of this year. Therefore, I am here today primarily to convey one simple message: All provisions of the USA PATRIOT Act that are scheduled to sunset at the end of this year must be made permanent. While we have made considerable progress in the war against terrorism in the past three-and-a-half years, al Qaeda and other terrorist groups still pose a grave threat to the safety and security of the American people. The tools contained in the USA PATRIOT Act have proven to be essential weapons in our arsenal to combat the terrorists, and now is not the time for us to be engaging in unilateral disarmament. Moreover, many provisions in the Act simply updated the law to reflect recent technological developments and have been used, as was intended by Congress, not only in terrorism cases, but also to combat other serious criminal conduct. If these provisions are not renewed, the Department's ability to combat serious offenses such as cybercrime, child pornography, and kidnappings will also be hindered.

As Congress considers whether to renew key USA PATRIOT Act provisions, I also wish to stress that I am open to any ideas that may be offered for improving these provisions. If members of this Committee or other members of Congress wish to offer proposals in this regard, I and others at the Department of Justice would be happy to consult with you and review your ideas. However, let me be clear about one thing: I will not support any proposal that would undermine the ability of investigators and prosecutors to disrupt terrorist plots and combat terrorism effectively.

It is also my sincere hope that we will be able to consider these crucial issues in a calm and thoughtful fashion. All of us seek to ensure the safety and security of the American people and to protect their civil liberties as well. As this debate goes forward, I will treat those who express concerns about the USA PATRIOT Act with respect and listen to their concerns with an open mind. I also hope that all who participate in the debate will stick to the facts and avoid overheated rhetoric that inevitably tends to obfuscate rather than elucidate the truth.

Today, I would like to use the rest of my testimony to explain how key provisions of the USA PATRIOT Act have helped to protect the American people. I will particularly focus on those sections of the Act that are scheduled to expire at the end of 2005. To begin with, I will discuss how the USA PATRIOT Act has enhanced the federal government's ability to share intelligence. Then, I will explain how the USA PATRIOT Act provided terrorism investigators with many of the same tools long available to investigators in traditional criminal cases. Additionally, I will explore how the USA PATRIOT Act updated the law to reflect new technology. And finally, I will review how the Act protects the civil liberties of the American people and respects the important role of checks and balances within the Federal Government.

INFORMATION SHARING

The most important reforms contained in the USA PATRIOT Act improved coordination and information sharing within the Federal Government. Prior to the attacks of September 11, 2001, our counterterrorism efforts were severely hampered by unnecessary obstacles and barriers to information sharing. These obstacles and barriers, taken together, have been described as a "wall" that largely separated intelligence personnel from law enforcement personnel, thus dramatically hampering the Department's ability to detect and disrupt terrorist plots.

It is vitally important for this Committee to understand how the "wall" was developed and how it was dismantled, not for the purpose of placing blame but rather to ensure that it is never rebuilt. Before the passage of the USA PATRIOT Act, the Foreign Intelligence Surveillance Act (FISA) mandated that applications for orders authorizing electronic surveillance or physical searches under FISA were required to include a certification that "the purpose" of the surveillance or search was to gather foreign intelligence information. This requirement, however, came to be interpreted by the courts and later the Department of Justice to require that the "primary purpose" of the collection was to obtain foreign intelligence information rather than evidence of a crime. And, because the courts evaluated the Department's purpose for using FISA, in part, by examining the nature and extent of coordination between intelligence and law enforcement personnel, the more coordination that occurred, the more likely courts would find that law enforcement, rather than foreign intelligence, had become the primary purpose of the surveillance or search, a finding that would prevent the court from authorizing surveillance under FISA. As a result, over the years, the "primary purpose" standard had the effect of constructing a metaphorical "wall" between intelligence and law enforcement personnel.

During the 1980s, a set of largely unwritten rules only limited information sharing between intelligence and law enforcement officials to some degree. In 1995, however, the Department established formal procedures that limited the sharing of information between intelligence and law enforcement personnel. The promulgation of these procedures was motivated in part by the concern that the use of FISA authorities would not be allowed to continue in particular investigations if criminal prosecution began to overcome intelligence gathering as an investigation's primary purpose.

As they were originally designed, the procedures were intended to permit a degree of interaction and information sharing between prosecutors and intelligence officers, while at the same time ensuring that the FBI would be able to obtain or continue FISA surveillance and later use the fruits of that surveillance in a criminal prosecution. Over time, however, coordination and information sharing between intelligence and law enforcement investigators became even more limited in practice than was permitted in theory. Due both to the complexities of the restrictions on information sharing and to a perception that improper information sharing could end a career, investigators often erred on the side of caution and refrained from sharing information. The end result was a culture within the Department sharply limiting the exchange of information between intelligence and law enforcement officials.

In hindsight, it is difficult to overemphasize the negative impact of the "wall." In order to uncover terrorist plots, it is essential that investigators have access to as much information as possible. Often, only by piecing together disparate and seemingly unrelated points of information are investigators able to detect suspicious patterns of activity, a phenomenon generally referred to as "connecting the dots." If, however, one set of investigators has access to only one-half of the dots, and another set of investigators has access to the other half of the dots, the likelihood that either set of investigators will be able to connect the dots is significantly reduced.

The operation of the "wall" was vividly illustrated in testimony from Patrick Fitzgerald, U.S. Attorney for the Northern District of Illinois, before the Senate Judiciary Committee:

I was on a prosecution team in New York that began a criminal investigation of Usama Bin Laden in early 1996. The team—prosecutors and FBI agents assigned to the criminal case—had access to a number of sources. We could talk to citizens. We could talk to local police officers. We could talk to other U.S. Government agencies. We could talk to foreign police officers. Even foreign intelligence personnel. And foreign citizens. And we did all those things as often as we could. We could even talk to al Qaeda members—and we did. We actually called several members and associates of al Qaeda to testify before a grand jury in New York. And we even debriefed al Qaeda members overseas who agreed to become cooperating witnesses.

But there was one group of people we were not permitted to talk to. Who? The FBI agents across the street from us in lower Manhattan assigned to a parallel intelligence investigation of Usama Bin Laden and al Qaeda. We could not learn what information they had gathered. That was "the wall."

Thanks in large part to the USA PATRIOT Act, this "wall" has been lowered. Section 218 of the Act, in particular, helped to tear down the "wall" by eliminating the "primary purpose" requirement under FISA and replacing it with a "significant purpose" test. Under section 218, the Department may now conduct FISA surveillance or searches if foreign-intelligence gathering is a "significant purpose" of the surveillance or search. As a result, courts no longer need to compare the relative weight of the "foreign intelligence" and "law enforcement" purposes of a proposed surveillance or search and determine which is the primary purpose; they simply need to determine whether a significant purpose of the surveillance is to obtain foreign intelligence. The consequence is that intelligence and law enforcement personnel may share information much more freely without fear that such coordination will undermine the Department's ability to continue to gain authorization for surveillance under FISA.

Section 218 of the USA PATRIOT Act not only removed what was perceived at the time as the primary impediment to robust information sharing between intelligence and law enforcement personnel; it also provided the necessary impetus for the removal of the formal administrative restrictions as well as the informal cultural restrictions on information sharing. Thanks to the USA PATRIOT Act, the Department has been able to move from a culture where information sharing was viewed with a wary eye to one where it is an integral component of our counterterrorism strategy. Following passage of the Act, the Department adopted new procedures specifically designed to increase information sharing between intelligence and law enforcement personnel. Moreover, Attorney General Ashcroft instructed every U.S. Attorney across the country to review intelligence files to discover whether there was a basis for bringing criminal charges against the subjects of intelligence investigations. He also directed every U.S. Attorney to develop a plan to monitor intelligence investigations, to ensure that information about terrorist threats is shared with other agencies, and to consider criminal charges in those investigations.

The increased information sharing facilitated by section 218 of the USA PATRIOT Act has led to tangible results in the war against terrorism: plots have been disrupted; terrorists have been apprehended; and convictions have been obtained in terrorism cases. Information sharing between intelligence and law enforcement personnel, for example, was critical in successfully dismantling a terror cell in Portland, Oregon, popularly known as the "Portland Seven," as well as a terror cell in Lackawanna, New York. Such information sharing has also been used in the prosecution of: several persons involved in al Qaeda drugs-for-weapons plot in San Diego, two of whom have pleaded guilty; nine associates in Northern Virginia of a violent extremist group known as Lashkar-e-Taiba that has ties to al Qaeda, who were convicted and sentenced to prison terms ranging from four years to life imprisonment; two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed, who were charged and convicted for conspiring to provide material support to al Qaeda and HAMAS; Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq as well as two counts of perjury; and Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation, who had a long-standing relationship with Osama Bin Laden and pleaded guilty to a racketeering charge, admitting that he diverted thousands of dollars from his charity organization to support Islamic militant groups in Bosnia and Chechnya. Information sharing between intelligence and law enforcement personnel has also been extremely valuable in a number of other ongoing or otherwise sensitive investigations that I am not at liberty to discuss today.

While the "wall" primarily blocked the flow of information from intelligence investigators to law enforcement investigators, another set of barriers, before the passage of the USA PATRIOT Act, often prevented law enforcement officials from sharing information with intelligence personnel and others in the government responsible for protecting the national security. Federal law, for example, was interpreted generally to prohibit federal prosecutors from disclosing information from grand jury testimony and criminal investigative wiretaps to intelligence and national defense officials even if that information indicated that terrorists were planning a future attack, unless such officials were actually assisting with the criminal investigation. Sections 203(a) and (b) of the USA PATRIOT Act, however, eliminated these obstacles to information sharing by allowing for the dissemination of that information to assist Federal law enforcement, intelligence, protective, immigration, national defense, and national security officials in the performance of their official duties, even if their duties are unrelated to the criminal investigation. (Section 203(a) covers grand jury information, and section 203(b) covers wiretap information). Section 203(d), likewise, ensures that important information that is obtained by law enforcement means may be shared with intelligence and other national security officials. This provision does so by creating a generic exception to any other law purporting to bar Federal law enforcement, intelligence, immigration, national defense, or national security officials from receiving, for official use, information regarding foreign intelligence or counterintelligence obtained as part of a criminal investigation. Indeed, section 905 of the USA PATRIOT Act requires the Attorney General to expeditiously disclose to the Director of Central Intelligence foreign intelligence acquired by the Department of Justice in the course of a criminal investigation unless disclosure of such information would jeopardize an ongoing investigation or impair other significant law enforcement interests.

The Department has relied on section 203 in disclosing vital information to the intelligence community and other federal officials on many occasions. Such disclosures, for instance, have been used to assist in the dismantling of terror cells in Portland, Oregon and Lackawanna, New York, to support the revocation of suspected terrorists' visas, to track terrorists' funding sources, and to identify terrorist operatives overseas.

The information sharing provisions described above have been heralded by investigators in the field as the most important provisions of the USA PATRIOT Act. Their value has also been recognized by the 9/11 Commission, which stated in its official report that "[t]he provisions in the act that facilitate the sharing of information among intelligence agencies and between law enforcement and intelligence appear, on balance, to be beneficial."

Since the passage of the USA PATRIOT Act, Congress has taken in the Homeland Security Act of 2002 and the Intelligence Reform and Terrorism Prevention Act of 2004 other important steps forward to improve coordination and information sharing throughout the Federal Government. If Congress does not act by the end of the year, however, we will soon take a dramatic step back to the days when unnecessary obstacles blocked vital information sharing. Three of the key information sharing provisions of the USA PATRIOT Act, sections 203(b), 203(d), and 218, are scheduled to sunset at the end of the year. It is imperative that we not allow this to happen. To ensure that the "wall" is not reconstructed and investigators are able to "connect the dots" to prevent future terrorist attacks, these provisions must be made permanent.

USING PREEXISTING TOOLS IN TERRORISM INVESTIGATIONS

In addition to enhancing the information sharing capabilities of the Department, the USA PATRIOT Act also permitted several existing investigative tools that had been used for years in a wide range of criminal investigations to be used in terrorism cases as well. Essentially, these provisions gave investigators the ability to fight terrorism utilizing many of the same court-approved tools that have been used successfully and constitutionally for many years in drug, fraud, and organized crime cases.

Section 201 of the USA PATRIOT Act is one such provision. In the context of criminal law enforcement, Federal investigators have long been able to obtain court orders to conduct wiretaps when investigating numerous traditional criminal offenses. Specifically, these orders have authorized the interception of certain communications to investigate the predicate offenses listed in the federal wiretap statute, 18 U.S.C. § 2516(1). The listed offenses include numerous crimes, such as drug crimes, mail fraud, passport fraud, embezzlement from pension and welfare funds, the transmission of wagering information, and obscenity offenses.

Prior to the passage of the USA PATRIOT Act, however, certain extremely serious crimes that terrorists are likely to commit were not included in this list, which prevented law enforcement authorities from using wiretaps to investigate these serious terrorism-related offenses. As a result, law enforcement could obtain under appropriate circumstances a court order to intercept phone communications in a passport fraud investigation but not a chemical weapons investigation or an investigation into terrorism transcending national boundaries.

Section 201 of the Act ended this anomaly in the law by amending the criminal wiretap statute to add the following terrorism-related crimes to the list of wiretap predicates: (1) chemical-weapons offenses; (2) certain homicides and other acts of violence against Americans occurring outside of the country; (3) the use of weapons of mass destruction; (4) acts of terrorism transcending national borders; (5) financial transactions with countries which support terrorism; and (6) material support of terrorists and terrorist organizations.

This provision simply enables investigators to use wiretaps when looking into the full range of terrorism-related crimes. This authority makes as much, if not more, sense in the war against terrorism as it does in traditional criminal investigations; if wiretaps are an appropriate investigative tool to be utilized in cases involving bribery, gambling, and obscenity, then surely investigators should be able to use them when investigating the use of weapons of mass destruction, acts of terrorism transcending national borders, chemical weapons offenses, and other serious crimes that terrorists are likely to commit.

It is also important to point out that section 201 preserved all of the pre-existing standards in the wiretap statute. For example, law enforcement must file an application with a court, and a court must find that: (1) there is probable cause to believe an individual is committing, has committed, or is about to commit a particular predicate offense; (2) there is probable cause to believe that particular communications concerning that offense will be obtained through the wiretap; and (3) "normal investigative procedures" have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous.

Section 206 of the USA PATRIOT Act, like section 201 discussed above, provided terrorism investigators with an authority that investigators have long possessed in traditional criminal investigations. Before the passage of the Act, multipoint or so-called "roving" wiretap orders, which attach to a particular suspect rather than a particular phone or communications facility, were not available under FISA. As a result, each time an international terrorist or spy switched communications providers, for example, by changing cell phones or Internet accounts, investigators had to return to court to obtain a new surveillance order, often leaving investigators unable to monitor key conversations.

Congress eliminated this problem with respect to traditional criminal crimes, such as drug offenses and racketeering, in 1986 when it authorized the use of multi-point or "roving" wiretaps in criminal investigations. But from 1986 until the passage of the USA PATRIOT Act in 2001, such authority was not available under FISA for cases involving terrorists and spies. Multi-point wiretaps could be used to conduct surveillance of drug dealers but not international terrorists. However, such authority was needed under FISA. International terrorists and foreign intelligence officers are trained to thwart surveillance by changing the communications facilities they use, thus making vital the ability to obtain "roving" surveillance. Without such surveillance, investigators were often left two steps behind sophisticated terrorists.

Section 206 of the Act amended the law to allow the FISA Court to authorize multi-point surveillance of a terrorist or spy when it finds that the target's actions may thwart the identification of those specific individuals or companies, such as communications providers, whose assistance may be needed to carry out the surveillance. Thus, the FISA Court does not have to name in the wiretap order each telecommunications company or other "specified person" whose assistance may be required.

A number of federal courts—including the Second, Fifth, and Ninth Circuits—have squarely ruled that multi-point wiretaps are perfectly consistent with the Fourth Amendment. Section 206 simply authorizes the same constitutional techniques used to investigate ordinary crimes to be used in national-security investigations. Despite this fact, section 206 remains one of the more controversial provisions of the USA PATRIOT Act. However, as in the case of multi-point wiretaps used for traditional criminal investigations, section 206 contains ample safeguards to protect the privacy of innocent Americans.

First, section 206 did not change FISA's requirement that the target of multi-point surveillance must be identified or described in the order. In fact, section 206 is always connected to a particular target of surveillance. For example, even if the Justice Department is not sure of the actual identity of the target of such a wiretap,

FISA nonetheless requires our attorneys to provide a description of the target of the electronic surveillance to the FISA Court prior to obtaining multi-point surveillance order.

Second, just as the law required prior to the Act, the FISA Court must find that there is probable cause to believe the target of surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or spy. In addition, the FISA Court must also find that the actions of the target of the application may have the effect of thwarting surveillance before multi-point surveillance may be authorized.

Third, section 206 in no way altered the robust FISA minimization procedures that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons.

Section 214 is yet another provision of the USA PATRIOT Act that provides terrorism investigators with the same authority that investigators have long possessed in traditional criminal investigations. Specifically, this section allows the government to obtain a pen register or trap-and-trace order in national security investigations where the information to be obtained is likely to be relevant to an international terrorism or espionage investigation. A pen register or trap-and-trace device can track routing and addressing information about a communication—for example, which numbers are dialed from a particular telephone. Such devices, however, are not used to collect the content of communications.

Under FISA, intelligence officers may seek a court order for a pen register or trap-and-trace to gather foreign intelligence information or information about international terrorism. Prior to the enactment of the USA PATRIOT Act, however, FISA required government personnel to certify not just that the information they sought to obtain with a pen register or trap-and-trace device would be relevant to their investigation, but also that the particular facilities being monitored, such as phones, were being used by foreign governments, international terrorists, or spies. As a result, it was much more difficult to obtain a pen register or trap-and-trace device order under FISA than it was under the criminal wiretap statute, where the applicable standard was and remains simply one of relevance in an ongoing criminal investigation.

Section 214 of the Act simply harmonized the standard for obtaining a pen register order in a criminal investigation and a national-security investigation by eliminating the restriction limiting FISA pen register and trap-and-trace orders to facilities used by foreign agents or agents of foreign powers. Applicants must still, however, certify that a pen register or trap-and-trace device is likely to reveal information relevant to an international terrorism or espionage investigation or foreign intelligence information not concerning a United States person. This provision made the standard contained in FISA for obtaining a pen register or trap-and-trace order parallel with the standard for obtaining those same orders in the criminal context. Now, as before, investigators cannot install a pen register or trap-and-trace device unless they apply for and receive permission from the FISA Court.

I will now turn to section 215, which I recognize has become the most controversial provision in the USA PATRIOT Act. This provision, however, simply granted national security investigators the same authority that criminal investigators have had for centuries—that is, to request the production of records that may be relevant to their investigation. For years, ordinary grand juries have issued subpoenas to obtain records from third parties that are relevant to criminal inquiries. But just as prosecutors need to obtain such records in order to advance traditional criminal investigations, so, too, must investigators in international terrorism and espionage cases have the ability, with appropriate safeguards, to request the production of relevant records.

While obtaining business records is a long-standing law enforcement tactic that has been considered an ordinary tool in criminal investigations, prior to the USA PATRIOT Act it was difficult for investigators to obtain access to the same types of records in connection with foreign intelligence investigations. Such records, for example, could be sought only from common carriers, public accommodation providers, physical storage facility operators, and vehicle rental agencies. In addition, intelligence investigators had to meet a higher evidentiary standard to obtain an order requiring the production of such records than prosecutors had to meet to obtain a grand jury subpoena to require the production of those same records in a criminal investigation.

To address this anomaly in the law, section 215 of the Act made several important changes to the FISA business-records authority so that intelligence agents would be better able to obtain crucial information in important national-security investigations. Section 215 expanded the types of entities that can be compelled to disclose information. Under the old provision, the FBI could obtain records only from "a common carrier, public accommodation facility, physical storage facility or vehicle rental

facility." The new provision contains no such restrictions. Section 215 also expanded the types of items that can be requested. Under the old authority, the FBI could only seek "records." Now, the FBI can seek "any tangible things (including books, records, papers, documents, and other items)."

I recognize that section 215 has been subject to a great deal of criticism because of its speculative application to libraries, and based on what some have said about the provision, I can understand why many Americans would be concerned. The government should not be obtaining the library records of law-abiding Americans, and I will do everything within my power to ensure that this will not happen on my watch.

Section 215 does not focus on libraries. Indeed, the USA PATRIOT Act nowhere mentions the word "library," a fact that many Americans are surprised to learn. Section 215 simply does not exempt libraries from the range of entities that may be required to produce records. Now some have suggested, since the Department has no interest in the reading habits of law-abiding Americans, that section 215 should be amended to forbid us from using the provision to request the production of records from libraries and booksellers. This, however, would be a serious mistake.

Libraries are currently not safe havens for criminals. Grand jury subpoenas have long been used to obtain relevant records from libraries and bookstores in criminal investigations. In fact, law enforcement used this authority in investigating the Gianni Versace murder case as well as the case of the Zodiac gunman in order to determine who checked out particular books from public libraries that were relevant in those murder investigations. And if libraries are not safe havens for common criminals, neither should they be safe havens for international terrorists or spies, especially since we know that terrorists and spies have used libraries to plan and carry out activities that threaten our national security. The Justice Department, for instance, has confirmed that, as recently as the winter and spring of 2004, a member of a terrorist group closely affiliated with al Qaeda used Internet service provided by a public library to communicate with his confederates.

Section 215, moreover, contains very specific safeguards in order to ensure that the privacy of law-abiding Americans, both with respect to their library records as well as other types of records, is respected. First, section 215 expressly protects First Amendment rights, unlike grand jury subpoenas. Even though libraries and bookstores are not specifically mentioned in the provision, section 215 does prohibit the government from using this authority to conduct investigations "of a United States person solely on the basis of activities protected by the First Amendment to the Constitution of the United States." In other words, the library habits of ordinary Americans are of no interest to those conducting terrorism investigations, nor are they permitted to be.

Second, any request for the production of records under section 215 must be issued through a court order. Therefore, investigators cannot use this authority unilaterally to compel any entity to turn over its records; rather, a judge must first approve the government's request. By contrast, a grand jury subpoena is typically issued without any prior judicial review or approval. Both grand jury subpoenas and section 215 orders are also governed by a standard of relevance. Under section 215, agents may not seek records that are irrelevant to an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

Third, section 215 has a narrow scope. It can only be used in an authorized investigation (1) "to obtain foreign intelligence information not concerning a United States person"; or (2) "to protect against international terrorism or clandestine intelligence activities." It cannot be used to investigate ordinary crimes, or even domestic terrorism. On the other hand, a grand jury many obtain business records in investigations of any federal crime.

Finally, section 215 provides for thorough congressional oversight that is not present with respect to grand-jury subpoenas. On a semi-annual basis, I must "fully inform" appropriate congressional committees concerning all requests for records under section 215 as well as the number of section 215 orders granted, modified, or denied. To date, the Department has provided Congress with six reports regarding its use of section 215.

Admittedly, the recipient of an order under section 215 is not permitted to make that order publicly known, and this confidentiality requirement has generated some fear among the public. It is critical, however, that terrorists are not tipped off prematurely about sensitive investigations. Otherwise, their conspirators may flee and key information may be destroyed before the government's investigation has been completed. As the U.S. Senate concluded when adopting FISA: "By its very nature, foreign intelligence surveillance must be conducted in secret."

UPDATING THE LAW TO REFLECT NEW TECHNOLOGY

As well as providing terrorism investigators many of the same tools that law enforcement investigators had long possessed in traditional criminal investigations, many sections of the USA PATRIOT Act updated the law to reflect new technology and to prevent sophisticated terrorists and criminals from exploiting that new technology. Several of these provisions, some of which are currently set to sunset at the end of this year, simply updated tools available to law enforcement in the context of ordinary criminal investigations to address recent technological developments, while others sought to make existing criminal statutes technology-neutral. I wish to focus on five such provisions of the Act, which are currently set to expire at the end of 2005. The Department believes that each of these provisions has proven valuable and should be made permanent.

Section 212 amended the Electronic Communications Privacy Act to authorize electronic communications service providers to disclose communications and records relating to customers or subscribers in an emergency involving the immediate danger of death or serious physical injury. Before the USA PATRIOT Act, for example, if an Internet service provider had learned that a customer was about to commit a terrorist act and notified law enforcement to that effect, the service provider could have been subject to civil lawsuits. Now, however, providers are permitted voluntarily to turn over information to the government in emergencies without fear of civil liability. It is important to point out that they are under no obligation whatsoever to review customer communications and records. This provision also corrected an anomaly in prior law under which an Internet service provider could voluntarily disclose the content of communications to protect itself against hacking, but could not voluntarily disclose customer records for the same purpose.

Communications providers have relied upon section 212 to disclose vital and time-sensitive information to the government on many occasions since the passage of the USA PATRIOT Act, thus saving lives. To give just one example, this provision was used to apprehend an individual threatening to destroy a Texas mosque before he could carry out his threat. Jared Bjarnason, a 30-year-old resident of El Paso, Texas, sent an e-mail message to the El Paso Islamic Center on April 18, 2004, threatening to burn the Islamic Center's mosque to the ground if hostages in Iraq were not freed within three days. Section 212 allowed FBI officers investigating the threat to obtain information quickly from electronic communications service providers, leading to the identification and arrest of Bjarnason before he could attack the mosque. It is not clear, however, that absent section 212 investigators would have been able to locate and apprehend Bjarnason in time.

Section 212 of the USA PATRIOT Act governed both the voluntary disclosure of the content of communications and the voluntary disclosure of non-content customer records in emergency situations; but in 2002, the Homeland Security Act repealed that portion of section 212 governing the disclosure of the content of communications in emergency situations and placed similar authority in a separate statutory provision that is not scheduled to sunset. The remaining portion of section 212, governing the disclosure of customer records, however, is set to expire at the end of 2005. Should section 212 expire, communications providers would be able to disclose the content of customers' communications in emergency situations but would not be able voluntarily to disclose non-content customer records pertaining to those communications. Such an outcome would defy common sense. Allowing section 212 to expire, moreover, would dramatically restrict communications providers' ability voluntarily to disclose life-saving information to the government in emergency situations.

Section 202, for its part, modernized the criminal code in light of the increased importance of telecommunications and digital communications. The provision allows law enforcement to use pre-existing wiretap authorities to intercept voice communications, such as telephone conversations, in the interception of felony offenses under the Computer Fraud and Abuse Act. These include many important cybercrime and cyberterrorism offenses, such as computer espionage and intentionally damaging a Federal Government computer. Significantly, section 202 preserved all of the pre-existing standards in the wiretap statute, meaning that law enforcement must file an application with a court, and a court must find that: (1) there is probable cause to believe an individual is committing, has committed, or is about to commit a particular predicate offense; (2) there is probable cause to believe that particular communications concerning that offense will be obtained through the wiretap; and (3) "normal investigative procedures" have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous. If wiretaps are an appropriate investigative tool to be utilized in cases involving bribery, gambling, and obscenity, as was the case prior to the passage of the USA PATRIOT

Act, then surely investigators should be able to use them when investigating computer espionage, extortion, and other serious cybercrime and cyberterrorism offenses.

Turning to section 220, that provision allows courts, in investigations over which they have jurisdiction, to issue search warrants for electronic evidence stored outside of the district where they are located. Federal law requires investigators to use a search warrant to compel an Internet service provider to disclose unopened e-mail messages that are less than six months old. Prior to the USA PATRIOT Act, some courts interpreting Rule 41 of the Federal Rules of Criminal Procedure declined to issue search warrants for e-mail messages stored on servers in other districts, leading to delays in many time-sensitive investigations as investigators had to bring agents, prosecutors, and judges in another district up to speed. Requiring investigators to obtain warrants in distant jurisdictions also placed enormous administrative burdens on districts in which major Internet service providers are located, such as the Northern District of California and the Eastern District of Virginia.

Section 220 fixed this problem. It makes clear, for example, that a judge with jurisdiction over a murder investigation in Pennsylvania can issue a search warrant for e-mail messages pertaining to that investigation that were stored on a server in Silicon Valley. Thus, investigators in Pennsylvania, under this scenario, can ask a judge familiar with the investigation to issue the warrant rather than having to ask Assistant United States Attorneys in California, who are unfamiliar with the case, to ask a judge in the United States District Court for the Northern District of California, who is also unfamiliar with the case, to issue the warrant.

The Department has already utilized section 220 in important terrorism investigations. As Assistant Attorney General Christopher Wray testified before this committee on October 21, 2003, section 220 was useful in the Portland terror cell case because "the judge who was most familiar with the case was able to issue the search warrants for the defendants' e-mail accounts from providers in other districts, which dramatically sped up the investigation and reduced all sorts of unnecessary burdens on other prosecutors, agents and courts." This section has been similarly useful in the "Virginia Jihad" case involving a Northern Virginia terror cell and in the case of the infamous "shoebomber" terrorist Richard Reid. Moreover, the ability to obtain search warrants in the jurisdiction of the investigation has proven critical to the success of complex, multi-jurisdictional child pornography cases.

Contrary to concerns voiced by some, section 220 does not promote forum-shopping; the provision may be used only in a court with jurisdiction over the investigation. Investigators may not ask any court in the country to issue a warrant to obtain electronic evidence.

It is imperative that section 220 be renewed; allowing the provision to expire would delay many time-sensitive investigations and result in the inefficient use of investigators', prosecutors', and judges' time.

Moving to section 209, that provision made existing statutes technology-neutral by providing that voicemail messages stored with a third-party provider should be treated like e-mail messages and answering machine messages, which may be obtained through a search warrant. Previously, such messages fell under the rubric of the more restrictive provisions of the criminal wiretap statute, which apply to the interception of live conversations. Given that stored voice communications possess few of the sensitivities associated with the real-time interception of telephone communications, it was unreasonable to subject attempts to retrieve voice-mail message stored with third-party providers to the same burdensome process as requests for wiretaps. Section 209 simply allows investigators, upon a showing of probable cause, to apply for and receive a court-ordered search warrant to obtain voicemails held by a third-party provider, preserving all of the pre-existing standards for the availability of search warrants. Since the passage of the USA PATRIOT Act, such search warrants have been used in a variety of criminal cases to obtain key evidence, including voicemail messages left for foreign and domestic terrorists, and to investigate a large-scale Ecstasy smuggling ring based in the Netherlands.

The speed with which voicemail is seized and searched can often be critical to an investigation given that deleted messages are lost forever. Allowing section 209 to expire, as it is set to do in 2005, would once again require different treatment for stored voicemail messages than for messages stored on an answering machine in a person's home, needlessly hampering law enforcement efforts to investigate crimes and obtain evidence in a timely manner.

Section 217 similarly makes criminal law technology-neutral, placing cyber-trespassers on the same footing as physical intruders by allowing victims of computer-hacking crimes voluntarily to request law enforcement assistance in monitoring trespassers on their computers. Just as burglary victims have long been able to invite officers into their homes to catch the thieves, hacking victims can now invite

law enforcement assistance to assist them in combating cyber-intruders. Section 217 does not require computer operators to involve law enforcement if they detect trespassers on their systems; it simply gives them the option to do so. In so doing, section 217 also preserves the privacy of law-abiding computer users by sharply limiting the circumstances under which section 217 is available. Officers may not agree to help a computer owner unless (1) they are engaged in a lawful investigation; (2) there is reason to believe that the communications will be relevant to that investigation; and (3) their activities will not acquire the communications of non-trespassers. Moreover, the provision amended the wiretap statute to protect the privacy of an Internet service provider's customers by providing a definition of "computer trespasser" which excludes an individual who has a contractual relationship with the service provider. Therefore, for example, section 217 would not allow Earthlink to ask law enforcement to help monitor a hacking attack on its system that was initiated by one of its own subscribers.

Since its enactment, section 217 has played a key role in sensitive national security matters, including investigations into hackers' attempts to compromise military computer systems. Section 217 is also particularly helpful when computer hackers launch massive "denial of service" attacks—which are designed to shut down individual web sites, computer networks, or even the entire Internet. Allowing section 217 to expire, which is set to occur in 2005, would lead to a bizarre world in which a computer hacker's supposed privacy right would trump the legitimate privacy rights of a hacker's victims, making it more difficult to combat hacking and cyberterrorism effectively.

PROTECTING CIVIL LIBERTIES

While the USA PATRIOT Act provided investigators and prosecutors with tools critical for protecting the American people, it is vital to note that it did so in a manner fully consistent with constitutional rights of the American people. In section 102 of the USA PATRIOT Act, Congress expressed its sense that "the civil rights and civil liberties of all Americans . . . must be protected," and the USA PATRIOT Act does just that.

In the first place, the USA PATRIOT Act contains several provisions specifically designed to provide additional protection to the civil rights and civil liberties of all Americans. Section 223, for example, allows individuals aggrieved by any willful violation of the criminal wiretap statute (Title III), the Electronic Communications Privacy Act, or certain provisions the FISA, to file an action in United States District Court to recover not less than $10,000 in damages. This provision allows an individual whose privacy is violated to sue the United States for money damages if Federal officers or employees disclose sensitive information without lawful authorization. Section 223 also requires Federal departments and agencies to initiate a proceeding to determine whether disciplinary action is warranted against an officer or employee whenever a court or agency finds that the circumstances surrounding a violation of Title III raise serious questions about whether that officer or employee willfully or intentionally violated Title III. To date, there have been no administrative disciplinary proceedings or civil actions initiated under section 223 of the USA PATRIOT Act. I believe that this reflects the fact that employees of the Justice Department consistently strive to comply with their legal obligations. Nevertheless, section 223 provides an important mechanism for holding the Department of Justice accountable, and I strongly urge Congress not to allow it to sunset at the end of 2005.

Additionally, section 1001 of the USA PATRIOT Act requires the Justice Department's Inspector General to designate one official responsible for the review of complaints alleging abuses of civil rights and civil liberties by Justice Department employees. This individual is then responsible for conducting a public awareness campaign through the Internet, radio, television, and newspaper advertisements to ensure that individuals know how to file complaints with the Office of the Inspector General. Section 1001 also directs the Office of Inspector General to submit to this Committee and the House Judiciary Committee on a semi-annual basis a report detailing any abuses of civil rights and civil liberties by Department employees or officials. To date, six such reports have been submitted by the Office of the Inspector General pursuant to section 1001; they were transmitted in July 2002, January 2003, July 2003, January 2004, September 2004, and March 2005. I am pleased to be able to state that the Office of the Inspector General has not documented in these reports any abuse of civil rights or civil liberties by the Department related to the use of any substantive provision of the USA PATRIOT Act.

In addition to containing special provisions designed to ensure that the civil rights and civil liberties of the American people are respected, the USA PATRIOT Act also

respects the vital role of the judiciary by providing for ample judicial oversight to guarantee that the constitutional rights of all Americans are safeguarded and that the important role of checks and balances within our Federal Government is preserved. As reviewed above, under section 214 of the Act, investigators cannot utilize a pen register or trap-and-trace device unless they apply for and receive permission from the FISA Court. Section 215 of the Act requires investigators to obtain a court order to request the production of business records in national security investigations. Section 206 requires the Foreign Intelligence Surveillance Court to approve the use of "roving" surveillance in national security investigations. Sections 201 and 202 require a Federal court to approve the use of a criminal investigative wiretap, and sections 209 and 220 require a Federal court to issue search warrants to obtain evidence in a criminal investigation.

Besides safeguarding the vital role of the judiciary, the USA PATRIOT Act also recognizes the crucial importance of congressional oversight. On a semiannual basis, for example, as noted before, I am required to report to this Committee and the House Judiciary Committee the number of applications made for orders requiring the production of business records under section 215 as well as the number of such orders granted, modified or denied. I am also required to fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate on a semiannual basis concerning all requests for the production of business records under section 215. These reports were transmitted by the Department to the appropriate committees in April 2002, January 2003, September 2003, December 2003, September 2004, and December 2004. Moreover, I am required by statute to submit a comprehensive report on a semiannual basis to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate regarding the Department's use of FISA. These reports contain valuable information concerning the Department's use of USA PATRIOT Act provisions, including sections 207, 214, and 218.

I would note that the Department has gone to great lengths to respond to congressional concerns about the implementation of the USA PATRIOT Act. The Department has, for example, provided answers to more than 520 oversight questions from Members of Congress regarding the USA PATRIOT Act. In the 108th Congress alone, in fact, the Department sent 100 letters to Congress that specifically addressed the USA PATRIOT Act. The Department also has provided witnesses at over 50 terrorism-related hearings, and its employees have conducted numerous formal and informal briefings with Members and staff on USA PATRIOT Act provisions. In short, the Department has been responsive and will continue to be responsive as Congress considers whether key sections of the USA PATRIOT Act will be made permanent.

CONCLUSION

In closing, the issues that we are discussing today are absolutely critical to our Nation's future success in the war against terrorism. The USA PATRIOT Act has a proven record of success when it comes to protecting the safety and security of the American people, and we cannot afford to allow many of the Act's most important provisions to expire at the end of the year. For while we certainly wish that the terrorist threat would disappear on December 31, 2005, we all know that this will not be the case. I look forward to working with the Members of this Committee closely in the weeks and months ahead, listening to your concerns, and joining together again on a bipartisan basis to ensure that those in the field have the tools that they need to effectively prosecute the war against terrorism. Finally, Mr. Chairman, we have taken the liberty of supplying the Committee with a copy of FBI Director Mueller's testimony concerning the USA PATRIOT Act, which he presented yesterday before the Senate's Committee on the Judiciary. We ask that it be made a part of this Committee's hearing record, as well.

I look forward to answering your questions today.

Chairman SENSENBRENNER. Before getting to questions, let me just explain the process that I intend to use during this hearing. The Chair has been making notes of the approximate order in which Members have arrived on both sides of the aisle, and after Mr. Conyers and I are done asking General Gonzales questions, the Chair will alternate from side to side in the order in which Members appeared and will let everybody know what the list is with the order.

Because we have a limited amount of time today and because those Members who are going to go to the Pope's funeral have to get out to Andrews Air Force Base, the Chair announces right now off the bat that he is going to strictly enforce the 5-minute rule on everybody, including himself. We will have a break for votes somewhere around 3. If all of the Members who wish to ask questions have not asked their questions by then, we will come back and the remaining Members will be able to ask their questions.

So the Chair now recognizes himself for 5 minutes.

Attorney General Gonzales, as you know, I was instrumental in putting the sunset into the PATRIOT Act because I felt that the Congress should have a chance to have the opportunity to review the effectiveness of the Act's provisions as well as use that as a tool to do oversight over the Department of Justice. Do you believe that the sunset should be completely repealed, or do you think that there should be another sunset put in, and if so, how far in the future do you think we should force another review?

Attorney General GONZALES. Mr. Chairman, it was my understanding that the sunset provisions were included in the Act because of concerns about whether or not the Congress had achieved the right balance between protecting our country and securing our civil liberties. We've now had a period of time to evaluate how these provisions work, how the Department has used these provisions. I think it's a strong record of success. I think the Act has been effective. I think the Department has acted responsibly. I think there is sufficient information for the Congress to make a determination that, in fact, these provisions should be made permanent.

As a matter of reality, we all understand that the Congress at any time, the next year or the year after, could at any time evaluate whether or not certain provisions should be discontinued, and so even if the decision were made to remove the sunsets, that would not, in my judgment, in any way affect the ability or the right or the authority of Congress to examine and reexamine the way that these authorities are working and the way that the Department is using these authorities.

Chairman SENSENBRENNER. One of the things that I believe all Members of the Committee and particularly I have heard is concerns about section 215. Let me say that—or make two points. First of all, I am gratified at your testimony that the Justice Department has never sought bookstore, medical, or gun sale records under section 215.

Secondly, I would observe that if section 215 is repealed, as some have advocated, all of these records would still be available to law enforcement through the procedure of a grand jury subpoena, and with a grand jury subpoena, it is up to the recipient to hire a lawyer and move to quash the subpoena in Federal court, whereas under section 215, there is judicial review by the FISA court before the FISA warrant is issued under section 215.

I salute your willingness to have some amendments to section 215 to clarify the process under which the Justice Department utilizes this section. Can you talk in a little bit greater detail on how you suggest section 215 be amended to do so?

Attorney General GONZALES. As I have indicated, Mr. Chairman, the Department has taken the position in litigation that we interpret 215 as including an implicit right for a recipient of a 215 order to challenge that order. We also read in the statute the right of a recipient to disclose the existence of a receipt of an order to an attorney in order to help them prepare such a challenge.

I, quite frankly, understand the concerns at the fact that the statute doesn't have those rights explicitly spelled out in the statute, and for that reason, the Department is quite comfortable supporting an amendment to make it clear that, in fact, those authorities should be included as part of a statute.

Another important point that we would support is the specific acknowledgement of what the appropriate standard is. There is some question as to whether or not a relevance standard is applicable in the statute. We believe it does. We believe that is the applicable statute—standard, even though that—and we think judges have interpreted 215 to impose a relevance standard. But in order to remove any doubt or ambiguity, we would support the explicit acknowledgment that that is the standard that must be met whenever we go to the Federal judge, that that is the standard that we have to meet in order to receive a 215 order.

Chairman SENSENBRENNER. Thank you. My time has expired.

The gentleman from Michigan, Mr. Conyers?

Mr. CONYERS. Thank you, Mr. Chairman. Thank you.

I have within the time allotted to me three questions. One is about the Brandon Mayfield incident in which the PATRIOT Act was used.

The second is about terrorists' access to guns in which we have a GAO study that shows, Mr. Attorney General, that out of 56 firearm purchase attempts by individuals designated as suspected terrorists, 47 of them were permitted to involve themselves in—were able to purchase weapons.

And my third question is about racial and religious profiling in which since September 11 the Department of Justice has interviewed over 3,000 Middle Eastern immigrants, counted mosques and surveyed their attendees, registered over 83,000 Arab and Muslim visitors, interviewed 10,000 Iraqi nationals, and I wanted to find out what all this profiling was for, racial and religious profiling, which is contrary to FBI guidelines, and what do we have to show for it?

Let's start with Brandon Mayfield, who really got hit up pretty hard and I think, to make this a short conversation, you've already conceded that the PATRIOT Act was involved, right?

Attorney General GONZALES. What I have said, Congressman, is that section 213 was not implicated—was not used. There were stories, I believe, in the press that section 213 of the PATRIOT Act was the basis for the search. That is not true.

What I have said is that the PATRIOT Act is implicated to the extent that this was a FISA search and that FISA, the provisions of FISA were amended by the PATRIOT Act. For example, section 218, which deals with changing the standard from the purpose to a significant purpose in targeting an intelligence investigation, and also sections——

Mr. CONYERS. Excuse me, sir. Sections 207 and 218 were involved, right? Sections——

Attorney General GONZALES. Sections 207 and 218, that's what I was just saying.

Mr. CONYERS. Yes.

Attorney General GONZALES. Yes.

Mr. CONYERS. So the answer is yes.

Attorney General GONZALES. To the extent that we're talking about utilizing FISA and to the extent that the PATRIOT Act amended provisions of FISA, yes. Provisions of the PATRIOT Act were used in connection with that investigation, but I might add that based on what I know today, and I'm limited in what I can say because this matter is in litigation, I don't believe that the Brandon Mayfield case is an example where there was a misuse or abuse of a provision of the PATRIOT Act.

Mr. CONYERS. Well, let me just ask you, can we on this Committee cooperate with you to open up those Mayfield files so we can learn exactly how the PATRIOT Act was used in this case? The Seattle Times and others widely report PATRIOT Act use in Portland, attorney investigation, Attorney General says, and goes on and on and on, and I think you've said the same thing here.

Attorney General GONZALES. Again, Congressman, this matter is in litigation so I'm likely to be limited about what information I can share with you, but I'm happy to go back and see what we can do to provide information to the Committee in connection with this case.

Mr. CONYERS. Let's go on to the——

Attorney General GONZALES. The GAO report. Congressman, it is up to Congress to determine who is able to possess a firearm in this country. Congress designates certain categories of people, based upon various actions, that make them disabled from owning a firearm. If someone does not have such a disability which has been recognized by Congress, even though they're a terrorist, there are limits to what this Department can do to prevent them——

Mr. CONYERS. Would you be willing to support legislation limiting a terrorist's access to such weapons?

Attorney General GONZALES. I think that we'd be willing to consider looking at such legislation, Congressman——

Mr. CONYERS. Well, 47 suspected terrorists were able to get weapons. What——

Attorney General GONZALES. Let me try to explain that we try to be very, very careful about who appears on the Terrorist Watch List.

Mr. CONYERS. Sure.

Attorney General GONZALES. There are various reasons that people appear on the Terrorist Watch List, and so the fact that someone appears on the Terrorist Watch List——

Mr. CONYERS. That doesn't make them a good guy.

Chairman SENSENBRENNER. The gentleman's time has expired.

The gentleman from California, Mr. Lungren?

Mr. LUNGREN. Thank you very much, Mr. Chairman, and welcome again to the Committee, Mr. Attorney General.

Mr. Attorney General, when I've had town hall meetings in my district, even though I'm a former Attorney General of California,

and try to explain it in legal terms, I've had people raise section 213. They don't know it as delayed notification. They know it by another name. And a concern is always raised about this would necessarily lead to abuses and somehow seems unfair.

This is an investigative authority that has been used in cases other than terrorism. Could you just explain why that is an important technique, an important authority, and how, if extending it to terrorism cases, it changes the nature of it or the seriousness of the authority given, or if it does not? That is, what would you say to my constituents who ask me this question at town hall meetings, despite my best efforts to answer them?

Attorney General GONZALES. I would respond by maybe giving them this hypothetical. I'm going to change some facts here about a hypothetical and how this tool can be very useful in dealing with terrorism, and that is, let's say, we uncover ammonium nitrate, a large stockpile of ammonium nitrate. It is a very important ingredient in creating a very dangerous bomb. So we discover this. We don't know who all is involved in this plot, this possible conspiracy. So we want to make sure we get everyone involved in it. On the other hand, we want to grab it because we're concerned that we may lose track of it and it may be used to build a bomb and kill lots of people.

And so we get a delayed notification warrant that allows us to come in. We substitute the ammonium nitrate with an inert substitute and we're able to continue the investigation to the appropriate time without jeopardizing a possible creation of a bomb, an explosion killing hundreds of people. So that would be an example of where the ability to go in and do a search without notifying the target can be extremely beneficial until the time comes when we have sufficient information to make our case, and that would be an example that I would provide to your constituents.

Mr. LUNGREN. And is that any different than what we do in other kinds of criminal cases with the delayed notification authority?

Attorney General GONZALES. Delayed notification warrants have been in place for many, many years in ordinary criminal investigations for a wide variety of crimes. People need to understand that it is under the jurisdiction and supervision of a Federal judge. We still have to show the probable—we still have to meet the probable cause standards, and so——

Mr. LUNGREN. And that is all done prior to the time that the entry is made or the——

Attorney General GONZALES. Absolutely. We go to a judge like in every other case and we make our case, present the facts, and the judge makes the determination whether or not we meet the standards under the Constitution.

Mr. LUNGREN. Mr. Attorney General, you have said here and you've said before, and I'll quote an article in the New York Times that quotes you as warning Congress that we cannot afford to assume the quiet of the day will mean peace for tomorrow and the terrorist threat will not expire, even if parts of the PATRIOT Act are allowed to. If we fail to renew these provisions of the PATRIOT Act, could you tell us how this would harm law enforcement, be-

cause we made sort of a broad statement that it would, but specifically, how would it?

Attorney General GONZALES. One major way would be in the sharing of information. If you look at the reports of the 9/11 Commission and the WMD Commission, both have acknowledged that a serious weapon—the most effective weapon in dealing with terrorism is in the sharing of information. And prior to the PATRIOT Act, there were questions within the law enforcement community about how much information could be shared by those in the Intelligence Community with law enforcement, and those questions were laid to rest by certain provisions in the PATRIOT Act.

If those provisions were sunsetted, we would once again be in a situation where law enforcement would be very, very cautious in sharing of information. They would want to check with their superiors, and so it would cause delays in investigations and I think would needlessly tie the hands of American investigators in dealing with this threat.

Mr. LUNGREN. Thank you, Mr. Attorney General. I might just say for the record, while I understand what you say about perhaps we don't have the need to put in the sunset in the future, as a spur to Congress to make sure we do appropriate oversight, I'm inclined to support a sunset provision in the future, because, frankly, this is serious and the people need to be assured that we are, in fact, doing the oversight that is necessary.

Chairman SENSENBRENNER. The time of the gentleman has expired.

The gentleman from California, Mr. Schiff?

Mr. SCHIFF. Mr. Attorney General, I want to thank you for being here. I'm a former Assistant U.S. Attorney and I greatly value the work done by Justice Department people all over the country.

I'm an original cosponsor of the House version of the PATRIOT bill. In my view, the PATRIOT bill was a bargain. We would give the Government greater ability to investigate and prosecute terrorism suspects, and in return, we would take upon ourselves greater responsibility for overseeing these more powerful tools.

In my view, we have not kept up our part of the bargain. We have not done adequate oversight of the PATRIOT bill in this House or in this Committee. For the Justice Department's part, I believe the Department has not been forthcoming with the information that we would need also to do our job of oversight.

And in one area in particular, I have been most concerned. This is an area both within, but largely without, the PATRIOT bill and that is the detention of Americans and lawful residents as enemy combatants. For 3 years now, I have been raising this issue, what the standards ought to be for the detention of an American, what due process should be afforded. I introduced legislation 3 years ago to authorize the detention of enemy combatants, but to ensure that there was access to judicial review and access to counsel.

We've had no hearing on any of this legislation. Indeed, requests to have a hearing just on the issue of the detention of Americans have not been successful. We have had no hearing on this subject. That's been our problem, our unwillingness to set any limit on the power of the executive to detain an American citizen. That's been our problem.

At the same time, efforts that I've made to learn information from the Justice Department and the Defense Department about our Government's own policies of when we treat someone as an enemy combatant or when we treat them as a criminal defendant—when we treat them as a defendant with all of the rights that attach to that, when we treat them as an enemy combatant with none of the due process that attaches to that, I have been unable to get really any meaningful information, even in classified form.

When you gave a speech to the ABA a year or two ago, it was the most information I had ever heard about how we were deciding when to treat someone as an enemy combatant. More information than you gave publicly was denied me in classified form. That cannot persist.

I find it odd that there aren't more voices in the Congress raising this issue, that aren't demanding that Congress act to set limits on the detention of Americans, to set due process for the detainees at Guantanamo. Of course, all this thing, not done for the terrorism suspects but done for all the rest of us, to protect our civil liberties and our due process. I find it very odd there have been so few voices in the Congress on this issue, but I find I have a new and powerful ally on the Supreme Court of the United States.

As you know, the District Courts have been conflicting about whether the executive has the power to detain enemy combatants and under what conditions. Justice Scalia, in one of his dissenting opinions, commented, "I frankly do not know whether the tools are sufficient to meet the Government's security needs, including the need to obtain intelligence through interrogation. It is far beyond my competence or the Court's competence to determine that, but it is not beyond Congress's." We could not have, I think, a stronger admonition that we need to act in the Congress, and so I'm in the unusual position of asking you to help us to do our job.

Mr. Attorney General, do you believe, as I do, that the Justice Department's power to detain enemy combatants, which I believe the Department has to have in the war on terrorism, don't you believe that power is strengthened when the Congress acts to provide both the authority clearly and the due process clearly? Isn't the power strengthened because it will now have the imprimatur of both the legislative and executive branch and, therefore, have the respect of the judicial branch? Shouldn't we act so that we don't have piecemeal decision making by the courts? Will you work with the Congress to propose legislation setting out the due process for the detention of Americans as enemy combatants and the detainees in Guantanamo?

Attorney General GONZALES. Congressman, there is a lot there to respond to. Generally, in the area of war, the framers of the Constitution gave both to the executive branch and to the legislative branch certain powers, and I think in the exercise of the power, I, for one, as someone who looks at these things, look at where you are on the continuing spectrum.

I mean, for example, if the—if America is attacked, I think this President, as Commander in Chief, can take action to defend this country without action by Congress. I think he has the authority to do that. But if we're talking about taking 100,000 troops into another country for an extended period of time, then it becomes, I

think, more difficult whether or not—can the Commander in Chief do that without any kind of Congressional authorization.

I think the Framers probably had it right. It probably works best, particularly when we talk about putting the lives of men and women at risk, to have both branches working together in most cases. Whether or not legislation is appropriate, these are very, very difficult issues. I have really discovered how difficult these issues have been these past 4 years.

There is a reason why courts around this country reach conflicting decisions about these issues, because they are so hard. Many of the issues have never been confronted in our courts before. It's a new kind of war, and some of the old rules just don't apply. And so we try to deal with them.

And so to answer directly your question about whether or not legislation would be beneficial, I'd have to look at the circumstances. I'd have to look at the legislation, quite frankly.

You're right. We waited too long, in my judgment, to respond, to explain to the American people what we're doing and why, and it was one of the things that I mentioned in that speech you referred to, is that we waited. We waited a long time because of concerns that we didn't want to say anything that might help the enemy, might jeopardize something that we're doing. But we finally acknowledged that we were hurting ourselves, that the American people and the Congress really needed to know what we were doing and why, and that was—I'm delighted to know about your speech, because I did, I think, talk a lot about the process that we used in designating someone as an enemy combatant or having them go through the criminal justice system.

Chairman SENSENBRENNER. The time of the gentleman has expired.

The time of the gentleman from Texas, Mr. Smith.

Mr. SMITH OF TEXAS. Thank you, Mr. Chairman.

General Gonzales, thank you for being here today. General Gonzales, recently, you made the statement that you felt that the PATRIOT Act is working and, in fact, it has helped to prevent additional terrorist attacks. Could you be more specific? Could you point to the number of individuals, the number of would-be terrorists who might have been detected and apprehended? Can you point to terrorist rings that might have been disrupted or broken up to substantiate that statement?

Attorney General GONZALES. It's kind of hard to sort of prove a negative or show a negative. I can certainly—I've got a list here of where the PATRIOT Act has been beneficial or helpful. I can certainly provide to the Congress and to you examples of cases where the PATRIOT Act has been very helpful.

Mr. SMITH OF TEXAS. Let me just——

Attorney General GONZALES. I would just repeat what I said earlier in a response to another question about, I mean, just the sharing of information. There's a reason that there's not been another attack in this country, quite frankly, and not just the PATRIOT Act. I know this Congress worked very hard in standing up a new Department, Homeland Security, so a lot of actions taken by the Government in order to defend this country.

But I think the PATRIOT Act has been very, very helpful. We have in various cities around the country, in Portland, Oregon, in Buffalo and Detroit, I mean, in New York City, rounded up people who were engaged in plotting another terrorist attack. Often times, we obtain convictions. Some critics of the Administration have said, well, you've only got low-level convictions. That's because we try to preempt something really bad from happening, and so sometimes we cannot—we have to move in early enough to prevent another attack and we don't have a sufficient basis to prosecute someone for something really serious.

Mr. SMITH OF TEXAS. General Gonzales, how many convictions have you obtained?

Attorney General GONZALES. I don't know, but I can get that information for you.

Mr. SMITH OF TEXAS. Okay. I would be curious about that.

Let me go to another aspect or another kind of terrorist threat. You are aware, I am sure, that last year, the number of individuals coming across our Southern border from terrorist-sponsoring nations increased dramatically, and I'm just wondering what we're doing to target the individuals who might be coming into our country to commit terrorist acts.

And as a sort of a second part of that question, I point out, which you also know to be the case, the Border Patrol tells us that for every three individuals seeking to come into the country illegally, two succeed. Two out of every three people who want to come into the country illegally are able to do so. We wouldn't be surprised, given that, that there might not be another terrorist attack. But what is your response as to how we can prevent that from occurring and how we target the individuals who might be coming across the border who would be—might be would-be terrorists from terrorist-sponsoring countries?

Attorney General GONZALES. Congressman, I know the immigration issue is one that you have spent a lot of time on and you have a lot of expertise and knowledge about. It is a very, very difficult issue. As I've said many times in talking about this issue, because we have a country that traditionally has invited immigrants, we embrace them, we want them to come in our country, it is the fabric of our great country, is the contributions of immigrants.

We have generally an open border in the South. People along the border communities cross the border every day, back and forth, so that they can go to work, provide for their families, and that's the reality of life.

On the other hand, a new reality after September 11 is the fact that we need to do what we can do to make it so that terrorists cannot come into this country. Of course, the Department of Homeland Security has now the primary responsibility for dealing with that. I know Mike Chertoff, he and I have spoken about this issue. We've invested money, the Congress working with the Administration and making sure additional monies are available for additional agents. Our technology is getting better. But we still have a long way to go. I mean, this is a very difficult issue. It's one that's existed for many, many years. If it were one that could easily be solved, it would have been solved a long time ago. But I just—we'll continue to work with the Congress to try to address it.

We understand it's a problem. I was in Mexico last week. We talked about this issue with President Fox and the Attorney General in Mexico, and so they understand that we consider it a serious—we're seriously concerned about it, and I was reassured by the Attorney General that they consider it an issue for them. They realize how harmful it would be for their economy, their tourism, if, in fact, we have a situation where terrorists come up from Latin America, other countries, through Mexico into our country and cause another attack. They realize how damaging that would be, and so they're very concerned about it, as well.

Mr. SMITH OF TEXAS. Thank you, General Gonzales. Regarding my first question, the number of convictions, I understand it's in the 80's to 90's range, and I'll look forward to that information.

Attorney General GONZALES. Thank you.

Mr. SMITH OF TEXAS. Thank you, Mr. Chairman.

Chairman SENSENBRENNER. The time of the gentleman has expired.

The gentleman from California, Mr. Berman?

Mr. BERMAN. Thank you very much, Mr. Chairman, and thank you, Mr. Attorney General, for being here and for at least conveying the impression that you sometimes hear and even understand the questions we ask. That's already an improvement over your predecessor.

The PATRIOT Act sunset provisions you've discussed, I frankly think most Members of Congress have come or will come to the conclusion that many of these sunsetted provisions should be—perhaps all of them should be continued, perhaps refined. Mr. Chairman, I would hope this review, though, would also take into account a number of unilateral actions—Mr. Schiff certainly brought up one in the context of the enemy combatants issue—that we should be considering that weren't part of the PATRIOT Act but were developed in response to September 11 and in our effort to fight a more effective war on terror.

Some of these include policies instituted without any input from Congress, mining data from public and non-public databases, blanket closure of deportation hearings to the public, blanket closure, denial of bond to whole classes of non-citizens, altering the makeup of the Board of Immigration Appeals in a way that has overwhelmed the Federal circuit courts, and permitting the DOG's immigration attorney's to unilaterally overrule an immigration judge when he has ordered someone released on bond.

Today, Mr. Delahunt and I are introducing a law we call the Civil Liberties Restoration Act. It doesn't repeal any part of the PATRIOT Act. It doesn't impede in any way the ability of agencies to share information. Our goal is simply to ensure there are appropriate checks and balances on a number of PATRIOT provisions as well as an opportunity for Congress to address some of the unilateral policy decisions that I just mentioned. They're all drafted, we think, in a way that tries to achieve the balance that you and others have talked about. I would hope at some point you might have a chance to take a look at some of the proposals contained in that legislation.

But I think the 9/11 Commission was instructive on this issue, and my question to you is—I'm going to mention—they established

some standards for the process that we are now about to embark on and I'd like your reaction to it. The 9/11 Commission essentially said we should reexamine the specific provisions that sunset, taking care not to renew any provision unless the Government can show, one, that the power actually materially enhances security, and two, that there is adequate supervision of the executive's use of the power to ensure protection of civil liberties.

Secondly, if the power is granted, there must be adequate guidelines and oversight to properly confine its use.

And thirdly, on the issue I've just touched on, because the issues of national security and civil liberties posed by anti-terrorism powers that are not part of the PATRIOT Act sunset are at least as serious as any posed by those provisions that do sunset, Congress should undertake the broader review of anti-terrorism powers both within and outside of the PATRIOT Act, using the same standard of review that I just mentioned for the sunset provisions.

Anything wrong with that as a methodological approach for us to begin this effort?

Attorney General GONZALES. I think this country was founded by people concerned about the exercise of power in our home country and I think it is appropriate to always—to question and to examine the exercise of power by the Government, and so I welcome—that's why I welcome this debate.

I think that the record shows that the PATRIOT Act has been effective. I think the record shows that the exercise of the authorities granted to the Department of Justice have been used wisely and judiciously. But I think that——

Mr. BERMAN. Let me just throw out one thing here. For instance, in our bill that we're introducing today, the blanket closure of all immigration hearings, why isn't it case by case? Where there's a legitimate national security reason to close that hearing, by all means, you ought to have the authority to have that hearing closed. But why does there need to be a blanket closure?

Attorney General GONZALES. Congressman, I wasn't involved——

Mr. BERMAN. Can you defend that decision?

Attorney General GONZALES.—I wasn't involved in that decision, and so I probably do not know—in fact, I know I don't know all the facts that were weighed or considered in connection with that——

Mr. BERMAN. From what you know now, what do you think of that?

Attorney General GONZALES. Well, I think that there were mistakes made, quite frankly, and I think if you look at the IG report about the detentions of immigrants, there were some mistakes made. We've worked very, very hard—the Department has worked hard to try and address and respond to the recommendations made by the IG. But in terms of the blanket, that would be something I would have to look at.

Chairman SENSENBRENNER. The time of the gentleman has expired.

The gentleman from Iowa, Mr. King?

Mr. KING. Thank you, Mr. Chairman.

Mr. Attorney General, I thank you for being here to testify today, I believe the first time in the position that you're in. I welcome you to the Judiciary Committee.

A series of questions have arisen as I listened to your testimony and the questions here today and one of them is with regard to the question asked by the Ranking Member. Fifty-six attempts to purchase guns and 47 of them were successful in purchasing guns, and as I listened to the follow-up question, I heard the phrase, "suspected terrorists." Was there any anticipation that suspected terrorists would be screened from getting guns, and could you also speak as to under what circumstances the other nine might have been prohibited?

Attorney General GONZALES. I don't have the information about the other nine. We—unless Congress says that if you have this disability or something or you have this characteristic or you've done this kind of action, you're going to be entitled to own a firearm in this country. As I've said before, we do not want to see a situation where terrorists have the right to possess a weapon in this country. But at the end of the day, all we can do is enforce the law.

Under our current structure, you are disabled if you've been involved in some kind of domestic abuse. You're disabled if you're an illegal immigrant. You're disabled if you're a felon. But in that list of disabilities is not the words "terrorist." That doesn't mean that we just give up. Obviously, when someone wants to purchase a weapon and there's a hit on the Terrorist Watch List, we tried to alert the local officials and see if we can get additional information to find out if there is a way that this person can either be arrested or deported or can we discover some kind of disability to prevent them from getting a weapon. But if we can't do that, they're entitled under the law to get a weapon.

Mr. KING. We don't have a category for suspected terrorists and I think that's the summary of that answer and I thank you.

Then on another subject matter, the PATRIOT Act requires the Inspector General of the Department of Justice to provide a twice-yearly report as to the civil liberties, whether they have been violated by use of the PATRIOT Act, and it's my understanding that those six reports have not found a single violation of civil liberties.

Would you care to expand on that? I guess the question comes to me is why do I continually hear the stories about civil liberties being violated—and I'd expand my question a little more in that I'm inclined to support eliminating the sunset on the PATRIOT Act for the very reason of the demagoguery that I hear about the abuse of the PATRIOT Act and not finding evidence of it.

Attorney General GONZALES. You are correct, sir, that the IG is required to submit a report semi-annually about abuses under the PATRIOT Act, and to date, he has not been able to report any abuses under the PATRIOT Act. I visited with our IG several weeks ago and asked him again, are you aware of any such abuses, and he said no.

And as I travel around the country and I've encouraged other officials within the Department of Justice to go out and try to solicit examples of where real abuses or misuses of the PATRIOT Act have occurred, there's a lot of misinformation, a lot of disinformation out there. Some people believe that because certain provisions may have been struck down, that means that the PATRIOT Act was somehow found unconstitutional, and we discov-

ered that, no, it related to a provision that was passed by the Congress years before the PATRIOT Act.

And so I think that, again, I think the record of the Department is a very good one regarding the use of the PATRIOT Act. I think that the record also reflects that Congress probably did a pretty good job in achieving a good balance between protection of civil liberties and protection of this country.

Mr. KING. Thank you. And then with regard to section 215, do you believe there's a reason to expand that to cover domestic terrorism, as well?

Attorney General GONZALES. I would have to look at that, Congressman. I don't have an answer for that, whether or not 215 should be expanded to include domestic terrorism.

Mr. KING. And then off of Mr. Smith's statement with regard to the—I mean, really, the amount of immigrants coming into this country on the illegal side, it looks like that number is over three million, if using that extrapolation of Mr. Smith's remarks. And out of that huge haystack, how would you think it would be logical that we could sort the terrorist needles out of 3.4 million illegals?

Attorney General GONZALES. I think it would be difficult. Obviously, from our perspective, I think it is good if we know who is coming into this country and why they're coming into this country. The key question is, how do we do that, and that's something that we're working on and I know Members of Congress have been thinking about and are continuing to work on it, because it is a very important issue.

Mr. KING. And I would suggest reducing the size of the haystack. Thank you, General Gonzales. Thank you, Mr. Chairman.

Chairman SENSENBRENNER. The gentleman's time has expired.

The gentleman from New York, Mr. Nadler?

Mr. NADLER. Thank you. Mr. Attorney General, my basic problem with all of this is that the Administration, the current Administration that's enforcing the PATRIOT Act seems to have no sense of limits and no sense of due process whatsoever when dealing with real or alleged terrorism cases. I will cite, for instance, the memo that you wrote justifying torture, which I am sure you won't characterize as such, but I will.

Number two, the whole doctrine of the enemy combatants that Mr. Schiff talked about in which the President has claimed the power to point his finger at any American citizen—or non-citizen—but any American citizen and say, you are an enemy combatant because I say so on the basis of secret information which I won't reveal to you or anyone else, and by that declaration, I have the power to throw you in jail forever with no due process, no hearing, no evidence, no nothing. Nobody, to my knowledge, no executive in an English-speaking country has made such a claim of tyrannical power since before Magna Carta, and yet—and the Justice Department under your predecessor had the nerve to say to the Federal courts that they didn't have the jurisdiction to even question the fact or the authority of the President.

Third, you stated in your opening statement that the PATRIOT Act was well considered and well balanced. Well, maybe it's balanced and maybe not, but it certainly wasn't well considered. If you recall how it passed here, this Committee considered in detail a

PATRIOT Act, considered for 4 days, voted on amendments, marked it up, unanimously reported the bill on a Thursday, I believe. Over the weekend, the leadership of the House together with the Administration took the well-considered bill, which I thought was balanced, and threw it in the garbage, wrote over the weekend an entirely new bill, presented this 200-and-some-odd-page bill to the House with two copies available, one for the Democrats, one for the Republicans, warm to the touch at 10 in the morning. We started the debate at 11 and voted on it at 1 and nobody had a chance to read it. So it's certainly not well considered. It may be well balanced, but certainly not well considered.

In light of all this, I have two specific questions about the bill. There are provisions in the PATRIOT Act that are fine and that have positively reformed the way intelligence is gathered and used to protect the United States and provisions that I think are over the top.

Last September, a judge in the Southern District of New York, Judge Morero, ruled that section 505 dealing with national security letters violated two constitutional principles, the first amendment right to freedom of speech and the right to be free from unreasonable searches and seizures under the fourth amendment. Section 505 authorizes the FBI, using only a piece of letterhead paper signed by a field agent in charge of a local FBI office, to demand private information without court review or approval, without the person being suspected of any crime, without ever having to tell him or her that it happened.

Moreover, the business from which the FBI gets these private records is gagged and prohibited from notifying the targeted individual, so they may never move in court to quash this request or to even question it.

Do you believe that section 505 should be either stricken or amended, question number one?

Question number two is that section 206 creates roving wiretaps in intelligence cases which allows the Government to get a single order that follows a target from phone to phone, which I think makes sense. But in addition, last year's Intelligence Authorization Act allows the Government to issue John Doe wiretaps where the phone and facility is known but the target is not. The combination of these two laws seems to allow for a general wiretap, one that follows an unknown suspect from unknown phone to unknown phone.

Should this section be changed to clarify that the Government would specify either the person or the phone to be tapped, or are we now into the business of general wiretaps like the British Writs of Assistance that helped spark the American Revolution?

Attorney General GONZALES. Thank you, Congressman. As to 505, I don't think that 505, I think, should be amended or deleted. The court, as I understand it, found a problem with the fact that a person did not have the right to contest the national security letter or to tell anyone about the national security letter, even though the Department took the position, yes, you do, and we argued that in that litigation.

Mr. NADLER. That was one of the problems it found.

Attorney General GONZALES. I don't think that the court had a problem per se with 505, and some people have characterized this as a decision by the court that somehow struck down a provision of the PATRIOT Act when an ACLU attorney himself even acknowledged that, no, that wasn't the case. The problem was the first amendment and the fourth amendment and it did not relate to the PATRIOT Act, in my judgment.

In terms of roving wiretaps, in my reading of 206, I believe that the Department has an obligation to identify a specific target. We may not know the name of that person, but we have to go before a Federal judge and give the judge enough information that the judge is comfortable that we've satisfied the probable cause standard as to a specific target being a foreign power or an agent of a foreign power. That's the first thing.

And so it's not the case that if we get a wiretap on person A and we discover—a roving wiretap on person A and we discover, whoops, this is not the right guy, let's listen to the phone of this person, if we go to person B, we have to get another order from a Federal judge. So it's not the case—we get an order for one specific person.

Now, when we go to the judge, we also go to the judge having to satisfy a probable cause standard as to a particular location or facility or phone that the terrorists or target is either about to use or is using. So it wouldn't be the case where we'd be able to simply get an order from a judge to tap the phones of everybody in an apartment building. The way it works is we get a roving wiretap on, say, terrorist A and terrorist A is on a cell phone. If he goes to a different cell phone, that roving wiretap would go with that terrorist to that second cell phone.

Chairman SENSENBRENNER. The gentleman's time has expired.

Without objection, immediately following Mr. Conyers' opening statement, a letter from Sarah W. Clash Drexler, Trial Attorney of the Department of Justice Civil Division, to Elden Rosenthal, an attorney in Portland, Oregon, relating to the Brandon Mayfield case will be inserted.

The gentleman from Florida, Mr. Feeney?

Mr. FEENEY. Thank you, Mr. Chairman, and thank you, General Gonzales. Like yourself and a lot of proponents of the PATRIOT Act as well as a lot of the critics and people that have voiced concerns, I'm interested in finding the appropriate balance between civil liberties and between protecting ourself against this enormous threat from terrorism, which is very real indeed.

I note that, amongst other things, that the Constitution is often not absolute when it comes to civil liberties. For example, the prohibition against certain searches and seizures is based on reasonableness, according to the Founders. What that means to me is that whether a search or a seizure is reasonable or unreasonable may depend on the threat at any given time, so that it may not be an absolute bar. I think the Founders invited us to change that bar based on the threat to the United States and, of course, habeas corpus can be suspended amongst other times, so certainly under article I, during periods of emergency, the Congress has the right to suspend habeas.

The other thing that I note here is there are not a lot of legal precedents. So you've been referring to arguments by the ACLU. We've got different lower court decisions recently. But the last time we were attacked by a hostile foreign power successfully on the continental U.S. was 1812. There hasn't been a lot of litigation since 1812 on what the Government can or can't do in this regard.

We did have a Civil War within our shores from 1860 to 1865. Chief Justice Rehnquist has written a very important book about 15 years before the terrorist attack called All the Laws But One after Lincoln's quote when he suspended habeas corpus and was criticized for doing so and he said, "Am I to suffer basically the loss of the Union and all of our laws as we defend one law, that being habeas?"

And I guess in that historical light, since we don't have a lot of recent precedents on how to do this balance, I'd like to ask you with respect to American citizens who are suspected under the PATRIOT Act or other provisions of law of engaging in war on terror whether you can compare them to, say, a rebellious Confederate soldier. Lincoln thought that States per se didn't have the right to secede. He treated individual soldiers, at least at the beginning of the war, as individual criminals. But he didn't give them any of the normal due process that we would expect criminals. When he captured somebody from Lee's army, he treated them as a prisoner of war. So there's that question, and to ask you whether that has any precedential value.

Lincoln's suspension of habeas corpus, of course, there were, among other things, railroads being torn apart in Maryland by sympathizers with the Southern rebellion and there were Union troops that were attacked on the way. Habeas was suspended. That was just one of several cases.

And finally, as you deal with whether the Civil War and some of the other historical episodes in our history where we have had to cut back on normally anticipated and expected civil liberties, finally, I'd like to congratulate you, because there's two things that we can with some comfort say after September 11. One is that there have been no other successful attacks, and while it's true, as you said, you can't prove a negative, that but for the PATRIOT Act, we would have been attacked successfully, we can note that our enemies have made clear they want to attack us and they have been unsuccessful since September 11. And as you say, to my knowledge, there has been no proven civil liberty abuse under the PATRIOT Act, even though people are invited to bring civil actions under certain cases if they feel like they've been.

So I guess I'm interested in an historical aspect here because we really have a huge dearth of constitutional precedents dealing with how this pendulum swings, civil liberties versus protecting us from foreign threats.

Attorney General GONZALES. Congressman, I'm not sure how to answer that question. One point that I would want to emphasize is that I don't view this, the PATRIOT Act or certain actions by this Government, as reflecting a decision that protecting our country is okay at the expense of civil liberties. I think we can have both. I think we need to have both, quite frankly. I think we need

to protect our country. We need to protect our civil liberties. I think that's very, very important.

I think the PATRIOT Act is an example of the Congress and the President coming together and trying to achieve that balance, because we all understand—there are reasons these safeguards are in here. Even after the—six weeks after the most horrific attack on this country, people still wanted to have safeguards because Members of Congress and the President understood that civil liberties, the protection of civil liberties, was equally important.

And so I think that it would be a mistake to say that, depending on what the circumstances of the moment are, that sometimes civil liberties should be sacrificed in any way in order to protect the security of this country.

Chairman SENSENBRENNER. The gentleman's time has expired.

The gentlewoman from Texas, Ms. Jackson Lee.

Ms. JACKSON LEE. Thank you very much, Mr. Chairman. Allow me on my time a moment of personal privilege to welcome General Gonzales and to recognize that our paths cross as lawyers in the City of Houston, and let me applaud you for your historical family background and the history that you're making on behalf of the American people.

And I might say that my questioning is not personal. I appreciate you very much and I wish your family and you best and well as you proceed in this very important position.

We have spoken on occasion on some issues dealing with civil rights and so I think you have a sense of my concern as we look at the issue of either reauthorizing or making permanent several positions—specific provisions of the PATRIOT One. I think it should be well noted that I supported a PATRIOT Act One legislative initiative as drafted in a bipartisan manner by this same Judiciary Committee. That was not the bill that arrived at the floor of the House and, therefore, I was compelled to stand, I think, more importantly with the Constitution and security by voting against it.

Let me just share very briefly some words that I think are important to note. "Individual liberty is individual power. The nation which enjoys the most freedom must necessarily be in proportion to its numbers the most powerful nation." That's John Quincy Adams.

Another by Samuel Adams notes that "the Constitution should never be construed to authorize Congress to infringe," and then it goes on to say, "on the ability of citizens to redress their grievances or to subject the people to unreasonable searches and seizures of their possessions, papers," or, as I said, possessions.

I say that because we seemingly have conceded to losing our rights because of the horrific act of 9/11. I think we are consistent in this Congress and in this Judiciary Committee to acknowledge, and I think you have acknowledged it, General, along with the President, that our highest responsibility is to secure the Nation and to secure the people of the United States. I don't step away from that responsibility.

I would argue, however, that the tone in which we have proceeded in the legislative initiatives have really done us in, and I say that because your beloved Texas now seems to be under the eye of the new Minutemen, Minutewomen. Border watchers have

eyes on Texas. So because we have either created this atmosphere of fear, because we have either not done our job, we have not protected civil liberties, we have not enforced laws that we already have dealing with border security, we now have men taking up arms and placing themselves on the border, even to the extent that Border Patrol agents have said it may be a dangerous condition. So I'm concerned about the tone.

In addition, before the PATRIOT Act Two was pulled, we even had a potential section 501 that would take away someone's citizenship, which the Supreme Court under Justice Warren said that the 14th amendment protects our citizenship unless we voluntarily give it up.

It is the tone that has been created, and frankly, I don't believe that the PATRIOT Act provisions really have made us safer. I hope that we will vet them at a very high standard as to the standard of how they have denied our civil liberties, how they've created an atmosphere for Guantanamo Bay, and I do not criticize the military that is doing their job. I do criticize the existence of Guantanamo Bay for no reason. I criticize the existence of a determination of enemy combatant, which seemingly has no basis in law.

So I raise these questions with you. One, would you be able to provide for me the numbers of Pakistani who were required to sign up on the registration list in the early part of 2002-2003, the numbers of them? You can't give me names. How many were signed up? How many terrorists were found off of that list? That is my first question, and you obviously may not have that at your fingertips. I'd appreciate your issue on that.

Section 206 is the roving wiretap, and my question to you on that, the value of the roving wiretap. It doesn't seem to have enough restraints in terms of, again, the litmus test of civil liberties.

And my last one is to ask prospectively, because of the tone that's been created, do you think it's viable that we should have as a provision of any PATRIOT Act the removal of one's natural born citizenship that is protected under the 14th amendment? And I thank the gentleman for his concern on these questions.

Attorney General GONZALES. I don't have the information on Pakistan. I'll see what I can learn and see what information can be provided.

On 206, 206 is—allows the use of roving wiretaps in connection with intelligence investigations, and the use of roving wiretaps based on a probable cause standard is something that's been around for many, many years, has been reviewed by the courts, and I do believe does meet constitutional standards.

In terms of removal of citizens, I don't recall the specific provision you're referring to in what was, quote, PATRIOT——

Ms. JACKSON LEE. Section 501.

Attorney General GONZALES.—PATRIOT Two, but I'd be happy to look at it and give you my views about it.

Chairman SENSENBRENNER. The gentlewoman's time has expired.

Ms. JACKSON LEE. I thank you.

Chairman SENSENBRENNER. The gentleman from Texas, Judge Gohmert.

Mr. GOHMERT. Thank you, Mr. Chairman.

General Gonzales, I've been a fan of yours for a long time, going back to my days as a judge and Chief Justice back in Texas. Proud to have you here. Thank you for your testimony.

I want to go quickly into these things. Five minutes goes fast. I was watching about 1 or 2 this morning a replay of some of your testimony yesterday with the FBI Director before the Senate and I wanted to clarify something with regard to section 215 and also 217. You had mentioned there was a lot of concern. Obviously, there is a lot of concern. Under 215, where it discusses that you or your designee may make an application for order and it's of a U.S. person, and it goes on that that would be to a judge of a court or magistrate, specifies that, and then it says if the judge finds the application meets the requirements of this section, then he will grant the warrant.

And I heard a lot of different discussion on different standards of proof and I want to make sure that—and I don't see anything in the section, haven't seen it, which says what is the burden of proof when you go before that judge that's designated and I want to make clear for the record—find out clearly for the record what is that standard you have to prove to that judge or magistrate.

Attorney General GONZALES. Our position is, is that the standard that has to be met is a relevance standard, the same kind of—similar to standards that you would have to show—to meet in connection, say, with a grand jury subpoena.

You are correct that the relevance—that standard is not explicitly mentioned in 215. Our experience is, is that judges have construed 215 to impose a relevance standard. That is a position that we have argued in litigation. It is one of the amendments to 215 that the Department would support because we believe that that is the appropriate standard, to include a specific relevance reference.

Mr. GOHMERT. Also, there's obviously been a lot of concern about the sharing of information, and as you've heard from both sides of the aisle, nobody's meaning this personal to you, but apparently, there was a precedent back in the early 1970's that had a counsel that was abusive enough he had one FBI file, went to prison for it. And then I hear tell there's even been a White House Administration so corrupt they might have even had 1,000 FBI files and didn't have an Attorney General with the wherefore to go ahead and prosecute such a terrible abuse. So you can understand why there'd be some concerns about those things if it's true that you could really have that kind of abuse at the highest levels. I'm not concerned about you or this good President, but you never know. You can have a President like that.

So who gets this information that you glean? Does it, under your interpretation, ever get to the White House?

Attorney General GONZALES. Oh, absolutely not. We're talking about matters relating to prosecution. Certainly when I was in the White House and as the White House Counsel, we tried to be very, very clear.

First of all, we tried to certainly limit any communications between the White House and the Department of Justice on any criminal matter. It would have to go through the counsel's office be-

cause we were very, very concerned about in any way of sharing information between the White House and the Department of Justice, and even in communications between the counsel's office and the Department of Justice, we were also very, very careful about the information and the kinds of questions we would ask about a particular case.

No, believe me, we understand how sensitive this information is and we took great care to ensure that we didn't get access, and the Department was very good in ensuring that the White House did not get access to very sensitive information.

Mr. GOHMERT. And just so you know, there are those of us who do not criticize an Attorney General or a Department of Justice that if they need information about Iraq, they question people that have knowledge about Iraq and don't go to New Zealand to ask a farmer just so they don't look like they're profiling.

But I want to ask you also, do you feel like there ought to be a criminal code with regard to violations of national security? Do we need that?

Attorney General GONZALES. Congressman, I don't know whether or not we need it or not, quite frankly. I think that our current laws seem to be working well, but obviously, if you're serious about it, I'd be happy to think about it.

Mr. GOHMERT. Well, thank you. I wish you would. And I am in favor of a sunset provision. Thank you very much, Mr. Chairman.

Chairman SENSENBRENNER. Thank you.

The gentlewoman from California, Ms. Lofgren.

Ms. LOFGREN. Thank you, Mr. Chairman, and I am glad that we are having this hearing. I have felt for the past several years that we should have had some oversight in a formal sense in the Committee. And I think back to those days after 9/11 and the Committee really did work closely together, and I remember over the weekend in this very room personally being here and working on the drafts before the Committee with Viet Din and others who were—and we had a unanimous vote, I believe, out of this Committee.

Key to that was a sunset to make sure that we hadn't made a mistake, and I think I'm going to want a continued sunset just so it forces the Committee to review how this is going.

Along those lines, and you've mentioned in answer to others that things are in litigation. I know that there's been times that the Committee hasn't received information because of security concerns. Every Member of the Committee has signed an oath and we are authorized to receive classified information in rooms that are here in the Capitol where you leave all your beepers outside. I'm hopeful that we can get the information you cannot give in a public session in a secure site so that we can fully understand what's going on here so that we can do our job.

I have a couple of questions on specific elements of the Act. You mentioned 215. I'll tell you, I don't think any of us had in mind libraries and bookstores when that provision was put together, and you say it's never been used with a library or a bookstore, and I'm wondering whether the Department would support an effort to specify that personally identifiable information in bookstores or libraries would be excluded from section 215.

I'm also interested in section 218. I want to know how many terrorism prosecutions have actually resulted from that section. If you don't have it today, I'd like it later. I just want to know the volume. How many have been issued and how many prosecutions for terrorism-related activities have occurred?

And then I also—five minutes is not enough to get all our questions done, but I do have a general concern about—well, many things, but also habeas corpus. The very initial draft of the first PATRIOT Act sent over from the Department had a provision to suspend habeas corpus. As we know, in article I, section 9, suspension of habeas corpus is a power reserved to the legislative branch. It never really made it to print, but we're not going to suspend habeas corpus. But, I'm concerned that in a back door sort of way, we've ended up with that result.

And one of the questions that's not in the PATRIOT Act itself, but it's part of the general effort on terrorism abatement, is the use of witness provisions, material witness statutes. The last update I've been able to find is from 2003, where the statute had been used supposedly 50 times. I don't know what's happened since that time, but here's the concern that's been raised in the press, that the material witness statute has been used but that it hasn't been used to produce testimony. So I'd like to know how many times this has been used in the Department's efforts to combat terrorism and how many of those individuals actually ended up testifying, because I do think that that is an issue relative to due process.

I'm hopeful that we will have a number of hearings. I haven't had a chance to ask the Chairman yet, but I'm wondering if you could address the three questions that I've asked.

Attorney General GONZALES. As to 215, whether or not I could support a provision that would exempt from the reach of 215 personal information from libraries and bookstores?

Ms. LOFGREN. Personally identifiable information from libraries, bookstores, and I think also medical records.

Attorney General GONZALES. Okay. I have said before—I mean, the Department has no interest in rummaging around and learning about people's personal library habits and looking at their medical records. We are concerned about making sure we have information about people who use libraries to plot for purposes of engaging in some kind of terrorist activity.

We know that, certainly in the criminal context, libraries have been used and there have been investigations, there have been subpoenas of library records in the criminal context, and we've had convictions——

Ms. LOFGREN. Well——

Attorney General GONZALES.—and my own judgment, Congresswoman, is that we should not allow libraries to become safe harbors for terrorists.

Ms. LOFGREN. If I may——

Chairman SENSENBRENNER. The time of the gentlewoman has expired.

Ms. LOFGREN. I'll give a follow-up question to you.

Chairman SENSENBRENNER. The gentleman from Indiana, Mr. Hostettler?

Mr. HOSTETTLER. Thank you, Mr. Chairman, and thank you, General Gonzales, for being here, and congratulations on your appointment and thank you for your willingness to take on such a tough job. I, like many of my colleagues, have received numerous questions since passage of the PATRIOT Act and my support of the PATRIOT Act regarding section 213. I would like to read to you the fourth amendment to the Constitution, and I have a question for you afterwards.

Quote, "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures should not be violated and no warrants shall issue but upon probable cause supported by oath or affirmation and particularly describing the place to be searched and the persons or things to be seized," end quote.

I don't see in the fourth amendment to the Constitution a requirement for prior notification. Do you see that in the fourth amendment——

Attorney General GONZALES. No, and——

Mr. HOSTETTLER.—in the text of the fourth amendment?

Attorney General GONZALES.—and I believe the Supreme Court in a case called, I think, *Dowdia v. United States,* has indicated that the fourth amendment does not require that notice be given when the warrant is executed, that it is constitutionally permissible to execute the warrant and to provide notice after the fact.

Mr. HOSTETTLER. And, in fact, even though I'm not suggesting that we do this, but the text of the amendment itself does not even require for any notification whatsoever, be it prior or delayed notification, the text of the amendment.

Attorney General GONZALES. Well, I presume your reading is correct and there does not appear to be a requirement for notice, but obviously we do give notice, and even in the connection of section 213, notice is given in every case.

Mr. HOSTETTLER. Thank you. I have a question also about section 215. You, I believe, stated in your oral testimony that a recipient of a section 215 order is allowed—can be allowed to challenge that order prior to its execution. Did I hear that correctly?

Attorney General GONZALES. It is our position that under 215, a recipient could challenge that order——

Mr. HOSTETTLER. Prior to its execution? Prior to the order being executed?

Attorney General GONZALES. And someone—if information is received, we believe that a person could seek to have that evidence or information suppressed in a subsequent proceeding. But yes, you do have the opportunity to challenge the execution of that order, in our judgment. We understand that 215 does not make that explicitly clear and we are prepared to support an amendment that would make that clear.

Mr. HOSTETTLER. Would there be a situation that you can foresee where that would be harmful to the investigation and potentially, therefore, the national security, if that process was allowed to be challenged prior to the execution?

Attorney General GONZALES. I suppose that it could be. Obviously, we would do work as quickly as we could to make sure that

that issue was heard and resolved by a judge as quickly as possible.

Mr. HOSTETTLER. Thank you very much. I yield back the balance of my time.

Chairman SENSENBRENNER. The gentleman from Virginia, Mr. Scott.

Mr. SCOTT. Thank you. Thank you, Mr. Chairman.

Mr. Gonzales, we've heard—in talking about FISA—you keep talking about terrorism. FISA is not limited to terrorism or even criminal activity, is it? General intelligence, foreign intelligence——

Attorney General GONZALES. Sure, yes.

Mr. SCOTT.—a trade deal, spying on people. So we're not necessarily talking about crimes.

Attorney General GONZALES. That is correct.

Mr. SCOTT. Is a roving wiretap limited to terrorism?

Attorney General GONZALES. Umm——

Mr. SCOTT. I mean, if you get a warrant——

Attorney General GONZALES. No. No. No. A roving wiretap is not limited to terrorism.

Mr. SCOTT. Not even——

Attorney General GONZALES. Roving wiretaps have been used in the criminal context for many, many years.

Mr. SCOTT. But if you get a FISA wiretap, you don't even have to start off with a crime, just foreign intelligence.

Attorney General GONZALES. Yes, that's correct.

Mr. SCOTT. You can get a roving wiretap, no crime even involved.

Attorney General GONZALES. But again, let me emphasize that this is not an authority that's used in the sole discretion of the Government. We do have to go to a Federal judge——

Mr. SCOTT. Okay. Well——

Attorney General GONZALES.—establish probable cause——

Mr. SCOTT. Probable cause of what?

Attorney General GONZALES. Establish probable cause that the target is either a foreign power or an agent of a foreign power and probable cause with respect to the location or facility that the target is either about to use or is using a certain telephone facility.

Mr. SCOTT. I didn't hear you say a crime is about to be committed because that's not part of a roving wiretap, and the probable cause, most people think you're talking about probable cause of a crime. That's not what you're talking about, is it? No.

Now, are you willing to limit this power to terrorism?

Attorney General GONZALES. Am I willing to limit section 206 to terrorism?

Mr. SCOTT. Right.

Attorney General GONZALES. Mr. Scott, I would have to look at that, and I'd be happy to consider that, but again, I do believe that this is an important tool——

Mr. SCOTT. Okay, but——

Attorney General GONZALES.—in dealing with the war on terrorism——

Mr. SCOTT. You keep talking about terrorism, and let's limit it to terrorism. We already ascertained that some of this, no crime is even implicated because you're talking about foreign intelligence.

Let me ask you another question on the roving wiretap. We had some discussion when we passed that thing that you ought to ascertain that the target is actually in the house where the phone is before you start listening to it. You can put these taps all over the place—cell phone, home phone, pay phone on the street corner if they use the phones. Shouldn't we require that you ascertain that the target is actually the one using the phone before you can start listening in?

Attorney General GONZALES. There is no ascertainment requirement even in the criminal context with respect to wire and electronic communications. There is an ascertainment requirement with respect to oral communications, such as bugging.

Mr. SCOTT. Should we put that in the bill, that if you're going to wiretap a person, you ought to ascertain that it's actually the person you're listening to, particularly because it may not be his home phone? It may be his next door neighbor's home phone if you know he keeps using that phone.

Attorney General GONZALES. Well, I think that the statute is written in such a way that you have to have probable cause that, in fact, the target——

Mr. SCOTT. You've got probable——

Attorney General GONZALES.—is using or about to use a particular phone.

Mr. SCOTT. And so you should—so there is implicated an ascertainment requirement that you've got to ascertain that the target is actually in the next-door neighbor's house before you start listening to the next door neighbor's phone.

Attorney General GONZALES. It's my understanding that under 206, you have to first identify a target and you cannot go up on a roving wiretap unless the target is either using or about to use the phone.

Mr. SCOTT. And so you wouldn't be offended with an ascertainment requirement.

On the——

Attorney General GONZALES. I would have to look at that, Mr. Scott.

Mr. SCOTT. Okay. We went to great lengths to change the law on foreign intelligence to suggest that you can get one of these warrants—it used to be if the purpose of the warrant was foreign intelligence, now if it's a substantial objective, not the primary objective. If the purpose of the warrant—of getting a FISA wiretap is something other than foreign intelligence, what is it? What are the other excuses for getting the FISA wiretap?

Attorney General GONZALES. If it's other than foreign intelligence?

Mr. SCOTT. Right.

Attorney General GONZALES. You mean——

Mr. SCOTT. The primary purpose is something other than foreign intelligence.

Attorney General GONZALES. Criminal activity.

Mr. SCOTT. You mean criminal activity without probable cause, without having to go through the rigamarol of getting a probable cause warrant?

Attorney General GONZALES. Mr. Scott, I would want to study this and get back to you on this.

Chairman SENSENBRENNER. The time of the gentleman has expired.

The gentleman from North Carolina, Mr. Coble.

Mr. COBLE. Thank you, Mr. Chairman.

General, several months ago, a constituent came to me and he said, "We've got to get rid of this PATRIOT Act. It has the trappings of creating a crisis in this country." I said, "Well, give me an example where it has adversely affected you." He said, "I can't do it." I said, "Well, give me an example of where it's adversely affected anyone you know or anyone you've heard about." "Can't do it." I said, "Well, you're not helping me any."

General, I fear this exchange between my constituent and me typifies widespread misunderstanding about the PATRIOT Act, that many people have heard how onerous and how bad it is, but they can't give you examples where they've been adversely affected. I think that applies to 213. I'm glad you mentioned 213 because I've talked to many people who believe that delayed notification of a search warrant was born when the PATRIOT Act was enacted, and, of course, it was available long before then, as you pointed out. Of course, that's not subject to being sunsetted.

Let me shift gears to the library situation. Some folks have referred to it as the "angry librarians' provision," and I'm not sure that's accurate. I don't know that the librarians are angry, but I think they're perplexed, probably, and perhaps because of misunderstanding, because I'm told, and I think you may have alluded to this this afternoon, I don't think any inquiries have been leveled against libraries, is that correct, under the PATRIOT Act?

Attorney General GONZALES. We have not exercised the authorities under section 215 for library records. Let me make one thing clear, because I want to be obviously forthcoming with the Committee. There have been library records produced to the FBI for purposes of a foreign intelligence investigation. We've gone forward to librarians. In some cases, the libraries have come to us concerned about the library habits of some of their customers and they have shared information with us voluntarily.

So I don't want to leave the Committee the impression that there hasn't been some exchange of library information with the FBI, but it is true that section 215—that authority under section 215 has not been used to obtain library records.

Mr. COBLE. All right. Let me ask you this, Mr. Attorney General. If the information can be obtained with a grand jury subpoena, which it can be done, that does not require a court order, why would the Department of Justice want to use a FISA order that requires a court order and limits the type of information that the Department can obtain?

Attorney General GONZALES. It may involve a very, very sensitive investigation where we may not want to jeopardize the source or the investigation itself, and therefore, we feel more comfortable pursuing a 215 order rather than a grand jury subpoena.

Mr. COBLE. Permit me to revisit the *Mayfield* case, and I realize there's litigation here and you're probably restricted as to how much you can say about that, but is it not true that the Attorney

General is currently investigating whether or not PATRIOT Act authorities were abused in the case? I'm told that it is ongoing.

Attorney General GONZALES. It is and has been looked at and is being looked at. I don't know if that review is complete, yes, by the Department.

Mr. COBLE. And finally, Mr. Attorney General, to follow up on Mr. Scott's questioning regarding the roving wiretaps, are there not two separate entities, that is to say, a roving wiretap for intelligence matters, on the one hand, and then a roving wiretap for criminal matters on the other, is that not correct?

Attorney General GONZALES. Section 206 deals with roving surveillance under FISA. There is authority—other authorities that govern the use of roving authorities in criminal matters.

Mr. COBLE. Well, I want to reiterate what you said earlier about the importance of preserving our civil liberties while at the same token arming ourselves against would-be terrorists, and I, not unlike you, I believe we can do both. And I don't know you, Mr. Attorney General, but I like you. I like your style. Good to have you up here.

Mr. Chairman, I beat the red light.

Chairman SENSENBRENNER. And now the other gentleman from North Carolina, Mr. Watt.

Mr. WATT. Thank you, Mr. Chairman, and first, let me apologize to General Gonzales for not being present to actually hear his testimony. Unfortunately, I have two hearings going on at the same time and I was trying to save CDBG and deal with the PATRIOT Act at the same time.

I got a briefing from my staff to try to avoid territory that had been covered by other Members of the Committee, so I want to zero in on one thing in which I was involved during the Committee's consideration of the PATRIOT Act and that's the Privacy and Civil Liberties Oversight Board. You're familiar with the provisions in the law that talk about that?

Attorney General GONZALES. I believe I am, Congressman.

Mr. WATT. Okay. All right. I'll just read, because I was interested to know what had transpired about the privacy oversight because privacy was obviously a major issue that we were confronting when we were trying to deal with this piece of legislation. So I got the Congressional Research Service to pull up—send us a report, and here's what it says.

It says the Conference Committee version of the intelligence reform legislation retained the mandate for a Privacy and Civil Liberties Oversight Board. While the board would have most of the review and advice responsibilities contained in the Senate-adopted version of the legislation, it would not have subpoena power, but was authorized to request the assistance of the Attorney General in obtaining desired information from persons other than Federal departments and agencies. Now, this is the intelligence reform bill that got passed and that they are giving me the update on.

It goes on to say that no nominations to membership positions on the Privacy and Civil Liberties Oversight Board were made in the early weeks of the 109th Congress and the President's fiscal year 2006 budget contained no request for funds for the panel.

Now, my question to you is, if—obviously Congress decided this Privacy Oversight Review Board was an important ingredient. You've superimposed this intelligence reform stuff on top of the PATRIOT Act. First of all—two questions. First of all, do you think it's important to have a Privacy Review Board——

Attorney General GONZALES. I think it is important that we review the actions of the Government to ensure that the privacy rights of Americans are protected.

Mr. WATT. Okay. Well, at least we are together at that point.

Second question, how could we extend the sunsetted provisions of the PATRIOT Act if the Congress having mandated—this says it was a mandate to create this board, and the President not having made any nominations to this board and not proposed any money to fund the operations of the board. I mean, it seems to me that that would be directly contrary to the wishes of the Congress.

Attorney General GONZALES. Well, I can assure you, Congressman, that the protection of the privacy rights and the civil liberties of all Americans is a priority for our President. I don't—not being in the White House, I don't know about the discussions or decisions regarding the budget. I do know—my latest information, it may be stale now, but my latest information is that the White House is in the process of identifying people to place on the board.

But in the interim, as you know, the President did sign an Executive Order creating a Privacy Board which——

Mr. WATT. No, he didn't create a Privacy Board. He created a Privacy Officer and he did that actually before we—the intelligence reform bill went through and we mandated for that purpose—Congress mandated for that purpose a board that was to be staffed, not an officer inside some department.

Attorney General GONZALES. Respectfully, Congressman, it is a board chaired by the Deputy Attorney General and includes representatives from various agencies——

Mr. WATT. All insiders.

Chairman SENSENBRENNER. The time of the gentleman has expired.

The gentleman from Arizona, Mr. Flake?

Mr. FLAKE. Thank you, Mr. Chairman, and thank you, General Gonzales.

Let me just try to bring this to the real world for a minute here with a real world scenario and see if we're on the same page here. You may be familiar with one of the Fox News analysts, Andrew Napolitano, who wrote an op-ed a while ago, and let me just read a portion of it and get your response to it.

Quote, "The Government can now, for the first time in American history, without obtaining the approval of a court, read a person's mail and prosecute a person on the basis of what is in the mail." Is that an accurate reflection of the law?

Attorney General GONZALES. I'm not—I don't believe it is an accurate reflection of the law. Again, if we're talking about the exercise of authorities under the PATRIOT Act, in most cases, it does involve the Department going to a Federal judge and getting permission to use those authorities.

Mr. FLAKE. I understand in most cases, but is that possible now for the first time in history, without obtaining the approval of a

court, to read a person's mail and then prosecute the person on the basis of what is in that mail?

Attorney General GONZALES. That sounds to me like it would be a search and I think that you would need probable cause to do that. You would need a warrant to do that and you'd have to go to a Federal judge in most cases, except, I think, in very rare circumstances, if in the event of an emergency, but even then, you'd have to go to a judge after the fact and explain what you've done. So I don't think that what he has said is accurate.

Mr. FLAKE. But it would be accurate if you say in certain cases, you would have to go to the judge after the fact——

Attorney General GONZALES. But those are very rare and extraordinary circumstances, and so——

Mr. FLAKE. How many of those circumstances have we had?

Attorney General GONZALES. I'm not aware of any.

Mr. FLAKE. None?

Attorney General GONZALES. I'm not aware of any.

Mr. FLAKE. If there are some, could you get back to my office with that information?

Attorney General GONZALES. I can certainly look into it.

Mr. FLAKE. Thank you. I appreciate that. There's a lot of talk about a wall between intelligence and law enforcement that the PATRIOT Act helped eliminate. Is it possible that that talk of this wall has been exaggerated. Let me just read a statement from Judge Royce Lamberth and then get your reaction.

"The FISA court has long approved, under controlled circumstances, the sharing of FISA information with criminal prosecutors as well as consultations between intelligence and criminal investigations where FISA surveillances and searches have been conducted." Is that the case? Do you dispute that statement?

Attorney General GONZALES. I think that in actual practice, it's been the case that law enforcement—before the PATRIOT Act, there was a reluctance amongst the law enforcement community and the Intelligence Community about sharing of information and that law enforcement personnel were concerned that if they shared too much information—if too much information was shared with intelligence, the Intelligence Community, it might jeopardize a prosecution. And so people were being very careful and there was a reluctance to share information, and I think after the PATRIOT Act, that reluctance has gone away.

Mr. FLAKE. So the wall was more a function of a culture that existed than——

Attorney General GONZALES. Well, there certainly was a culture that existed. Rightly or wrongly, I think people wanted to be very, very careful because people in—most people in Government really do—are concerned about doing the right thing and not doing things that in any way infringe upon the civil liberties of ordinary Americans. And so, you know, I certainly wouldn't characterize it, I mean, as a—I think people were just doing what they thought was the right thing to do.

Mr. FLAKE. Now they're less reluctant to infringe, or——

Attorney General GONZALES. Well, now they know. They've been given clear guidance that this is appropriate conduct and it is lawful conduct.

Mr. FLAKE. With regard to delayed notification, what is the longest period of time now that a person can be under surveillance without their knowledge?

Attorney General GONZALES. My understanding is that there have been six cases where the judge has said—has not imposed a time to provide notice that it had been an ongoing investigation. The judge has said, well, we'll see how the investigation proceeds. So there have been six such cases. You put those aside, I think the longest time period has been 120 or—it's been 180 days.

Mr. FLAKE. A hundred-and-eighty-days?

Attorney General GONZALES. Yes.

Mr. FLAKE. But in those six cases, it's fair to assume that some of those investigations may still be going on or they're ongoing?

Attorney General GONZALES. I don't know. That may be, in fact, be the case, but I'm not sure.

Mr. FLAKE. Very quickly, before my time runs out, let me just be clear about the Justice Department's preference or position, I guess, on sunsets. I want to commend the Chairman for insisting on the sunset. I think to the extent that we've been careful and circumspect, it's largely as a result of the sunset provision. Are you saying that the Justice Department wants to do away with the sunset provision?

Attorney General GONZALES. I don't know whether or not the sunsets are necessary. I fully trust Congress to perform its oversight functions. I hope Congress doesn't need the sunset provisions in order to perform its oversight functions. The sunsets were put in there initially because of the fact that people were concerned that decisions had been reached quickly about the bill. We now have a history of three-and-a-half years, and so my view is that Congress has all the authority it needs to perform the oversight necessary in the way that this Department exercises the authorities under the PATRIOT Act.

Chairman SENSENBRENNER. And the time of the gentleman is expired, and to paraphrase President Reagan, you trust and we verify.

The gentleman from Massachusetts, Mr. Delahunt.

Mr. DELAHUNT. Yes. I thank the Chairman and I welcome General Gonzales and I welcome your words.

To segue the gentleman from Arizona, Mr. Flake, you referenced you have confidence in Congress to exercise its oversight responsibilities and functions in our constitutional order, but I share the same concern that my colleague to my left, Mr. Schiff, articulated earlier to you about the lack of cooperation during the course of the past 4 years in terms of providing that information to Members of Congress so that we can exercise our oversight. So I would suggest that when we talk about sunsets, sunsets have played a very, I think, important role because now we seem to be engaged hopefully in a new way.

I've had my own experience. I served on the—as an adjunct, if you will, on the Government Reform Committee during its inquiry into the conduct of some individuals in the office of the Boston FBI and it was only under threat of subpoena that we were able to secure a prosecutorial memorandum that dated back some 40 years

that had nothing in there whatsoever that could be interpreted to be endangering of national security.

So I really hope that we are moving, and I listened to your words and I respect those words, but I hope we're moving in a different direction in terms of the relationship between this branch, this Committee, and the Department of Justice.

You know, I think it's critical in a viable democracy to emphasize that the concerns of a citizen to their privacy are absolutely essential, and at the same time that as much transparency as possible is important in terms of the confidence of the American people in its Government, in the integrity of its Government. It's a balancing act, and I understand that.

But myself and Mr. Berman filed legislation today. He alluded to it earlier in his question to you about the issue of data mining. It's a concept that I'm sure you're familiar with where there's a broad search of both public and non-public databases without a particularized need being articulated to discern whether there are patterns that may implicate some sort of terrorist cabal. He and I, as part of a bill that, with the support of the Chairman, came out of Committee, didn't go anywhere when it got further along the legislative process, but that would have required each head of a Federal agency to report to Congress about their initiatives regarding data mining.

The American people are concerned about privacy. I would suggest that this is something that I hope you would review carefully and support if we are going to have the kind of relationship between the branches, and specifically this Committee, that you have expressed and others have expressed.

I don't know if you're familiar with that particular provision, but if you have any comments, I'd like to hear them.

Attorney General GONZALES. I look forward to reading your legislation. I can say that I, like other Americans, would be very concerned about this issue. I think protection of privacy rights are very, very important, and rather than comment any further, I'll read the legislation and be happy to talk to you about it.

Mr. DELAHUNT. I look forward to hearing from you. I'd make one final observation, is that, you know, when we see that there are 14 million new papers that have been classified, 25 percent over the previous year according to the latest reports, I just want to let you know that I think many of us, and I think on both sides of the aisle, are very concerned about what's happening as far as a culture of concealment, if you will, and secrecy in Government that's got to be addressed.

Attorney General GONZALES. Thank you, Congressman.

Chairman SENSENBRENNER. The gentleman yields back.

The gentleman from Virginia, Mr. Goodlatte.

Mr. GOODLATTE. Thank you, Mr. Chairman. Thank you for holding this hearing.

General Gonzales, welcome, and thank you for the fast start you've gotten as our new Attorney General and thank you for coming to speak with us today.

I'd like to call your attention to a couple of other issue areas that very much relate to our security but are not directly on the PATRIOT Act. I would like to follow up on the topic that the gen-

tleman from Texas, Mr. Smith, addressed earlier, and that is immigration. I have legislation in the Congress to address a problem that was identified by the State Department last year with regard to the Visa Diversity Program, or also called the Visa Lottery Program, whereby individuals are given not just a visitor's visa, but permanent resident status in the United States not based upon any particular job skill, not based upon having any close family relationship with anybody, but simply by having a little bit of information put into a computer. Millions of people around the world do this, and then 50,000 are drawn out every year, the lucky winners, and receive green cards to come to the United States.

Last year, the State Department's Inspector General testified before the Immigration Subcommittee that the Visa Lottery Program posed a significant risk that hostile intelligence officers and terrorists, especially those with no previous criminal backgrounds, could apply for the lottery and be awarded permanent resident status, and I wonder if the Department of Justice has conducted any analysis on the threat posed by this program. Have you or anybody else at the Department examined this report from the State Department?

Attorney General GONZALES. I'm not aware of any examination, Congressman, but I'd be happy to look at it. It sounds—it concerns me, so I'd be happy to look at it and get back to you.

Mr. GOODLATTE. That would be very helpful and I would appreciate that.

Now, the other area that I'm concerned about is in the area of piracy, particularly intellectual property theft, which is increasingly viewed as being something that's being used by various subversive organizations, including terrorist organizations, as a fundraising mechanism to fund their operations. As author of the "No Electronic Theft Act, or NET Act," and other legislation dealing with piracy, and as co-chair of the Congressional International Anti-Piracy Caucus, I'd like to first commend the Department of Justice for its work in setting up the Intellectual Property Task Force. This has, frankly, been long overdue.

For years, we've had legislation on the books to enforce these laws, but not enough priority was made for it. That was done last year. Other efforts have been made by the Department, as well, to combat intellectual property theft. Projects like Operation Fast Link is a promising example of how our Government can work internationally to ensure that the messages sent are that intelligence piracy is a serious crime, and I'm wondering what your intentions are as the new head of the Department. Is that leadership going to continue in the effort to investigate and prosecute these types of intellectual property crimes?

Attorney General GONZALES. Absolutely. It will remain a priority for the Department. In fact, I'm going out to, I believe, California perhaps later this month to talk about this issue to some of the groups out there. We realize that it remains a problem. It is a vehicle to finance potential terrorism activities and so, yes, very much so a priority. We continue to consider the work of the Intellectual Property Task Force as very, very important.

Mr. GOODLATTE. Good. Thank you very much. The last area I'd like to address is the problem that we're seeing all across the coun-

try. It's particularly a very serious problem in my district. Our United States Attorney for the Western District of Virginia, John Brantley, briefed Senator Warner and I last week on the problem with methamphetamines. This seems to be a particularly great problem in rural areas all across the country. The Shenandoah Valley has been particularly hard hit.

It's a problem that entails being able to get hold of various basic household commodities and make some very dangerous drugs from them. I'm not sure that people realize that they're injecting Drano and battery acid and phosphine gas, some of the things that go into making methamphetamines, when they inject this, but it is a serious problem in rural areas and I'm wondering, is the Department under your leadership committed to meeting the increased need for law enforcement efforts because of the prevalence of this particular type of illegal drug activity in rural parts of America?

Attorney General GONZALES. Absolutely, yes. Just in my 2 months as Attorney General, in my visits with law enforcement, I have been struck by how often I've been told how serious this problem is all across the country.

Chairman SENSENBRENNER. The gentleman's time has expired.

The gentleman from New York, Mr. Weiner.

Mr. WEINER. Thank you, General. Welcome, and thank you for taking so much of your time.

I hope you recognize by this point in the hearings, both in the other body and here, what the fundamental problem is that you face with Congress now, is that, in essence, what the PATRIOT Act reflected was a desire on the part of the Administration of greater authority, and you essentially said to Members of Congress like myself, trust us that we're going to use it wisely, that we're going to use it with discretion, we're going to use it with restraint. And that is why, when you say, well, why do you need something like delayed notification, well, you have to trust us and trust the judge because, frankly, the individual that is being—that the search is over is not going to know and be able to fight to defend their own rights.

And where you've lost so many of us, including people like myself who have been eager, as a New Yorker and someone who considers himself as a moderate on law enforcement things, is this cloak of secrecy that has dominated the discussion over the last 4 years. Obviously, a rise in FISA activity and yet there's less information than there has perhaps ever been. Reports of secret arrests and detentions without charges. What it does is it makes us, who were happy about a sunset, completely unwilling to say either, first of all, extend them, or even further, to eliminate the sunset altogether.

And then you compound it with other actions in other parts of the Justice Department that completely run counter to real efforts to fight terrorism—the virtual elimination of the COPS program, for example. Your predecessor sat in that chair and said what a great program it was. The President of the United States praised the program, and yet the Justice Department has virtually eliminated it. Homeland security starts at home. Not in this Administration. The COPS program hiring component has all but been eliminated, literally taking cops off the streets.

So that what Members like myself and Mr. Delahunt and Mr. Schiff and folks on the other side of the aisle are speaking to is this notion that you made a compact. Give us more authority and entrust us to use it wisely. In order for that compact to be successful, in order to get us to say, okay, we agree 4 years later that that has been the case, there has to be more information.

And what has this attitude on the part of the Justice Department brought? Well, it's brought on one side you saying, well, people are creating phantoms of lost liberty, and I think some on the left have said, well, there's enormous intrusions on our lives. Only with more full disclosure to Congress, only with a more full debate that goes on between you and the American public is this going to happen. And frankly, that hasn't happened.

You have exaggerated its value. I believe many on the left have exaggerated the harm it's caused. But fundamentally, you've lost the trust of so many in this Congress. When people like myself and Paul Wellstone of blessed memory vote for the PATRIOT Act, it is because fundamentally we believe it's important to make things safe and we trust those in positions of power to enforce it wisely, and I think you've let us down.

You've let us down because you've let us down in ways that are fundamental and easy to fix. When Congress asks for cooperation, as Mr. Delahunt says, your first reflex shouldn't be no. When there's questions about secret arrests and detentions, you know, frankly, if your concern is about reinforcing the idea that the Justice Department is operating prudently, talk more freely. Have a frank discussion about what's going on in the world. We should not wait until the day of a Senate hearing to find out that there are 35 instances that section 215 was used and 155 times that the sneak-and-peek provisions were used under the PATRIOT Act.

It is that level of information that, frankly, I think might have even helped your side of the argument if they had been released more steadily over the course of the last 4 years. So that, I would argue, is your problem.

Can I ask a question? I want to make sure I understand it. Section 215, the sneak-and-peek provisions that have delayed notifications, if we were to take away those expanded rights, there are no searches that could not happen. It would simply be a question of whether or not a judge was notified first or whether the citizen was notified first, is that right? But both of those cases, you'd still be able to do the investigations?

Attorney General GONZALES. I don't know—you're talking about 213. I don't know whether or not we would be able to continue the investigation. The fact that we would in some cases have to make a hard choice whether or not to try to take possession of, say, contraband in order to prevent it—say drugs, for example—we'd have to make a hard choice between taking a chance and letting the drugs be distributed in order that we could identify all the Members of a very serious drug ring or take possession of the drugs and then jeopardize not knowing who those folks are.

So if 213, the authorities under 213 were eliminated, I think that it could jeopardize some very important investigations.

Chairman SENSENBRENNER. The gentleman's time has expired.

And last but not least, the gentleman from Alabama, Mr. Bachus.

Mr. BACHUS. Thank you.

Mr. Attorney General, I want to address something that you may not have heard too much about, but that's a 1970 explosive permit law. Now, that law, when Homeland Security came into existence and we passed a lot of the new dictates under the laws we're talking about reauthorizing, the ATF started requiring an explosive permit for anyone that worked in the mines that was around explosives. They asked different mine workers to fill out an application to continue to handle these explosives.

Now, I'll give you an example. I had three mine workers in my district that were taken off the job as a result of their applications. Now, let me tell you about one that agreed earlier today to let me use his name. He's Mickey Birchfield. He's worked 15 years in the mines. He's transported employees and explosives for 15 years. About a month or two ago, he filled out one of these applications and he listed that 17 years ago, when he was 18 years old, he had a disorderly conduct misdemeanor and he said, "I think I paid a $50 fine." Well, the ATF checked and didn't find any record of this, so the only way they knew about it is he said, you know, "When I was 18 years old, I got arrested for disorderly conduct."

He has been reassigned off that job to a lower-paying job and he is waiting for the ATF appeal process, and I said 3 weeks ago. It's 3 months ago, and they still haven't acted on that. First of all, they've taken the disorderly conduct thing when he was 18 and taken him off the job.

My question to you is, are you familiar with the ATF and this explosive permitting procedure that they've established, because I have another coal miner that actually was taken off the job and because they didn't have a place for him, he's actually unemployed now. He has actually decided to retire. But do you know, are there any guidelines to how long the ATF can hold these cases, and why—I mean, I just—could you just tell me maybe why, under what rationale they would——

Attorney General GONZALES. I wish I could, Congressman. I don't know. I presume that there are guidelines in place. I'd be happy to go back and look to see what's there and see if we can provide you some additional information about these cases.

Mr. BACHUS. Yes, and you see, that's a real case that is happening today. The reason I bring that up is that you have asked for Homeland Security—you've asked for new powers, new tools to combat terrorism and we've given you these tools and we hope that there are safeguards in place that we won't have what I consider a civil liberty violation against this guy. He's actually been—his pay has been reduced. Two other individuals in the district, one is a result of two DUIs, one in 1975 and one in 1984. He's no longer permitted to work in the mines. As I said, he was a year and a half away from retirement and he was told that this process is taking over a year, so he just retired.

Attorney General GONZALES. Maybe we should have our staffs talk and we'll get some additional information. I'll see what we can find out.

Mr. BACHUS. You know, I guess what aggravates this, when we hear, and you've got questions about this, when we hear that people that are on the Terrorist Watch List can purchase guns and then you get a guy that when he was 18 years old had a disorderly conduct thing and he can't work at his job, it raises all kinds of questions. And I know that what I've been told is the list is overly broad and it has a lot of inaccuracies in it, but, you know, it's being used every day when people try to move around this country.

And it's not just these. It's just one thing after another, like I talked to a group this week, Epileptic Foundation, and you'd be amazed at children with—they have these magnetic devices that are implanted within their body. The——

Chairman SENSENBRENNER. The gentleman's time has expired.

Mr. BACHUS.—what they have to go through when they go through screening at the airport. So they're put aside and sometimes 30, 40 minutes, even though they have a letter saying——

Chairman SENSENBRENNER. The gentleman's time has expired.

The gentleman from Maryland, the late Mr. Van Hollen. [Laughter.]

Mr. VAN HOLLEN. Thank you, Mr. Chairman, and Mr. Attorney General, thank you for your testimony. As one of the newest Members of the Committee, it's, I guess, my privilege to be one of the people batting clean-up at the end here, but thank you for your testimony.

I actually want to pick up on a related issue which has to do with the GAO report that came out recently showing that a number of individuals on the Terrorist Watch List were able to go into gun shops and legally purchase weapons in this country. I just want to pursue that line of questioning for a minute, because as I understand it right now, if you're on the Terrorist Watch List, you're not able to board an aircraft. You're able to be detained at the airport and not allowed to board an aircraft, is that right?

Attorney General GONZALES. That is correct.

Mr. VAN HOLLEN. And the purpose of that, I assume, is to protect the public safety, is that right?

Attorney General GONZALES. That is correct.

Mr. VAN HOLLEN. All right. Does it make sense to you that we stop a person from boarding the airline in order to protect the public safety, that individual can turn around, get in their car, go to the local gun shop and buy 20 semi-automatic assault weapons? Does that make sense to you, Mr. Attorney General?

Attorney General GONZALES. I think that we should be doing everything we can to ensure that people that are, in fact, terrorists, shouldn't have weapons in this country, the truth of the matter is. But unless they are disabled from having a weapon under the statute, there's not much that we can do, other than maybe trying to get them out of the country or find a way to see if there's any kind of disability under the statute that would allow us to deny them a firearm.

And so, again, at the end of the—I mean, we don't want terrorists to have firearms, but at the end of the day, we have to enforce the law. Unless they have a disability under the statute, then they're entitled to a weapon.

Mr. VAN HOLLEN. No, I thank you for that and I understand the law is the law and we have to enforce it. My question really is, would you be willing to work with Congress and do you think it's a good idea to try and change the law where somebody is legitimately on the Terrorist Watch List? I understand there are issues with respect to that, but if someone is determined to have been legitimately put on the Terrorist Watch List, would you not agree—I'm asking whether you would not agree that it doesn't make sense from a public safety point of view to allow that person to go to the gun shop and buy 20 semi-automatic assault weapons.

Attorney General GONZALES. Well, what I can agree is that if you're a terrorist, you shouldn't have a weapon in this country, and so I do agree with you on that.

Mr. VAN HOLLEN. Let me ask you this, Mr. Attorney General. One of the issues that is raised is the quality of the Terrorist Watch List.

Attorney General GONZALES. Right.

Mr. VAN HOLLEN. What mechanism is in place today for an individual whose name has been put on that list to contest whether or not they should be legitimately put on that list? What do you have today to make sure that the quality of that list is actually good and people aren't wrongfully put on that list?

Attorney General GONZALES. That is a good question. I don't know the answer to that, but I'll be happy to get back to you on it.

Mr. VAN HOLLEN. It seems to me that there's been a lot of discussions with respect to the fact that the quality of the list may not be so good and, therefore, we can't necessarily use that to deny people their right to go purchase a handgun, and that's absolutely true, but it seems to me that somebody who's being denied access to an airplane, if they're wrongfully put on that list, it should be very clear to every American citizen who thinks they're wrongfully put on that list what mechanism procedure they have to get their name off.

Attorney General GONZALES. I don't want the Committee to leave with the impression that we have a shabby Terrorist Watch List. Obviously, no one wants that. We all want the best list possible and we work very, very hard to make sure that the list is accurate. We get information from a variety of agencies who are looking at different threats. Say someone is concerned about terrorist financing, and so someone may end up on the Terrorist Watch List because of concerns about their support of terrorist activity—financial support of terrorist activities.

So I say all of that sort of defending the—I mean, there's been a great effort within the Administration to try to make the Terrorist Watch List a valuable tool and one that we can depend on. But it's a difficult issue and I look forward to working with you on possible legislation. I'd be happy to consider it.

Mr. VAN HOLLEN. Thank you, and Mr. Chairman, if I could just close making two points, to the extent that we can depend on it and it's a valuable tool and someone is on there because they pose a risk to public safety, it seems to me that the question of whether they should be allowed to go down to the local gun store and buy 20 handguns or semi-automatic or whatever weapons it may be is

one that we need to change to the extent that they're legitimately on there.

And to the extent they're not legitimately on there, I would very much appreciate an answer to the question about how an American citizen goes about getting their name off it if they think they're wrongfully on it. It seems to me it's obviously a great unfair burden for a citizen to be placed on the Watch List without any mechanism that is familiar to the public for how they go about getting their name off of it.

Attorney General GONZALES. I think the Watch List has been a valuable tool. I think it has been helpful in dealing with a terrorist threat. Obviously, there have been mistakes that have been made, but I look forward to working with you.

Chairman SENSENBRENNER. The time of the gentleman has expired.

General, let me say that I think this was an extremely valuable hearing in kicking off our review of the sunsetted provisions of the PATRIOT Act. You have done well.

Attorney General GONZALES. Thank you.

Chairman SENSENBRENNER. I hope your next invitation to come up here, whenever that may be, as a friendly invitation because these types of exchanges, I think, help clarify the issues, help do away with a lot of the hype that has come about as a result of this law in particular, and we look forward not only to working with you and the Department relative to this legislation, but also in doing oversight which makes you do your job better and the American public have the confidence that you're doing your job better.

Ms. JACKSON LEE. Mr. Chairman——

Mr. CONYERS. Mr. Chairman——

Chairman SENSENBRENNER. So thank you again for coming.

Ms. JACKSON LEE. Mr. Chairman, would you yield for a question?

Mr. CONYERS. Mr. Chairman?

Chairman SENSENBRENNER. The gentleman from Michigan.

Mr. CONYERS. I join in that thankfulness that you were here and have started this routine with us. It's very important. And I'd like unanimous consent to add in after my opening remarks "Seeking the Truth from Justice" from Laura Murphy, former Director of the American Civil Liberties Union.

Chairman SENSENBRENNER. Without objection.

Ms. JACKSON LEE. Mr. Chairman, could you yield for a question, please?

Chairman SENSENBRENNER. The gentlewoman from Texas.

Ms. JACKSON LEE. Thank you, Mr. Chairman. Will the record remain open or will we be able to submit questions for the record? I have a question about Dr. Yaha Ghoul, a thoracic surgeon who is in detention at this point.

Chairman SENSENBRENNER. The record will remain open relative to questions relative to the general oversight of the USA PATRIOT Act. I don't know if the letter the gentlewoman is referring to relates to the USA PATRIOT Act. If so, the record will remain open for that purpose. But on matters related to other than the PATRIOT Act, I think it is best to deal with that issue in another context.

Ms. JACKSON LEE. I thank the Chairman, and I'd like to submit for the record "On Liberty" by John Stuart Mill, 1859. I'd like to submit that into the record.

Chairman SENSENBRENNER. I assume the copyright has expired on that, so without objection.

[The article of Mr. Mill follows in the Appendix]

Chairman SENSENBRENNER. The Committee stands adjourned.

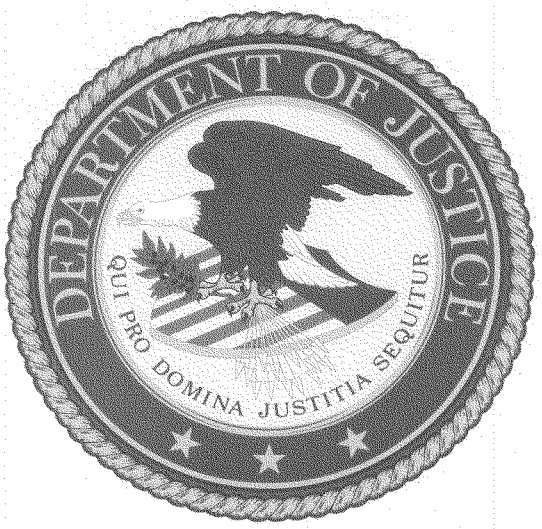
Ms. JACKSON LEE. I thank the Chairman.

[Whereupon, at 3:27 p.m., the Subcommittee was adjourned.]

APPENDIX

Material Submitted for the Hearing Record

USA PATRIOT ACT:
SUNSETS REPORT



APRIL 2005

Introduction:

On October 26, 2001, President Bush signed into law the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act ("USA PATRIOT Act" or "Act"). This legislation, which was passed by both houses of Congress with overwhelming, bipartisan majorities, updated and strengthened laws governing the investigation and prosecution of terrorism within the parameters of our Constitution and our national commitment to the protection of civil rights and civil liberties.

At the end of 2005, sixteen provisions of the USA PATRIOT Act are scheduled to expire: sections 201, 202, 203(b), 203(d), 204, 206, 207, 209, 212, 214, 215, 217, 218, 220, 223, and 225. This report, which was prepared by the Department of Justice at the request of Senator Dianne Feinstein of California, analyzes each of the sixteen provisions. In particular, this report, on a provision-by-provision basis, seeks to: (1) explain how, and the extent to which, these sixteen sections changed the legal landscape, (2) summarize how these sections of the Act have been used by the Department to protect the American people, and (3) survey and analyze any criticisms of the provisions.

In addition to this report, the Department has transmitted many other reports to Congress that provide information explaining in what manner and how frequently the Department has utilized particular USA PATRIOT Act provisions. Most importantly, such information is contained in the semi-annual reports submitted by the Attorney General to the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate regarding the Department's use of the Foreign Intelligence Surveillance Act. Six such reports have been submitted to Congress covering the periods in which USA PATRIOT Act authorities were utilized. These reports were transmitted by the Department in April 2002, January 2003, September 2003, December 2003, September 2004, and December 2004.

Moreover, section 1001 of the USA PATRIOT Act requires the Department's Office of Inspector General to submit to the House and Senate Judiciary Committees on a semi-annual basis a report detailing any abuses of civil rights and civil liberties by Department employees or officials. To date, six such reports have been submitted by the Office of the Inspector General pursuant to section 1001; these reports were transmitted in July 2002, January 2003, July 2003, January 2004, September 2004, and March 2005. Significantly, the Office of the Inspector General to date has not documented in these reports any abuse of civil rights or civil liberties by the Department related to the use of any substantive provision of the USA PATRIOT Act.

As this report demonstrates, some of the sixteen USA PATRIOT Act provisions that are scheduled to sunset are controversial while others have been subject to little criticism. The Department believes that the criticisms of these particular provisions are misguided and that it is vital that all of these provisions be made permanent so that investigators and prosecutors have the tools they need to protect the American people.

The Department hopes that this report will assist Congress and the American people in evaluating each of these provisions as the important debate over renewing these sixteen sections begins.

Section 201: Authority to Intercept Wire, Oral, and Electronic Communications Relating to Terrorism

Text of Section 201:

> Section 2516(1) of title 18, United States Code, is amended --
>
> > (1) by redesignating paragraph (p), as so redesignated by section 434(2) of the Antiterrorism and Effective Death Penalty Act of 1996 (Public Law 104-132; 110 Stat. 1274), as paragraph (r); and
> >
> > (2) by inserting after paragraph (p), as so redesignated by section 201(3) of the Illegal Immigration Reform and Immigrant Responsibility Act of 1996 (division C of Public Law 104-208; 110 Stat. 3009-565), the following new paragraph:
> >
> > "(q) any criminal violation of section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2339A, or 2339B of this title (relating to terrorism); or".

How Current Law Now Reads:

> **"§ 2516. Authorization for interception of wire, oral, or electronic communications**
>
> > **(1)** The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—
> >
> > ...
> >
> > **(q) any criminal violation of section 229 (relating to chemical weapons); or sections 2332, 2332a, 2332b, 2332d, 2332f, 2339A, 2339B, or 2339C of this title (relating to terrorism); or..."**

Analysis:

In the criminal law enforcement context, federal investigators have long been able to obtain court orders to intercept wire communications (voice communications over a phone) and oral communications (voice communications in person) to investigate the predicate offenses listed in federal wiretap statute, 18 U.S.C. § 2516(1). The listed offenses included numerous traditional crimes, including drug crimes, mail fraud, and passport fraud. Prior to the passage of the USA PATRIOT Act, however, certain extremely serious crimes that terrorists are likely to commit – including chemical weapons offenses, killing United States nationals abroad, using weapons of mass destruction, and providing material support to foreign terrorist organizations – were not

listed in 18 U.S.C. § 2516(1). This prevented law enforcement authorities from using many forms of electronic surveillance to investigate these serious criminal offenses. As a result, law enforcement therefore could obtain under appropriate circumstances, a court order to intercept phone communications in a passport fraud investigation but not a chemical weapons investigation or an investigation into the murder of a United States national abroad.

Section 201 of the USA PATRIOT Act ended this anomaly in the law by amending 18 U.S.C. § 2516(1) to add the following to the list of predicate offenses under the criminal wiretap statute: chemical weapons offenses, 18 U.S.C. § 229; certain homicides and other acts of violence against United States nationals occurring outside of the United States, 18 U.S.C. § 2332; use of weapons of mass destruction; 18 U.S.C. § 2332a; violent acts of terrorism transcending national borders, 18 U.S.C. § 2332b; financial transactions with countries which support terrorism, 18 U.S.C. § 2332d; material support of terrorists, 18 U.S.C. § 2339A; and material support of terrorist organizations, 18 U.S.C. § 2339B. Two other predicate offenses were subsequently added to this list by Public Law 107-197 (Implementation of the International Convention for the Suppression of Terrorist Bombings): bombings of places of public use, government facilities, public transportation systems, and infrastructure facilities, 18 U.S.C. § 2332f; and financing of terrorism, 18 U.S.C. § 2339C. As a result, in addition to those offenses added by section 201, if section 201 were allowed to expire at the end of 2005, these two additional offenses may cease to be predicates under the wiretap statute as well.

It is important to point out that section 201 of the USA PATRIOT Act preserved all of the pre-existing standards in the wiretap statute. For example, law enforcement still must: (1) apply for and receive a court order; (2) establish probable cause to believe an individual is committing, has committed, or is about to commit a particular predicate offense; (3) establish probable cause to believe that particular communications concerning that offense will be obtained through the wiretap; and (4) establish that "normal investigative procedures" have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous.

Section 201 is extremely valuable to the Justice Department's counterterrorism efforts because it enables investigators to gather information when looking into the full range of terrorism-related crimes. If wiretaps are an appropriate investigative tool to be utilized in cases involving bribery, gambling, and obscenity, then surely investigators should be able to use them when investigating the use of weapons of mass destruction, acts of terrorism transcending national boundaries, and chemical weapons offenses.

Since the passage of the USA PATRIOT Act, Justice Department investigators have utilized section 201 to investigate, among other things, potential weapons of mass destruction offenses as well as the provision of material support to terrorists and foreign terrorist organizations. In total, as of March 10, 2005, the Department had utilized section 201 on four occasions. These four uses occurred in two separate investigations. One of these cases involved an Imperial Wizard of the White Knights of the Ku Klux

Klan, who attempted to purchase hand grenades for the purpose of bombing abortion clinics and was subsequently convicted of numerous explosives and firearms charges.

In part because section 201 preserves all of the preexisting standards for obtaining a wiretap, it has not engendered significant opposition among critics of the USA PATRIOT Act. For example, the Electronic Frontier Foundation (EFF), which has been quite critical of many provisions of the USA PATRIOT Act, has taken the position that it "does not necessarily oppose" the renewal of section 201.[1] In addition, the Center for Democracy & Technology (CDT), which describes itself as "working for civil liberties on the Internet" and has strongly opposed many USA PATRIOT Act provisions, has taken the position that section 201 in its view is not controversial.[2] To be sure, the Electronic Privacy Information Center (EPIC) has noted that "[b]ecause the government already had substantial authority under FISA to obtain a wiretap of a suspected terrorist, the real effect of [section 201] is to permit wiretapping of a United States person suspected of domestic terrorism."[3] It is entirely appropriate, however, to utilize the same surveillance technique in such an investigation as can be used in other criminal investigations. To the extent that there is probable cause to believe that Americans who are not connected to international terrorist groups are planning to use chemical weapons or weapons of mass destruction, it is absolutely vital that the Justice Department have all appropriate tools at its disposal to investigate such conduct.

Section 202: Authority to Intercept Wire, Oral, and Electronic Communications Relating to Computer Fraud and Abuse Offenses

Text of Section 202:

> Section 2516(1)(c) of title 18, United States Code, is amended by striking "and section 1341 (relating to mail fraud)," and inserting "section 1341 (relating to mail fraud), a felony violation of section 1030 (relating to computer fraud and abuse),".

How Current Law Now Reads:

> **"§ 2516. Authorization for interception of wire, oral, or electronic communications**
>
> **(1)** The Attorney General, Deputy Attorney General, Associate Attorney General, or any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General or acting Deputy Assistant Attorney General in the Criminal Division specially designated by the Attorney General, may authorize an application to a Federal judge of competent jurisdiction for, and such judge may grant in conformity with section 2518 of this chapter an order authorizing or approving the interception of wire or oral communications by the Federal Bureau of

[1] Electronic Frontier Foundation, "Let the Sun Set on PATRIOT - Section 201, 'Authority to Intercept Wire, Oral, and Electronic Communications Relating to Terrorism,' and Section 805, 'Material Support of Terrorism'", (March 31, 2004) (available at http://www.eff.org/Privacy/Surveillance/Terrorism/PATRIOT/sunset/201.php).

[2] Center for Democracy & Technology. "PATRIOT Act Sunsets", (May 7, 2004) (available at http://www.cdt.org/security/20040507sunsets.pdf).

[3] "EFF and EPIC Analysis Of The USA PATRIOT Act" (available at http://post911timeline.org/USAPA.htm).

Investigation, or a Federal agency having responsibility for the investigation of the offense as to which the application is made, when such interception may provide or has provided evidence of—

...

(c) any offense which is punishable under the following sections of this title: section 201 (bribery of public officials and witnesses), section 215 (relating to bribery of bank officials), section 224 (bribery in sporting contests), subsection (d), (e), (f), (g), (h), or (i) of section 844 (unlawful use of explosives), section 1032 (relating to concealment of assets), section 1084 (transmission of wagering information), section 751 (relating to escape), section 1014 (relating to loans and credit applications generally; renewals and discounts), sections 1503, 1512, and 1513 (influencing or injuring an officer, juror, or witness generally), section 1510 (obstruction of criminal investigations), section 1511 (obstruction of State or local law enforcement), section 1591 (sex trafficking of children by force, fraud, or coercion), section 1751 (Presidential and Presidential staff assassination, kidnapping, and assault), section 1951 (interference with commerce by threats or violence), section 1952 (interstate and foreign travel or transportation in aid of racketeering enterprises), section 1958 (relating to use of interstate commerce facilities in the commission of murder for hire), section 1959 (relating to violent crimes in aid of racketeering activity), section 1954 (offer, acceptance, or solicitation to influence operations of employee benefit plan), section 1955 (prohibition of business enterprises of gambling), section 1956 (laundering of monetary instruments), section 1957 (relating to engaging in monetary transactions in property derived from specified unlawful activity), section 659 (theft from interstate shipment), section 664 (embezzlement from pension and welfare funds), section 1343 (fraud by wire, radio, or television), section 1344 (relating to bank fraud), sections 2251 and 2252 (sexual exploitation of children), section 2251A (selling or buying of children), section 2252A (relating to material constituting or containing child pornography), section 1466A (relating to child obscenity), section 2260 (production of sexually explicit depictions of a minor for importation into the United States), sections 2421, 2422, 2423, and 2425 (relating to transportation for illegal sexual activity and related crimes), sections 2312, 2313, 2314, and 2315 (interstate transportation of stolen property), section 2321 (relating to trafficking in certain motor vehicles or motor vehicle parts), section 1203 (relating to hostage taking), section 1029 (relating to fraud and related activity in connection with access devices), section 3146 (relating to penalty for failure to appear), section 3521(b)(3)(relating to witness relocation and assistance), section 32 (relating to destruction of aircraft or aircraft facilities), section 38 (relating to aircraft parts fraud), section 1963 (violations with respect to racketeer influenced and corrupt organizations), section 115(relating to threatening or retaliating against a Federal official), section 1341 (relating to mail fraud), **a felony violation of section 1030 (relating to computer fraud and abuse)**, section 351 (violations with respect to congressional, Cabinet, or Supreme Court assassinations, kidnapping, and assault), section 831 (relating to prohibited transactions involving nuclear materials), section 33 (relating to destruction of motor vehicles or motor vehicle facilities), section 175 (relating to biological weapons), section 1992 (relating to wrecking trains), a felony violation of section 1028 (relating to production of false identification documentation), section 1425 (relating to the procurement of citizenship or nationalization unlawfully), section 1426 (relating to the reproduction of naturalization or citizenship papers), section 1427 (relating to the sale of naturalization or citizenship papers), section 1541 (relating to passport issuance without authority), section 1542 (relating to false statements in passport applications), section 1543 (relating to forgery or false use of passports), section 1544 (relating to misuse of passports), or section 1546 (relating to fraud and misuse of visas, permits, and other documents);"

Analysis:

Just as many traditional terrorism-related offenses were not listed as wiretap predicates in 18 U.S.C. § 2516(1) before passage of the USA PATRIOT Act, neither were many important cybercrime or cyberterrorism offenses. Therefore, while criminal investigators could obtain wiretap orders to monitor wire communications (voice communications over a phone) and oral communications (voice communications in person) to investigate gambling offenses, they could not use such techniques in appropriate cases involving certain serious computer crimes. Section 202 of the USA PATRIOT Act eliminated this anomaly and brought the criminal code up to date with modern technology by adding felony offenses under the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, such as computer espionage, extortion, and intentionally damaging a federal government computer, to the list of wiretap predicates in 18 U.S.C. § 2516(1).

As with section 201, section 202 of the USA PATRIOT Act preserved all of the pre-existing standards in the wiretap statute. For example, law enforcement still must: (1) apply for and receive a court order; (2) establish probable cause to believe an individual is committing, has committed, or is about to commit a particular predicate offense; (3) establish probable cause to believe that particular communications concerning that offense will be obtained through the wiretap; and (4) establish that "normal investigative procedures" have been tried and failed or reasonably appear to be unlikely to succeed or are too dangerous.

As of March 10, 2005, the Justice Department had used section 202 of the USA PATRIOT Act on two occasions. These two uses occurred in a computer fraud investigation that eventually broadened to include drug trafficking.

It is important that section 202 of the USA PATRIOT Act remain available to prosecutors should it be needed in appropriate investigations, such as these. If wiretaps are an appropriate investigative tool to be utilized in cases involving bribery, obscenity, and passport fraud, then surely investigators should be able to use such tools when investigating attempts to damage the computer systems of the federal government. In addition, commentators have noted section 202 benefits Internet service providers (ISPs) by making it "easier for the government to assist them by conducting surveillance related to hacking, denial of service attacks, and related Computer Fraud and Abuse Act (CFAA) violations."[4]

Section 202, like section 201, has not engendered significant opposition. Indeed, the CDT, which has opposed many USA PATRIOT Act provisions, has taken the position that section 202 is not controversial.[5] As one commentator has explained, section 202 "simply modernize[d] the federal police powers in light of the increased

[4] *See* Ronald L. Plesser, James J. Halpert & Emilio W. Cividanes, "USA PATRIOT Act for Internet and Communications Companies", Computer and Internet Lawyer, March 2002.
[5] *See supra* note 2.

importance of telecommunications and digital communications in the economy and society."[6]

Section 203(b): Authority to Share Criminal Investigative Information (Electronic, Wire, and Oral Interception Information)

Text of Section 203(b):

> **(b) AUTHORITY TO SHARE ELECTRONIC, WIRE, AND ORAL INTERCEPTION INFORMATION-**
>
> (1) LAW ENFORCEMENT- Section 2517 of title 18, United States Code, is amended by inserting at the end the following:
>
> > "(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.".
>
> (2) DEFINITION- Section 2510 of title 18, United States Code, is amended by--
>
> > (A) in paragraph (17), by striking "and" after the semicolon;
> >
> > (B) in paragraph (18), by striking the period and inserting "; and"; and
> >
> > (C) by inserting at the end the following:
> >
> > > "(19) 'foreign intelligence information' means--
> > >
> > > > '(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--
> > > >
> > > > > '(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
> > > > >
> > > > > '(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

[6] *See* Jon Garon, "The Electronic Jungle: The Application of Intellectual Property Law to Distance Education," 4 Vand. J. Ent. L. & Prac. 146, 166 (2002).

'(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

'(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

'(i) the national defense or the security of the United States; or

'(ii) the conduct of the foreign affairs of the United States.".

How Current Law Now Reads:

"18 U.S.C. § 2517. Authorization for disclosure and use of intercepted wire, oral, or electronic communications

...

(6) Any investigative or law enforcement officer, or attorney for the Government, who by any means authorized by this chapter, has obtained knowledge of the contents of any wire, oral, or electronic communication, or evidence derived therefrom, may disclose such contents to any other Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to the extent that such contents include foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. § 401a)), or foreign intelligence information (as defined in subsection (19) of section 2510 of this title), to assist the official who is to receive that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information."

"18 U.S.C. § 2510. Definitions

...

(17) 'electronic storage' means—

(A) any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof; and

(B) any storage of such communication by an electronic communication service for purposes of backup protection of such communication;

(18) 'aural transfer' means a transfer containing the human voice at any point between and including the point of origin and the point of reception;

(19) 'foreign intelligence information', for purposes of section 2517(6) of this title, means--

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States."

Analysis:

Before the enactment of the USA PATRIOT Act, federal law was interpreted to limit the ability of federal law enforcement officials to share terrorism-related information derived from certain investigative techniques with national defense officials and members of the intelligence community in order to protect the American people from terrorism. For example, before the Act, federal law was interpreted generally to prohibit federal prosecutors from disclosing information from criminal investigative wiretaps to intelligence and national defense officials even if that information indicated that terrorists were planning a future attack, unless such officials were assisting with the criminal investigation. Consequently, as the 9/11 Congressional Joint Inquiry Report and the report of the 9/11 Commission confirm, our ability to connect the dots and thus prevent terrorist attacks was inhibited by a lack of coordination and information sharing within the federal government.

Section 203(b) of the USA PATRIOT Act was one of the many provisions in the Act designed to alleviate this problem by facilitating information sharing among those federal officials working to prevent terrorist attacks. Because of Section 203(b), when authorities executing a criminal investigative wiretap discover foreign intelligence information, that information may now be passed on to other federal law enforcement, intelligence, protective, immigration, national defense, or national security officials for use in their official duties.

Section 203(b) specifically pertains to information: (1) related to the protection of the United States against a foreign attack or other foreign hostile action, against sabotage or international terrorism by a foreign power or its agents, or against foreign clandestine intelligence activities; (2) concerning a foreign power or territory related to the national defense, security, or foreign affairs activities of the United States; or (3) constituting foreign intelligence or counterintelligence as defined in Section 3 of the National Security Act of 1947 (that is, (a) "information relating to the capabilities, intentions, or activities of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities" or (b) "information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign

organizations, or foreign persons, or international terrorist activities."). 50 U.S.C. §§ 401a(2), (3)).

Significantly, intelligence information discovered through a criminal investigative wiretap that identifies an American citizen or a permanent resident alien may be shared with other federal officials only pursuant to guidelines mandated by the USA PATRIOT Act and promulgated by the Attorney General.[7]

The Department has made disclosures of vital information to the intelligence community and other federal officials under section 203(b) on many occasions. For example, such disclosures have been used to track terrorists' funding sources and to identify terrorist operatives overseas.

Section 203(b) of the USA PATRIOT Act closed a dangerous gap between criminal investigations and counterterrorism and other national-security investigations. Each restriction on information sharing makes it more difficult for investigators to "connect the dots" to prevent terrorist attacks. Allowing section 203(b) to expire would impede the ability of law enforcement officers to pass along information obtained from wiretaps to other federal officials, including intelligence officers, and thus would help rebuild the "wall" between our law enforcement and intelligence and defense officials that existed before September 11.

Indeed, were section 203(b) allowed to expire, United States law enforcement officers would be allowed to share certain foreign intelligence information collected through criminal investigative wiretaps with foreign intelligence services, such as MI-5, see 18 U.S.C. § 2517(7), but would arguably not be allowed to share that same information with the CIA. Such an outcome would be directly contrary to the spirit of the recently enacted Intelligence Reform and Terrorism Prevention Act of 2004, which included many provisions designed to enhance information sharing within the federal government. While the Homeland Security Act authorized the disclosure of information obtained from such wiretaps to appropriate federal, state, local, and foreign government officials in specified foreign intelligence situations, see 18 U.S.C. § 2517(8), this authority is not as broad as the authority contained in section 203(b).[8] Moreover, allowing section 203(b) and other USA PATRIOT Act provisions that have facilitated information sharing to expire would hinder the ability of Director of National Intelligence

[7] *See* Memorandum of the Attorney General, Guidelines for Disclosure of Grand Jury and Electronic, Wire, and Oral Interception Information Identifying United States Persons (Sept. 23, 2002) (available at http://www.usdoj.gov/olp/section203.pdf).

[8] Section 203(b) amended 18 U.S.C. § 2517 to allow sharing of information including foreign intelligence, counterintelligence, or foreign intelligence information, as these terms are defined in title 18 and the National Security Act of 1947. 18 U.S.C. § 2517(6). Should section 203(b) sunset, information-sharing would be permissible with respect to only a subset of such information, as specifically defined in section 2517(8), which limits information-sharing to information of "a threat of actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power, domestic or international sabotage, domestic or international terrorism, or clandestine intelligence gathering activities by an intelligence service or network of a foreign power or by an agent of a foreign power, within the United States or elsewhere, for the purpose of preventing or responding to such a threat." 18 U.S.C. § 2517(8).

to unify the intelligence community and to assemble a complete picture of terrorism-related information for the President and officials with key national-security and/or homeland-security responsibilities.

Section 203(b) has been subject to criticism from opponents of the USA PATRIOT Act. The ACLU made the most typical objection to the provision on October 23, 2001 (before passage of the USA PATRIOT Act), when it stated that "While some sharing of information may be appropriate in some limited circumstances, it should only be done with strict safeguards. . . . The bill lacks all of these safeguards."[9]

Yet, section 203(b), and the guidelines promulgated for its use, contain precisely the type of safeguards that the provision's critics have advocated. First, Title III itself imposes substantial burdens on law enforcement prior to the collection of the information at issue, greater than that necessary to obtain a search warrant. This provision does not reduce those requirements, but just provides the ability to appropriately share the information after it is collected under court order. Second, on September 23, 2002, the Attorney General issued privacy guidelines governing the sharing of wiretap information that identifies a United States person with the intelligence community. These guidelines provide important safeguards to United States persons identified in information disclosed to the intelligence community under the USA PATRIOT Act. They require that precautions be taken to ensure information is used appropriately, including labeling of all such information before disclosure, and handling the information according to specific protocols designed to ensure its appropriate use. Third, section 203(b) only allows for the sharing of a certain limited class of information gathered under Title III, such information related to national security matters. It does not provide authority to share all information gathered under Title III authority. And fourth, an individual who receives any information under the provision can use it only "in the conduct of that person's official duties."

Section 203(d): Authority to Share Criminal Investigative Information (Foreign Intelligence Information)

Text of Section 203(d):

> (d) FOREIGN INTELLIGENCE INFORMATION.—
>
> > (1) IN GENERAL.—Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 3 of the National Security Act of 1947 (50 U.S.C. 401a)) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

[9] *See* "How the USA PATRIOT Act Puts the CIA Back in the Business of Spying on Americans" (available at http://www.aclu.org/congress/l102301j.html).

(2) DEFINITION.—In this subsection, the term ''foreign intelligence information'' means—

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against—

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to—

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States.

How Current Law Now Reads:

"50 U.S.C. § 403-5d. Foreign intelligence information

(1) In general

Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence (as defined in section 401a of this title) or foreign intelligence information obtained as part of a criminal investigation to be disclosed to any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official in order to assist the official receiving that information in the performance of his official duties. Any Federal official who receives information pursuant to this provision may use that information only as necessary in the conduct of that person's official duties subject to any limitations on the unauthorized disclosure of such information.

(2) Definition

In this section, the term 'foreign intelligence information' means--

(A) information, whether or not concerning a United States person, that relates to the ability of the United States to protect against--

(i) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(ii) sabotage or international terrorism by a foreign power or an agent of a foreign power; or

(iii) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or

(B) information, whether or not concerning a United States person, with respect to a foreign power or foreign territory that relates to--

(i) the national defense or the security of the United States; or

(ii) the conduct of the foreign affairs of the United States."

Analysis:

Section 203(d) also facilitates information sharing and does so more broadly than section 203(b) by allowing law enforcement officials to share foreign intelligence information obtained as part of a criminal investigation with any Federal law enforcement, intelligence, protective, immigration, national defense, or national security official to assist them in the performance of their official duties. Section 203(d) creates a generic exception to any other law purporting to bar federal law enforcement officials or intelligence, immigration, national defense, or national security officials from receiving, for official use, information regarding foreign intelligence or counterintelligence obtained as part of a criminal investigation.

Section 203(d) has been used by the Department on a regular basis and has been instrumental to the increased coordination and information sharing between intelligence and law enforcement personnel that has taken place in the last three-and-a-half years. This provision, for example, has been utilized to help investigators "connect the dots" and break up terror cells within the United States, such as those in Portland, Oregon, and Lackawanna, New York. It has also been used to revoke suspected terrorists' visas and prevent their reentry into the country.

The provision also contains important safeguards to ensure that it is not misused. A federal official who receives any information under the provision can use it only "in the conduct of that person's official duties." Additionally, that official is bound by "any limitations on the unauthorized disclosure of such information."

The information sharing provisions are overwhelmingly heralded by investigators as the most important provisions of the USA PATRIOT Act. The new ability to share critical information has significantly altered the entire manner in which terrorism investigations are conducted, allowing for a much more coordinated and effective approach than was possible before the passage of the USA PATRIOT Act.

Perhaps the best example of information sharing now permitted by section 203 of the USA PATRIOT Act takes place in the National Counterterrorism Center (NCTC) (formerly the Terrorist Threat Integration Center). The NCTC receives information lawfully collected by its member entities, which include representatives from the law enforcement community. The FBI, one of the NCTC's key members, relies upon section 203(d) of the USA PATRIOT Act to provide information to NCTC analysts on intelligence, protective, immigration, national defense, national security, and terrorism information (a subset of foreign intelligence and counterintelligence information) obtained as part of FBI criminal investigations. In particular, section 203(d) authorizes law enforcement officers to disclose foreign intelligence or counterintelligence information to various federal officials, notwithstanding any other legal restriction.

Information provided to NCTC pursuant to section 203 of the PATRIOT Act is used in three crucial NCTC missions: the production of all-source terrorism analysis, updating the database used by other federal entities to prevent known or suspected terrorists from entering the United States, and the sharing of terrorism-related information across the federal government.

Furthermore, section 203 of the PATRIOT Act facilitates the NCTC's ability to provide strategic analysis to policy makers and actionable leads to officers within the Department of Homeland Security (DHS), the FBI, and the Intelligence Community, transcending traditional government boundaries. The NCTC uses section 203 to assemble terrorism information, both foreign and domestic, and provide the various counterterrorism mission partners with the all-source intelligence necessary to combat and prevent terrorism activities.

The NCTC estimates that the number of known or appropriately suspected terrorists intercepted at borders of the United States, based on FBI reporting alone, has increased due to the information sharing provisions of the USA PATRIOT Act. The NCTC maintains TIPOFF, an up-to-date database of known and appropriately suspected terrorists. The NCTC relies upon various agencies, which provide terrorist identity information on an on-going basis. Much of the terrorist identities information the NCTC receives from the FBI is collected by in the course of criminal investigations and is shared pursuant to section 203.

The NCTC facilitates information sharing through its NCTC Online homepage, where classified information from the intelligence and law enforcement communities on terrorism intelligence is integrated. On a daily basis, NCTC receives and shares intelligence from various law enforcement reports, including those provided by the Transportation Security Administration and Customs and Border Protection. NCTC's efforts to "connect the dots" and share terrorism intelligence across the federal government will be severely restricted if such information sharing is prohibited in the future. In the absence of mandatory or permissive statutory provisions like section 203(d), each Executive Branch entity would be required to identify proper legal authority prior to sharing or disseminating information outside of the collecting agency or community.

FBI Field Offices have also specifically noted that provisions such as section 203(d) enable case agents to involve other agencies in investigations, resulting in a style of teamwork that: enables more effective and responsive investigations; improves the utilization of resources; allows for follow-up investigations by other agencies when the criminal subject leaves the United States; and helps prevent the compromise of foreign intelligence investigations.

Even though the law prior to the USA PATRIOT Act provided for some exchange of information, the law was complex and, as a result, agents often erred on the side of caution and refrained from sharing information. The USA PATRIOT Act's new information sharing authorities, including section 203, eliminated that hesitation and now allow agents to work more openly with other government entities resulting in a much

stronger team approach. Such an approach is necessary in order to effectively prevent and detect the complex web of terrorist activity. As a result, FBI Field Offices report enhanced liaison with state, local and other Federal agencies, resulting in better relationships. If even a portion of the information sharing capabilities are allowed to "sunset" or terminate, then an element of uncertainty will be re-introduced and agents will again hesitate and take the time necessary to seek clarification of the relevant legal restrictions prior to sharing information. This hesitation will lead to less teamwork and much less efficiency. For all of these reasons, section 203(d) should be renewed.

Section 204: Clarification of Intelligence Exceptions from Limitations on Interception and Disclosure of Wire, Oral, and Electronic Communications

Text of Section 204:

> Section 2511(2)(f) of title 18, United States Code, is amended—
>
> > (1) by striking "this chapter or chapter 121" and inserting "this chapter or chapter 121 or 206 of this title"; and
> >
> > (2) by striking "wire and oral" and inserting "wire, oral, and electronic".

How Current Law Now Reads:

> **"18 U.S.C. § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited**
> ...
>
> (2)
> ...
>
> > (f) Nothing contained in this chapter or chapter 121 or 206 of this title, or section 705 of the Communications Act of 1934, shall be deemed to affect the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 101 of the Foreign Intelligence Surveillance Act of 1978, and procedures in this chapter or chapter 121 and the Foreign Intelligence Surveillance Act of 1978 shall be the exclusive means by which electronic surveillance, as defined in section 101 of such Act, and the interception of domestic wire, oral, and electronic communications may be conducted."

Analysis:

The purpose of this provision is two-fold. First, it clarifies that chapter 206 of title 18, which governs the installation and use of pen registers and trap-and-trace devices, will not interfere with certain foreign intelligence activities that fall outside of the definition of "electronic surveillance" in the Foreign Intelligence Surveillance Act ("FISA"). *See* 147 Cong. Rec. S11,006 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy) (explaining that the purpose of section 204 of the USA PATRIOT Act, entitled "Clarification of intelligence exceptions from limitations on interception and disclosure

of wire, oral, and electronic communications," was "to make clear that these procedures [including those set forth in chapter 206] do not apply to the collection of foreign intelligence information under the statutory foreign intelligence authorities").

Second, section 204 clarifies that the exclusivity provision in section 2511(2)(f) of title 18 applies not only to the interception of wire and oral communications, but also to the interception of electronic communications. Section 2511(2)(f) reflects Congress's intent, when it enacted FISA and the Electronic Communications Privacy Act of 1986, to make the procedures in chapter 119 of title 18 ("Title III") (regulating the interception and disclosure of wire, electronic, and oral communications), chapter 121 of title 18 (regulating access to stored wire and electronic communications and transactional records), and FISA (regulating electronic surveillance undertaken to acquire foreign intelligence information) the exclusive procedures for conducting electronic surveillance, as defined by FISA, and intercepting certain types of domestic communications.

Section 204 remedies an apparent omission in the Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848, which, among other things, amended chapter 119 of title 18 ("Title III") to provide procedures for intercepting electronic communications and added chapter 121 to title 18 to provide procedures for accessing stored electronic communications, but neglected to make a corresponding change to clarify that the exclusivity provision in section 2511(2)(f) applies to the interception of not only wire and oral, but also electronic, communications.

Section 204 has been criticized by some opponents of the USA PATRIOT Act. For instance, EPIC has implied that section 204 improperly circumvented proper methods of investigation: it argued that the section "amended Title III and the Stored Communications Access Act so that stored voice-mail communications, like e-mail, may be obtained by the government through a search warrant rather than through more stringent wiretap orders."[10]

However, criticism of section 204, which appears to represent the view of a small minority,[11] obscures the fact that section 204 is, as the nonpartisan Congressional Research Service has observed, "essentially a technical amendment." Moreover, EPIC appears to confuse section 204 with section 209 of the Act.[12] In an age when terrorists use electronic communications just like everyone else, it is important to preserve section 204, a technical amendment that merely clarifies what Congress had always intended the statute to mean.

---

[10] *See supra* note 3.

[11] For instance, CDT, which has criticized many provisions of the USA PATRIOT Act, has stated that section 204 is among the provisions "that are not controversial." *See supra* note 2.

[12] Charles Doyle, Congressional Research Service, "USA PATRIOT Act: A Sunset Sketch" at CRS-3 (June 20, 2004).

Section 206: Roving Surveillance Authority under FISA

Text of Section 206:

> Section 105(c)(2)(B) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(c)(2)(B)) is amended by inserting `, or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons,' after `specified person'."

How Current Law Now Reads:

> **"50 U.S.C. § 1805. Issuance of order**
> ...
> (c) Specifications and directions of orders
>
> An order approving an electronic surveillance under this section shall--
> ...
>
> (2) direct--
>
> (A) that the minimization procedures be followed;
>
> (B) **that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person, or in circumstances where the Court finds that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance**;
>
> (C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of Central Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and
>
> (D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid."

Analysis:

A multipoint or "roving" wiretap order attaches to a particular suspect rather than to a particular phone or other communications facility. Prior to enactment of the USA PATRIOT Act, such wiretaps, which have long been available in the criminal investigative context, were not available under FISA. They were and are needed, however, international terrorists and foreign intelligence officers are trained to thwart surveillance by changing the communications facilities they use, thus making roving wiretaps particularly necessary in this context. Without roving wiretaps, investigators were often left two steps behind sophisticated terrorists.

Before the USA PATRIOT Act, 50 U.S.C. § 1805(c)(2)(B) permitted the Foreign Intelligence Surveillance Court ("FISA Court") to order "specified persons" (third parties such as telephone companies) to provide assistance and information to federal authorities in installing a wiretap or collecting information related to a foreign intelligence investigation. However, each time a suspect switched modes of communication, for example by obtaining a new cell phone, investigators had to return to the FISA Court for a new order just to change the name of the "specified person" needed to assist in monitoring the wiretap. This requirement significantly reduced the effectiveness of FISA surveillance.

Section 206 eliminated this problem. It amended 50 U.S.C. § 1805(c)(2)(B) to allow the FISA Court to issue roving wiretap orders under FISA in cases where the target's actions may thwart surveillance. Specifically, it inserted language into section 1805(c)(2)(B) permitting the FISA Court to direct the wiretap order to specified persons and "other persons" if the court finds that the "actions of the target of the application may have the effect of thwarting the identification of a specified person" who would be required to assist in installing the court-authorized wiretap. Thus, the FISA Court does not have to name in the wiretap order each telecommunications company or other "specified person" whose assistance might be required. Section 206 also allowed the FISA Court to compel any necessary additional parties to assist in the installation of the wiretap and to furnish all information, facilities, or technical assistance necessary without specifically naming such persons in the wiretap order. Significantly, however, section 206 did not change the requirement that the target of the electronic surveillance must be identified or described in the order.

The ACLU has argued that wiretaps issued pursuant to section 206 "pose a greater challenge to privacy because they are authorized secretly without a showing of probable cause of crime. This Section represents a broad expansion of power without building in a necessary privacy protection."[13]

This argument, however, ignores the fact that section 206 did not alter the requirement that before approving electronic surveillance, the FISA Court must find that there is probable cause to believe that the target of the surveillance is either a foreign power or an agent of a foreign power, such as a terrorist or spy. Moreover, for years, law enforcement has been able to use roving wiretaps to investigate traditional crimes, including drug offenses and racketeering. The authority to use roving wiretaps in traditional criminal investigations has existed since 1986. Section 206 simply authorized the same techniques in foreign intelligence investigations.

In addition, wiretaps under section 206 can be ordered only after the FISA court makes a finding that the actions of the target of the application may have the effect of thwarting the surveillance. A number of federal courts – including the Second, Fifth, and Ninth Circuits – have squarely ruled that similar roving wiretaps are perfectly consistent

[13] American Civil Liberties Union, *How the Anti-Terrorism Bill Limits Judicial Oversight of Telephone and Internet Surveillance* (Oct. 23, 2001) (available at http://www.aclu.org/congress/1102301g.html).

with the Fourth Amendment, *see, e.g.*, *United States v. Gaytan*, 74 F.3d 545 (5th Cir. 1996); *United States v. Bianco*, 998 F.2d 1112 (2d Cir. 1993); *United States v. Petti*, 973 F.2d 1441 (9th Cir. 1992), and no court of appeals has found otherwise.

Some have claimed that section 206 "authorizes intelligence investigators to conduct 'John Doe' roving surveillance – meaning that the FBI can wiretap every single phone line, mobile communications device or Internet connection that a suspect might be using, without ever having to identify the suspect by name. This, it is argued, gives the FBI a 'blank check' to violate the communications privacy of countless innocent Americans."[14]

Labeling wiretaps authorized under section 206 as "John Doe" wiretaps, however, is misleading. Even if the government is not sure of the actual identity of the target of such a wiretap, FISA nonetheless requires the government to provide "a description of the target of the electronic surveillance" to the FISA Court prior to obtaining a surveillance order. 50 U.S.C. § 1805(c)(1)(A). In certain cases involving terrorists and spies, the government simply may not know the name of the terrorist or spy in question, but still must be able to conduct surveillance of that individual, whom it already has probable cause to believe is involved in terrorism or espionage. A surveillance order under section 206 therefore is always connected to a particular target of surveillance. Moreover, as then-Attorney General Ashcroft explained in a January 28, 2004, letter to Senator Hatch, the government "cannot change the target of its surveillance under such a wiretap order; it must instead apply to the FISA court for a new order for the new target."

A related objection is that section 206 lacks an "ascertainment" requirement supposedly needed to preclude the surveillance of law-abiding Americans. As asserted by John Podesta, former Chief of Staff to President Clinton:

> The main difference between roaming wiretaps under current criminal law and the new FISA authority is that current criminal law requires that law enforcement "ascertain" that the target of a wiretap is actually using a device to be tapped. Section 206 contains no such provision. Ensuring that FISA wiretaps only roam when intelligence officials "ascertain" that the subject of an investigation is using a device, before it is tapped, would prevent abuse of this provision. For example, without the ascertainment requirement, it is conceivable that all the pay phones in an entire neighborhood could be tapped if suspected terrorists happened to be in that neighborhood. Bringing FISA roaming wiretaps in line with criminal roaming wiretaps would prevent such abuse and provide greater protection to the privacy of ordinary Americans.[15]

---

[14] *See* Electronic Frontier Foundation, "Let the Sun Set on PATRIOT - Section 206: 'Roving Surveillance Authority Under the Foreign Intelligence Surveillance Act of 1978'", (Feb. 24, 2004) (available at http://shop.eff.org/Privacy/Surveillance/Terrorism/PATRIOT/sunset/206.php).

[15] *See* American Bar Association, Section on Individual Rights and Responsibilities, "USA PATRIOT Act: The Good, the Bad, and the Sunset," *Human Rights Magazine* (Winter 2002).

This criticism misses the mark. The specific "ascertainment" requirement contained in the criminal wiretap statute, *see* 18 U.S.C. § 2518(12), applies to the interception of oral communications, such as through hidden microphones, and not to the interception of wire or electronic communications, such as telephone calls. This provision of the criminal wiretap statute states that the interception of an oral communication "shall not begin until the place where the communication is to be intercepted is ascertained by the person implementing the interception order." Applying that ascertainment requirement to FISA roving wiretaps, as would be done by the SAFE Act, which was introduced in the 108th Congress, would therefore make it harder to conduct effective surveillance of international terrorists than of drug dealers.[16] Moreover, section 206 in no way altered the robust FISA minimization procedures that limit the acquisition, retention, and dissemination by the government of information or communications involving United States persons.

Indeed, Podesta himself has endorsed the rationale underlying section 206, writing that before the USA PATRIOT Act: "FISA required a separate court order be obtained for each communication carrier used by the target of an investigation. In the era of cell phones, pay phones, e-mail . . . , and BlackBerry wireless e-mail devices, such a requirement is a significant barrier in monitoring an individual's communications. Section 206 allows a single wiretap to legally 'roam' from device to device, to tap the person rather than the phone. In 1986, Congress authorized the use of roaming wiretaps in criminal investigations that are generally subject to stricter standards than FISA intelligence gathering, so extending this authority to FISA was a natural step."[17] Section 206 should be preserved. Without this crucial authority, investigators would once again often be struggling to catch up to sophisticated terrorists trained to constantly change phones in order to avoid surveillance.

Section 207: Duration of FISA Surveillance of Non-United States Persons Who Are Agents of a Foreign Power

Text of Section 207:

> (a) DURATION -
>
> > (1) SURVEILLANCE- Section 105(c)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(e)(1)) is amended by--
> >
> > > (A) inserting "(A)" after "except that"; and
> > >
> > > (B) inserting before the period the following: ", and (B) an order under this Act for a surveillance targeted against an agent of a foreign power, as defined in section 101(b)(1)(A) may be for the period specified in the application or for 120 days, whichever is less".
> >
> > (2) PHYSICAL SEARCH- Section 304(d)(1) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824(d)(1)) is amended by--

[16] *See* S. 1709 (The Security and Freedom Ensured Act of 2003), 108th Congress, § 2.
[17] *Id.*

(A) striking "forty-five" and inserting "90";

(B) inserting "(A)" after "except that"; and

(C) inserting before the period the following: ", and (B) an order under this section for a physical search targeted against an agent of a foreign power as defined in section 101(b)(1)(A) may be for the period specified in the application or for 120 days, whichever is less".

(b) EXTENSION-

(1) IN GENERAL- Section 105(e)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805(e)(2)) is amended by--

(A) inserting "(A)" after "except that"; and

(B) inserting before the period the following: ", and (B) an extension of an order under this Act for a surveillance targeted against an agent of a foreign power as defined in section 101(b)(1)(A) may be for a period not to exceed 1 year".

(2) DEFINED TERM- Section 304(d)(2) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1824(d)(2) is amended by inserting after "not a United States person," the following: "or against an agent of a foreign power as defined in section 101(b)(1)(A),".

How Current Law Now Reads:

§ 1805. Issuance of order

...

(c) Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated

(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that (A) an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title, for the period specified in the application or for one year, whichever is less, and (B) an order under this chapter for a surveillance targeted against an agent of a foreign power, as defined in section 1801(b)(1)(A) of this title may be for the period specified in the application or for 120 days, whichever is less.

(2) Extensions of an order issued under this subchapter may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that (A) an extension of an order under this chapter for a surveillance targeted against a foreign power, as defined in section 1801(a)(5) or (6) of this title, or against a foreign power as defined in section 1801(a)(4) of this title that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period, and (B) an extension of an order under this chapter for a surveillance targeted against an agent of a foreign power as defined in section 1801(b)(1)(A) of this title may be for a period not to exceed 1 year.

(3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

§ 1824. Issuance of order

...

(d) Duration of order; extensions; assessment of compliance

(1) An order issued under this section may approve a physical search for the period necessary to achieve its purpose, or for 90 days, whichever is less, except that (A) an order under this section shall approve a physical search targeted against a foreign power, as defined in paragraph (1), (2), or (3) of section 1801(a) of this title, for the period specified in the application or for one year, whichever is less, and (B) an order under this section for a physical search targeted against an agent of a foreign power as defined in section 1801(b)(1)(A) of this title may be for the period specified in the application or for 120 days, whichever is less.

(2) Extensions of an order issued under this subchapter may be granted on the same basis as the original order upon an application for an extension and new findings made in the same manner as required for the original order, except that an extension of an order under this chapter for a physical search targeted against a foreign power, as defined in section 1801(a)(5) or (6) of this title, or against a foreign power, as defined in section 1801(a)(4) of this title, that is not a United States person, or against an agent of a foreign power as defined in section 1801(b)(1)(A) of this title, may be for a period not to exceed one year if the judge finds probable cause to believe that no property of any individual United States person will be acquired during the period.

(3) At or before the end of the period of time for which a physical search is approved by an order or an extension, or at any time after a physical search is carried out, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

Analysis:

Prior to the passage of the USA PATRIOT Act, surveillance orders issued by the FISA Court and directed against agents of a foreign power, such as international terrorists or spies, had a maximum duration of 90 days, and could be extended with court approval for additional periods of 90 days. Physical search orders issued by the FISA Court and directed against agents of a foreign power were effective for no more than 45 days. These short timeframes forced Justice Department investigators to needlessly divert manpower from the primary mission of detecting and disrupting potential terrorist attacks in order to return frequently to the FISA Court to extend FISA search and surveillance orders even in routine matters where there was no question about the legal sufficiency of a particular case.

Section 207 of the USA PATRIOT Act helped to ameliorate this problem by increasing the maximum time duration for FISA surveillance and physical search orders. Now, initial surveillance orders directed against non-United States person members of international terrorist groups or officers and employees of foreign powers may be in

effect for up to 120 days (instead of 90 days),[18] and such orders may be extended for a maximum of one year (instead of 90 days) at a time with court approval. Similarly, physical search orders may now remain effective for up to 90 days (instead of 45 days) in the case of agents of a foreign power who are United States persons and 120 days (instead of 45 days) with respect to non-United States person members of international terrorist groups or officers and employees of foreign powers. In the case of non-United States person members of international terrorist groups or officers and employees of foreign powers, such search orders may be extended for up to one year with court approval in certain circumstances.

While many critics of the USA PATRIOT Act, such as the CDT, have expressed the view that section 207 is not controversial,[19] others disagree. EFF, for example, opposes the renewal of section 207.[20] EFF complains the time limits for FISA wiretaps and searches before the passage of the USA PATRIOT Act "were already generous compared to taps and warrants available to the FBI in criminal investigations."[21] Wiretap orders in the criminal context, for example, may only initially authorize surveillance for up to 30 days, and such orders may only be extended by a court for 30 days at a time. EFF further asserts that the only benefit derived from section 207 is "reduced paperwork" and that this benefit comes at the cost of the interception of "many more innocent communications" between "many more innocent persons."[22]

These criticisms of section 207, however, fall wide of the mark. To begin with, section 207 does not make it easier to conduct surveillance of innocent Americans. The provision does not change the requirement that surveillance and physical search orders may only be directed against those the FISA Court finds probable cause to believe are foreign powers or agents of foreign powers. Moreover, the extended time periods for FISA wiretap and surveillance orders only apply to certain agents of a foreign power who are not United States persons. Such time periods thus do not apply to wiretaps and surveillance orders directed against United States citizens or lawful permanent resident aliens. Finally, section 207 in no way altered the robust FISA minimization procedures that limit the acquisition, retention, and dissemination of information or communications involving United States persons.

Perhaps more importantly, however, EFF's criticism significantly underemphasizes the important benefits brought about by section 207. The Department

---

[18] Pursuant to 50 U.S.C. § 1805(e)(1), surveillance orders may now be directed against agents of a foreign power, as defined in 50 U.S.C. § 1801(b)(1)(A), for a maximum of 120 days. Agents of a foreign power, as defined in 50 U.S.C. § 1801(b)(1)(A), are non-United States persons who "act[] in the United States as an officer of employee of a foreign power, or as a member of a foreign power defined in [50 U.S.C. § 1801(a)(4)]." Title 50 U.S.C. § 1801(a)(4), in turn, refers to "a group engaged in international terrorism or activities in preparation therefor."

[19] *See supra* note 2.

[20] Electronic Frontier Foundation, "Let the Sun Set on PATRIOT - Section 207: 'Duration of Surveillance of Non-United States Persons Who Are Agents of a Foreign Power'" (Mar. 2, 2004) (available at http://www.eff.org/Privacy/Surveillance/Terrorism/PATRIOT/sunset/207.php).

[21] *Id.*

[22] *Id.*

believes that section 207 has made a critical contribution to protecting the national security of the United States by making changes to the time periods for which electronic surveillance and physical searches are authorized under FISA. This is critical, because by doing so, it has conserved the limited resources that are available at the FBI and the Department's Office of Intelligence Policy and Review to process FISA applications. Instead of devoting time to the mechanics of processing FISA applications, which are considerable, government resources can be devoted to other investigative activity as well as reviewing compliance with laws, executive orders, and policy guidelines intended to ensure appropriate oversight of the use of intelligence collection authorities.

For example, prior to enactment of section 207, in order to conduct electronic surveillance and physical search of foreign diplomats and non-resident alien terrorists during one calendar year, the government had to file four applications for electronic surveillance covering successive 90-day periods, and eight applications for physical search covering successive 45-day periods, for a total of 12 separate applications. Thanks to section 207, however, this number can be reduced to two applications -- one combined electronic surveillance and physical search application for an initial period of 120 days, and, at the end of that 120-day period, a second combined application for one year (provided that the court finds that there is probable cause to believe that no property of any individual United States person will be acquired during the one year physical search authorization period). This represents an 83 percent reduction in the amount of paperwork involved to target clearly legitimate agents of foreign powers, and allows the government to devote those resources to other important tasks.

Section 207 also enables the government to more efficiently conduct electronic surveillance and physical search of United States persons who are agents of a foreign power. While section 207 did not change the time periods applicable for electronic surveillance of United States persons, which remained at 90 days, by making the time periods of electronic surveillance orders and physical search orders equivalent with respect to United States persons, it has enabled the Department to file streamlined combined electronic surveillance and physical search applications that, in the past, were tried but abandoned as too cumbersome to do effectively. Thus, prior to enactment of section 207, in order to conduct electronic surveillance and physical search of such targets, the government had to file four applications for electronic surveillance covering successive 90-day periods, and eight applications for physical search covering successive 45-day periods, for a total of 12 separate applications. Thanks to section 207, this number can be reduced to four combined electronic surveillance and physical search applications. This represents a two-thirds reduction in the number of applications the government is required to file with the FISA court in these circumstances.

This provision has not merely led to reduced paperwork; section 207 has resulted in a more effective utilization of available personnel resources and the collection mechanisms authorized under FISA. It has allowed investigators to focus their efforts on more significant and complicated terrorism-related cases and to spend more time ensuring that appropriate oversight is given to investigations involving the surveillance of United States persons. Given the finite resources at the Justice Department's disposal, the use of personnel to prepare and process routine extensions of FISA surveillance and

search orders reduces the manpower available to focus on preventing terrorist attacks as well as processing new applications for FISA surveillance. While the Department has been subjected to criticism by some for processing FISA applications too slowly, great strides have been made in the recent years in improving the efficiency of the FISA process because of both the addition of new personnel and the use of section 207. However, were section 207 allowed to expire, much of this progress would be reversed, and Justice Department personnel would be forced to spend significantly more time on the routine extensions of current FISA orders and significantly less time on new applications.

While specific information regarding the Department's use of section 207 is classified, relevant data has been provided to Congress in the Attorney General's semi-annual report on the Department's use of the Foreign Intelligence Surveillance Act. Such reports were transmitted to Congress in April 2002, January 2003, September 2003, December 2003, September 2004, and December 2004.

Section 209: Seizure of Voice-Mail Messages Pursuant to Warrants

Text of Section 209:

Title 18, United States Code, is amended--

(1) in section 2510--

(A) in paragraph (1), by striking beginning with "and such" and all that follows through "communication"; and

(B) in paragraph (14), by inserting "wire or" after "transmission of"; and

(2) in subsections (a) and (b) of section 2703--

(A) by striking "CONTENTS OF ELECTRONIC" and inserting "CONTENTS OF WIRE OR ELECTRONIC" each place it appears;

(B) by striking "contents of an electronic" and inserting "contents of a wire or electronic" each place it appears; and

(C) by striking "any electronic" and inserting "any wire or electronic" each place it appears.

How Current Law Now Reads:

"§ 2510. Definitions

As used in this chapter--

(1) 'wire communication' means any aural transfer made in whole or in part through the use of facilities for the transmission of communications by the aid of wire, cable, or other like connection between the point of origin and the point of reception (including the use of such connection in a switching station) furnished or operated by any person engaged in

providing or operating such facilities for the transmission of interstate or foreign communications or communications affecting interstate or foreign commerce;
...
(14) 'electronic communications system' means any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications;"

"§ 2703. Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.—

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing."

Analysis:

Prior to the passage of the USA PATRIOT Act, law enforcement officers were able to obtain access to voice messages stored on home answering machines with a search warrant. Likewise, under the Electronic Communications Privacy Act ("ECPA"), 18 U.S.C. § 2703 et seq., law enforcement officers needed only a search warrant to access stored electronic communications, such as e-mail. If, however, a voice-mail message was stored on a voice-mail system with a telecommunications provider, instead of on an answering machine, law enforcement officers were required to meet the higher standard necessary for obtaining a wiretap order. This was because access to stored wire communications (such as voice-mail) was governed by the wiretap statute, 18 U.S.C. § 2510(1), instead of ECPA.

Regulating stored wire communications through the wiretap statute created large and unnecessary burdens for criminal investigators. Stored voice communications, however, possess few of the sensitivities associated with the real-time interception of telephones, making the extremely burdensome process of obtaining a wiretap order unreasonable. Moreover, in large part, the pre-USA PATRIOT Act statutory framework envisioned a world in which technology-mediated voice communications (such as telephone calls) were conceptually distinct from non-voice communications (such as faxes, pager messages, and e-mail). To the limited extent that Congress had acknowledged that data and voice might co-exist in a single transaction, it had not anticipated the convergence of these two kinds of communications typical of today's telecommunications networks. With the advent of MIME — Multipurpose Internet Mail Extensions — and similar features, an e-mail may now include one or more "attachments" consisting of any type of data, including voice recordings. As a result, a law enforcement officer seeking to obtain a suspect's unopened e-mail from an Internet service provider by means of a search warrant (as required under 18 U.S.C. § 2703(a)) has no way of knowing whether the inbox messages include voice attachments (i.e., wire communications), which could not be compelled using a search warrant.

Section 209 of the USA PATRIOT Act solved these problems by harmonizing the rules for obtaining stored "wire" communications (e.g., voice-mail) with those for obtaining stored "electronic" communications (e.g., e-mail), making 18 U.S.C. § 2703 equally applicable to both and eliminating the disparity in treatment of what was essentially the same type of information. As a result, just as law enforcement may obtain access to voice messages stored on a home answering machine or stored e-mail messages through the use of a search warrant, law enforcement may now also obtain voice-mail stored electronically with a telecommunications provider through the use of a warrant rather than through the use of a wiretap order.

Section 209 preserved all of the pre-existing standards for the availability of search warrants. For example, law enforcement still must: (1) apply for and receive a court order; and (2) establish probable cause that the property to be searched or seized is evidence of a crime or property that is designed for use, intended for use, or was used in committing a crime.

Section 209 of the USA PATRIOT Act thus modernized federal law by enabling investigators to more quickly access suspects' voice-mail by using a search warrant. This is important because the speed with which voice-mail is seized and searched can be critical to an investigation where time is of the essence. Section 209 has been very useful to the Department, and warrants issued pursuant to this provision have been used to obtain evidence in a variety of criminal cases, including a number of drug trafficking investigations, such as an investigation of a large-scale ecstasy smuggling ring based in the Netherlands, an investigation into a series of violent robberies, and a kidnapping investigation.

Section 209 has not generated significant opposition. However, some, such as EFF, have complained that section 209 unnecessarily reduces the privacy of Americans' voice-mail.[23] Such critics have failed to explain, however, why it should be harder for law enforcement to gain access to voice-mail messages stored on the system of a telecommunications provider than to messages stored on a home answering machine or to e-mail messages stored by an Internet service provider. To date, no persuasive explanation has been provided.

Section 212: Emergency Disclosure of Electronic Communications to Protect Life and Limb

Text of Section 212:

(a) DISCLOSURE OF CONTENTS-

(1) IN GENERAL- Section 2702 of title 18, United States Code, is amended--

(A) by striking the section heading and inserting the following:

"Sec. 2702. Voluntary disclosure of customer communications or records";

(B) in subsection (a)--

(i) in paragraph (2)(A), by striking "and" at the end;

(ii) in paragraph (2)(B), by striking the period and inserting "; and"; and

(iii) by inserting after paragraph (2) the following:

"(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the

[23] *See* Electronic Frontier Foundation, "Let the Sun Set on PATRIOT - Section 209: 'Seizure of Voice Mail Messages Pursuant to Warrants'", (Mar. 10, 2004) (available at http://www.eff.org/Privacy/Surveillance/Terrorism /PATRIOT/sunset/209.php).

contents of communications covered by paragraph (1) or (2)) to any governmental entity.";

(C) in subsection (b), by striking "EXCEPTIONS- A person or entity" and inserting "EXCEPTIONS FOR DISCLOSURE OF COMMUNICATIONS- A provider described in subsection (a)";

(D) in subsection (b)(6)--

(i) in subparagraph (A)(ii), by striking "or";

(ii) in subparagraph (B), by striking the period and inserting "; or"; and

(iii) by adding after subparagraph (B) the following:

"(C) if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person requires disclosure of the information without delay."; and

(E) by inserting after subsection (b) the following:

"(c) EXCEPTIONS FOR DISCLOSURE OF CUSTOMER RECORDS- A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--

"(1) as otherwise authorized in section 2703;

"(2) with the lawful consent of the customer or subscriber;

"(3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

"(4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information; or

"(5) to any person other than a governmental entity.".

(2) TECHNICAL AND CONFORMING AMENDMENT- The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2702 and inserting the following:

"2702. Voluntary disclosure of customer communications or records.".

(b) REQUIREMENTS FOR GOVERNMENT ACCESS-

(1) IN GENERAL- Section 2703 of title 18, United States Code, is amended--

(A) by striking the section heading and inserting the following:

"Sec. 2703. Required disclosure of customer communications or records";

(B) in subsection (c) by redesignating paragraph (2) as paragraph (3);

(C) in subsection (c)(1)--

(i) by striking "(A) Except as provided in subparagraph (B), a provider of electronic communication service or remote computing service may" and inserting "A governmental entity may require a provider of electronic communication service or remote computing service to";

(ii) by striking "covered by subsection (a) or (b) of this section) to any person other than a governmental entity.

"(B) A provider of electronic communication service or remote computing service shall disclose a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a) or (b) of this section) to a governmental entity' and inserting `)";

(iii) by redesignating subparagraph (C) as paragraph (2);

(iv) by redesignating clauses (i), (ii), (iii), and (iv) as subparagraphs (A), (B), (C), and (D), respectively;

(v) in subparagraph (D) (as redesignated) by striking the period and inserting "; or"; and

(vi) by inserting after subparagraph (D) (as redesignated) the following:

"(E) seeks information under paragraph (2).";and

(D) in paragraph (2) (as redesignated) by striking "subparagraph (B)" and insert "paragraph (1)".

(2) TECHNICAL AND CONFORMING AMENDMENT- The table of sections for chapter 121 of title 18, United States Code, is amended by striking the item relating to section 2703 and inserting the following:

"2703. Required disclosure of customer communications or records.".

How Current Law Now Reads:

"§ 2702. Voluntary disclosure of customer communications or records

(a) Prohibitions.--Except as provided in subsection (b)--

(1) a person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service; and

(2) a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents of any communication which is carried or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service;

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing; and

(3) a provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by paragraph (1) or (2)) to any governmental entity.

(b) Exceptions for disclosure of communications.-- A provider described in subsection (a) may divulge the contents of a communication--

(1) to an addressee or intended recipient of such communication or an agent of such addressee or intended recipient;

(2) as otherwise authorized in section 2517, 2511(2)(a), or 2703 of this title;

(3) with the lawful consent of the originator or an addressee or intended recipient of such communication, or the subscriber in the case of remote computing service;

(4) to a person employed or authorized or whose facilities are used to forward such communication to its destination;

(5) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;

(6) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032);

(7) to a law enforcement agency--

(A) if the contents--

(i) were inadvertently obtained by the service provider; and

(ii) appear to pertain to the commission of a crime; or

> (8) to a Federal, State, or local governmental entity, if the provider, in good faith, believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency.
>
> (c) Exceptions for disclosure of customer records.--A provider described in subsection (a) may divulge a record or other information pertaining to a subscriber to or customer of such service (not including the contents of communications covered by subsection (a)(1) or (a)(2))--
>
> (1) as otherwise authorized in section 2703;
>
> (2) with the lawful consent of the customer or subscriber;
>
> (3) as may be necessarily incident to the rendition of the service or to the protection of the rights or property of the provider of that service;
>
> (4) to a governmental entity, if the provider reasonably believes that an emergency involving immediate danger of death or serious physical injury to any person justifies disclosure of the information;
>
> (5) to the National Center for Missing and Exploited Children, in connection with a report submitted thereto under section 227 of the Victims of Child Abuse Act of 1990 (42 U.S.C. 13032); or
>
> (6) to any person other than a governmental entity.

Analysis:

Prior to the passage of the USA PATRIOT Act, federal law contained no special provision authorizing electronic communication service providers to disclose voluntarily customer records or communications to federal authorities in emergency situations. If, for example, an Internet service provider ("ISP") possessed information that, if disclosed to the government, could prevent an imminent terrorist attack, an ISP making such a disclosure on a voluntary basis might have been sued civilly since providing such information did not fall within one of the statutory exceptions to the limitations on disclosure contained in the Electronic Communications Privacy Act ("ECPA"), even if that disclosure was necessary to save lives.

In addition, prior to the enactment of the USA PATRIOT Act, federal law did not expressly permit an ISP to voluntarily disclose customer records (such as a subscriber's login records) to the government to protect itself against hacking. The law did, however, allow providers to disclose the content of communications for this reason. *See* 18 U.S.C. §§ 2702(b)(5), former § 2703(c)(1)(B). This created a nonsensical anomaly in the law as the right to disclose the content of communications logically implies the less-intrusive ability to disclose non-content records. Moreover, as a practical matter, providers need to have the right to disclose to law enforcement the facts surrounding attacks on their systems. For example, when an ISP's customer hacks into the ISP's network, gains complete control over an e-mail server, and reads or modifies the e-mail of other customers, the provider must have the legal ability to report the complete details of the crime.

Section 212 corrected both of these inadequacies in the statute. First, it amended 18 U.S.C. § 2702(b)(6) to permit, but not require, a service provider to disclose to federal authorities either content or non-content customer records in emergencies involving an immediate risk of death or serious physical injury to any person. It is important to recognize, however, that this voluntary disclosure authority does not create an affirmative obligation on service providers to review customer communications in search of such imminent dangers. Section 212 also amended ECPA to allow service providers to disclose information to protect their rights and property. Specifically, it amended 18 U.S.C. § 2702(c)(3) to clarify that service providers do have the statutory authority to disclose non-content records to protect their rights and property.

In 2002, the Homeland Security Act repealed that portion of section 212 governing the disclosure of the content of communications in emergency situations and placed similar authority in a separate statutory provision, 18 U.S.C. § 2702(b)(7). The Homeland Security Act, however, did not alter that portion of section 212 pertaining to the voluntary disclosure of non-content customer records in emergency situations. Thus, were Section 212 of the USA PATRIOT Act allowed to expire at the end of 2005, an ISP would find itself in the anomalous position of being able to voluntarily disclose the content of customers' communications in emergency situations but not being able to voluntarily disclose non-content customer records pertaining to those communications in emergency situations.

Section 212 has been used often and has already saved lives. To give just a few examples, voluntary disclosures from computer service providers pursuant to section 212 have assisted law enforcement in safely recovering an 88-year-old Wisconsin woman who was kidnapped and held for ransom while bound in an unheated shed during a cold Wisconsin winter and in safely recovering four kidnapped or missing children. For instance, a few months ago, Bobbie Jo Stinnett of Skidmore, Missouri, who was eight months pregnant, was found strangled in her home lying in a pool of her own blood. Her unborn daughter had been cut out of her womb with a kitchen knife. Police officers examined a computer found in Bobbie Jo's home. They discovered that she had been active on the Internet in connection with her dog-breeding business. As the investigation intensified, the officers found an exchange from a message board between Bobbie Jo and someone who called herself Darlene Fischer. Fischer claimed to be interested in a dog. She had asked Bobbie Jo for directions to her house for a meeting on December 16—the same day as the murder. Using section 212, FBI agents and examiners at the Regional Computer Forensic Laboratory in Kansas City were able to trace Darlene Fischer's messages to a server in Topeka, find Darlene Fischer's email address, and then trace it to a house in Melvern, Kansas. Darlene Fischer's real name was in fact Lisa Montgomery. Montgomery was arrested and subsequently confessed, and baby Victoria Jo Stinnett was found alive—less than 24 hours after she was cut from her mother's womb.

Section 212 was also used to foil an alleged kidnapping plot that turned out to be an extortion racket. Additionally, the provision has been used to successfully respond to a cyberterrorist threat to the South Pole Research Station, a bomb threat to a high school, a threat to kill the employees of a European company as well as their families, and a

threat to burn down an Islamic mosque in Texas. In all of these cases, voluntary disclosures from Internet service providers were critical to apprehending the perpetrators before their threats could be carried out. These are just a few examples of the utility of section 212.

Although section 212 has not been the subject of significant criticism, EFF has complained that computer service providers should not be able to disclose customer records or communications unless a court or grand jury demands them.[24] Requiring that procedure, however, would eliminate the vital benefits provided by section 212. First, section 212 allows a service provider to disclose information voluntarily not only when the government seeks it, but also when the service provider itself becomes aware of an emergency that poses a threat to life and limb. To require a court order or subpoena in such a case would require the service provider first to contact authorities and provide a sufficient basis for authorities to seek such an order, then would require authorities to obtain the order and serve it on the provider, and only then would the critical information be made available. That cumbersome process would waste precious time in an emergency. Second, even in the more usual case where the government seeks information from a service provider in response to an emergency, obtaining a court order or subpoena could still take a significant amount of time. In some emergency situations, even a matter of minutes might mean the difference between life and death. EFF complains that section 212 may result in unnecessary invasions of privacy because an ISP's belief that a life-threatening emergency justifies the disclosure of customer records or communications may turn out to be mistaken. Such mistakes are no doubt bound to happen. However, section 212 requires the ISPs' belief to be a reasonable one,[25] and, in order to save lives, their evaluation of the situation must be made at the time of the emergency and should not be subject to Monday-morning quarterbacking.

Section 214: Pen Register and Trap and Trace Authority under FISA

Text of Section 214:

> (a) APPLICATIONS AND ORDERS- Section 402 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1842) is amended--
>
> > (1) in subsection (a)(1), by striking "for any investigation to gather foreign intelligence information or information concerning international terrorism" and inserting "for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution";

---

[24] *See* Electronic Frontier Foundation, "Let the Sun Set on PATRIOT - Section 212 and Homeland Security Act Section 225: 'Emergency Disclosures of Electronic Communications to Protect Life and Limb'", (Mar. 24, 2004) (available at http://www.eff.org/Privacy/Surveillance/Terrorism/PATRIOT/sunset/212.php).

[25] The relevant standard with respect to the disclosure of communications was changed by the Homeland Security Act from reasonable belief to good-faith belief.

(2) by amending subsection (c)(2) to read as follows:

"(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.";

(3) by striking subsection (c)(3); and

(4) by amending subsection (d)(2)(A) to read as follows:

"(A) shall specify--

`(i) the identity, if known, of the person who is the subject of the investigation;

"(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

"(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order.".

(b) AUTHORIZATION DURING EMERGENCIES- Section 403 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1843) is amended--

(1) in subsection (a), by striking "foreign intelligence information or information concerning international terrorism" and inserting "foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution"; and

(2) in subsection (b)(1), by striking "foreign intelligence information or information concerning international terrorism" and inserting "foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution".

How Current Law Now Reads:

"50 U.S.C. § 1842. Pen registers and trap and trace devices for foreign intelligence and international terrorism investigations

(a) Application for authorization or approval

(1) Notwithstanding any other provision of law, the Attorney General or a designated attorney for the Government may make an application for an order or an extension of an order authorizing or approving the installation and use of a pen register or trap and trace device for any investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution which is being conducted by the Federal Bureau of Investigation under such guidelines as the Attorney General approves pursuant to Executive Order No. 12333, or a successor order.

...

(c) Executive approval; contents of application

...

(2) a certification by the applicant that the information likely to be obtained is foreign intelligence information not concerning a United States person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

...

(d) Ex parte judicial order of approval

...

(2) An order issued under this section--

(A) shall specify--

(i) the identity, if known, of the person who is the subject of the investigation;

(ii) the identity, if known, of the person to whom is leased or in whose name is listed the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied;

(iii) the attributes of the communications to which the order applies, such as the number or other identifier, and, if known, the location of the telephone line or other facility to which the pen register or trap and trace device is to be attached or applied and, in the case of a trap and trace device, the geographic limits of the trap and trace order."

"50 U.S.C. § 1843. Authorization during emergencies

(a) Requirements for authorization

Notwithstanding any other provision of this subchapter, when the Attorney General makes a determination described in subsection (b) of this section, the Attorney General may authorize the installation and use of a pen register or trap and trace device on an emergency basis to gather foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution if--

> (1) a judge referred to in section 1842(b) of this title is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to install and use the pen register or trap and trace device, as the case may be, on an emergency basis; and
>
> (2) an application in accordance with section 1842 of this title is made to such judge as soon as practicable, but not more than 48 hours, after the Attorney General authorizes the installation and use of the pen register or trap and trace device, as the case may be, under this section.
>
> (b) Determination of emergency and factual basis
>
> A determination under this subsection is a reasonable determination by the Attorney General that--
>
> (1) an emergency requires the installation and use of a pen register or trap and trace device to obtain foreign intelligence information not concerning a United States person or information to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution before an order authorizing the installation and use of the pen register or trap and trace device, as the case may be, can with due diligence be obtained under section 1842 of this title[.]"

Analysis:

A pen register is a device that can track routing and addressing information about a communication – for example, which numbers are dialed from a particular telephone. Pen registers, however, are not used to collect the substance of communications. Similarly, a trap-and-trace device tracks numbers used to call a particular telephone, without monitoring the substance of the telephone conversation. Both devices are routinely used in criminal investigations where, in order to obtain the necessary order authorizing use of the device, the government must show simply that the information sought is relevant to an ongoing investigation.

Under FISA, government officials may seek a court order for a pen register or trap-and-trace device to gather foreign intelligence information or information about international terrorism or espionage. Prior to enactment of the USA PATRIOT Act, however, FISA required government personnel to certify not just that the information they sought was relevant to an intelligence investigation, but also that the facilities to be monitored had been used or were about to be used to contact a foreign agent or an agent of a foreign power, such as a terrorist or spy. Thus, it was much more difficult to obtain an effective pen register or trap-and-trace order in an international terrorism investigation than in a criminal investigation.

Section 214 of the USA PATRIOT Act eliminated the provision cabining FISA pen register and trap-and-trace orders to facilities used by foreign agents or those engaged in international terrorist or clandestine intelligence activities, thus bringing authorities for terrorism and other foreign intelligence investigations into line with similar criminal authorities. *See* 50 U.S.C. § 1842(c)(3). Significantly, however, applicants must still certify that the devices are likely to reveal information relevant to a foreign intelligence investigation, such as an international terrorism or espionage investigation. This provision made the standard contained in FISA for obtaining a pen

register or trap-and-trace order parallel with the standard for obtaining a pen register or trap-and-trace order in the criminal context. This section preserved the requirement predicating the government's installation of a pen register on permission from the independent FISA court, which must find that the government's application satisfies the requirements of the Act before it authorizes use of the device.

The Department has applied section 214 to international terrorism and counterintelligence investigations, including a case where the subject was believed to be attempting to procure nuclear arms. In one terrorism case, the only phone that the FBI could prove was used by the subject was his associate's phone. Additionally, the FBI had insufficient information that this associate was an agent of a foreign power. Thus, under the previous standard for a FISA pen register or trap-and-trace order, the FBI may not have succeeded in obtaining a pen register or trap-and-trace order. The standard established by section 214, however, allowed the agents to obtain the order by demonstrating that the information to be collected was relevant to an ongoing terrorism investigation. The information obtained by the order was valuable because it demonstrated the extent that the subject and his associate were communicating with subjects of other terrorism investigations. In another example, section 214 allowed FISA pen-register authority to be obtained based on the fact that information was likely to result in foreign intelligence information. This provision allowed the FBI to collect data on target lines even when the subject was out of the country and provided valuable intelligence information regarding the subject and terrorism-related matters.

Current law requires the Department to "fully inform" the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate on a semi-annual basis concerning all uses of pen register and trap and trace devices pursuant to FISA. It also requires the Department to provide those committees as well as the House and Senate Judiciary Committees a semi-annual report setting forth the total number of applications made for orders approving the use of pen registers or trap-and-trace devices under FISA along with the total number of such orders either granted, modified, or denied. *See* 50 U.S.C. § 1846. The Department transmitted the aforementioned reports to Congress regarding the use of section 214 in April 2002, January 2003, September 2003, December 2003, September 2004, and December 2004.

The Electronic Privacy Information Center has voiced the most common criticism of section 214: that it "significantly eviscerates the constitutional rationale for the relatively lax requirements that apply to foreign intelligence surveillance."[26] This criticism misses the mark; section 214 in fact goes *further* to protect privacy than the U.S. Constitution requires. The Supreme Court has long held that law enforcement is not constitutionally required to obtain court approval before installing a pen register. Under long-settled Supreme Court precedent, the use of pen registers 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." *Smith v. Maryland*, 442 U.S. 735, 744 (1979).

[26] *See* "The USA PATRIOT Act" (available at http://www.epic.org/privacy/terrorism/usapatriot/).

Consequently, the Constitution does not require that law enforcement obtain court approval before installing a pen register. Moreover, section 214 explicitly safeguards First Amendment rights by providing that any "investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution."

Section 215: Access to Records and Other Items Under the Foreign Intelligence Surveillance Act

Text of Section 215:

Title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) is amended by striking sections 501 through 503 and inserting the following:

"SEC. 501. ACCESS TO CERTAIN BUSINESS RECORDS FOR FOREIGN INTELLIGENCE AND INTERNATIONAL TERRORISM INVESTIGATIONS.

(a) (1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall--

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(b) Each application under this section--

(1) shall be made to--

(A) a judge of the court established by section 103(a); or

(B) a United States Magistrate Judge under chapter 43 of title 28, United States Code, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) to protect against international terrorism or clandestine intelligence activities.

(c) (1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

SEC. 502. CONGRESSIONAL OVERSIGHT.

(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 402.
(b) On a semiannual basis, the Attorney General shall provide to the Committees on the Judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period--

(1) the total number of applications made for orders approving requests for the production of tangible things under section 402; and

(2) the total number of such orders either granted, modified, or denied."

How Current Law Now Reads:

"§ 1861. Access to certain business records for foreign intelligence and international terrorism investigations

(a) (1) The Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(b) Each application under this section

(1) shall be made to--

(A) a judge of the court established by section 1803(a) of this title; or

(B) a United States Magistrate Judge under chapter 43 of Title 28, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall specify that the records concerned are sought for an authorized investigation conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities.

(c) (1) Upon an application made pursuant to this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of records if the judge finds that the application meets the requirements of this section.

(2) An order under this subsection shall not disclose that it is issued for purposes of an investigation described in subsection (a).

(d) No person shall disclose to any other person (other than those persons necessary to produce the tangible things under this section) that the Federal Bureau of Investigation has sought or obtained tangible things under this section.

(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

§ 1862. Congressional oversight

(a) On a semiannual basis, the Attorney General shall fully inform the Permanent Select Committee on Intelligence of the House of Representatives and the Select Committee on Intelligence of the Senate concerning all requests for the production of tangible things under section 1861 of this title.

(b) On a semiannual basis, the attorney general shall provide to the committees on the judiciary of the House of Representatives and the Senate a report setting forth with respect to the preceding 6-month period--

(1) the total number of applications made for orders approving requests for the production of tangible things under section 1861 of this title; and

(2) the total number of such orders either granted, modified, or denied."

Analysis:

Prior to the passage of the USA PATRIOT Act, it was difficult for the government to obtain court orders for access to business records and other tangible items in connection with national security investigations. Such records, for example, could be sought from only common carriers, public accommodation providers, physical storage facility operators, and vehicle rental agencies. *See* 50 U.S.C. §§ 1861-1863 (2000 ed.). In addition, intelligence investigators had to meet a much higher evidentiary standard to obtain an order requiring the production of such records than prosecutors had to meet to obtain a grand jury subpoena to require the production of those same records in a criminal investigation. *See id.*

As a result, section 215 of the USA PATRIOT Act made several important changes to the FISA business records authority so that intelligence agents are better able to obtain crucial information in important national security investigations. For example, just as there is no artificial limit to the range of items or types of entities that criminal prosecutors may subpoena, section 215 now allows the FISA Court to issue orders requiring the production of any business record or tangible item, and there is no limitation on the types of entities from which items may be sought. Similarly, just as prosecutors in a criminal case may subpoena any item so long as it is relevant to their investigation, so too may the FISA Court issue an order requiring the production of records or items that are relevant to investigations to protect against international terrorism or clandestine intelligence activities.

Section 215 may be the most widely-criticized provision of the Act. Much of this criticism, however, has resulted from inaccurate characterizations of what is contained in the provision. Critics, for example, have complained that section 215 does not require the government to make any evidentiary showing in order to obtain a court order requiring the production of records. So long as the government certifies that the records are being sought for an international terrorism or espionage investigation, critics contend that the FISA Court has no choice but to issue the requested order.[27]

This portrayal of section 215, however, is categorically false. Pursuant to section 215, a judge "shall" issue an order "approving the release of records if the judge finds that the application meets the requirements of this section." 50 U.S.C. § 1861(c)(1) (emphasis added). As a result, before issuing an order requiring the production of any records under section 215, a federal judge must find that the requested records are sought for (and thus relevant to) "an authorized investigation . . . to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1861(b)(2).

Section 215's opponents also claim that the provision is open to abuse and fishing expeditions because court orders under section 215 are subject to less oversight and a lower burden of proof than are grand jury subpoenas in criminal investigations.[28]

Once again, however, this criticism is completely inaccurate. Section 215 orders, in fact, are subject to greater judicial oversight than are grand jury subpoenas, which prosecutors regularly use to obtain business records in criminal investigations. A court must explicitly authorize the use of section 215 to obtain business records. A grand jury subpoena for such records, by contrast, is typically issued without any prior involvement by a judge. Section 215 orders are similarly subject to greater congressional oversight than are grand jury subpoenas. Every six months, the Attorney General must "fully inform" the House and Senate Intelligence Committees "concerning all requests for the production of tangible things" under section 215. 50 U.S.C. § 1862(a). There is no similar mechanism, however, for congressional oversight of grand jury subpoenas.

---

[27] *See, e.g.*, Letter from Ralph G. Neas, President of People for the American Way, and Marge Baker, Director of Public Policy for People for the American Way, to Members of Congress, July 6, 2004.
[28] *See id.*

Section 215 orders are also subject to the same burden of proof as are grand jury subpoenas -- a relevance standard. Just as grand jury subpoenas may be issued to obtain records that are relevant to a criminal investigation, a court may issue orders requiring the production of records under section 215 that are relevant to an authorized international terrorism or espionage investigation. Some critics have complained that section 215 does not contain a "relevance" standard because the word "relevance" is not specifically mentioned in the provision itself. Section 215, however, states that the FISA Court may only enter an order requiring the production of records if such records are "sought for an authorized investigation conducted in accordance with [50 U.S.C. § 1861(a)(2)] to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities." 50 U.S.C. § 1862(a). This is the equivalent of a relevance standard because if records are irrelevant to an investigation, then they are not being "sought for" that investigation.

Finally, many organizations, including the American Library Association, have attacked section 215 because of its potential application to library records, raising the ominous spectre of Big Brother monitoring Americans' reading habits or Internet usage.[29] The arguments made by these critics, however, do not take into account the safeguards built into the provision, well-established grand jury practice, and the reality of the terrorist threat.

Although a section 215 order could be issued to a library so long as a judge determined that the library possessed records relevant to an international terrorism or espionage investigation, the provision does not single libraries out or even mention them at all; it simply does not exempt libraries from the range of entities that may be required to produce records. This lack of a special exemption for libraries, however, is completely consistent with criminal investigative practice. Prosecutors have always been able to obtain records from bookstores and libraries through grand jury subpoenas. For instance in the 1997 Gianni Versace murder case, a Florida grand jury subpoenaed records from public libraries in Miami Beach. Similarly, in the famed Zodiac gunman investigation, a grand jury in New York subpoenaed library records after investigators came to believe that the gunman was inspired by a Scottish occult poet and wanted to learn who had checked out the poet's books.

The fact that section 215 does not exempt libraries is also wise policy. Libraries should not be carved out as safe havens for terrorists and spies. The Department, for example, has confirmed that as recently as the winter and spring of 2004, a member of a terrorist group closely affiliated with al Qaeda used Internet service provided by a public library to communicate with his confederates. Furthermore, we know that spies have used public library computers to do research to further their espionage and to communicate with their co-conspirators. For example, Brian Regan, a former TRW employee working at the National Reconnaissance Office, who recently was convicted of

[29] *See, e.g.*, Campaign for Reader Privacy, "What is Section 215?" (available at http://www.readerprivacy.com/?mod[type]=learn_more).

espionage, extensively used computers at five public libraries in Northern Virginia and Maryland to access addresses for the embassies of certain foreign governments.

The concern that section 215 somehow allows the government to target Americans because of the books that they read or websites that they visit also misses the mark because the provision explicitly protects First Amendment rights. It provides that an investigation under this section shall "not be conducted of a United States person solely upon the basis of activities protected by the First Amendment to the Constitution of the United States." 50 U.S.C. § 1861(a)(2)(B).

Many critics have also complained that those who receive a section 215 order requiring the production of records are not allowed to tell others that they received the order.[30] Such a nondisclosure requirement, however, is standard operating procedure for the conduct of surveillance in sensitive international terrorism or espionage investigations. As the U.S. Senate concluded when adopting the Foreign Intelligence Surveillance Act: "By its very nature, foreign intelligence surveillance must be conducted in secret."[31] Were information identifying the targets of international terrorism and espionage investigations revealed, according to the U.S. Court of Appeals for the D.C. Circuit, such disclosures would "inform terrorists of both the substantive and geographic focus of the investigation[,] . . . would inform terrorists which of their members were compromised by the investigation, and which were not[,] . . . could allow terrorists to better evade the ongoing investigation and more easily formulate or revise counter-efforts * * * [and] be of great use to al Qaeda in plotting future terrorist attacks or intimidating witnesses in the present investigation."[32] Maintaining the secrecy of such investigations is therefore centrally important to the Department's ability to gather information regarding the activities of international terrorists and hostile foreign adversaries without causing the disclosure of information that would undermine its efforts to prevent further acts of terrorism.

On September 18, 2003, the Attorney General declassified the fact that as of that date, section 215 of the USA PATRIOT Act had not been used. Subsequent information regarding the utilization of section 215 (or lack thereof) remains classified but has been provided to Congress on a semiannual basis as required by 50 U.S.C. § 1862. In particular, the Department has reported to Congress six times on its use of section 215. These reports were transmitted by the Department in April 2002, January 2003, September 2003, December 2003, September 2004, and December 2004.

Some opponents of section 215 have seized on the fact that the provision was not used in the two years following the passage of the USA PATRIOT Act and used it as evidence that the provision is not necessary and should be repealed.[33] The fact that an

---

[30] *See id.*

[31] S. Rep. No. 95-604, 95th Cong. 2d Sess., at 60 (1978).

[32] *Center of National Security Studies v. U.S. Department of Justice*, 331 F.3d 918, 928-29 (D.C. Cir. 2003).

[33] *See* Kim Zetter, "ACLU Chief Assails Patriot Spin" *Wired News* (Sept. 23, 2003) (available at http://www.wired.com/news/conflict/0,2100,60541,00.html?tw=wn_story_related).

authority may be used infrequently, however, does not denigrate its importance; to the contrary, it is important that the authority exists for situations in which a section 215 order could be critical to the success of an investigation. Just as a police officer knows that his firearm may be invaluable in preventing crime, even if he cannot predict when he might need to draw it from his holster, section 215 provides investigators an authority they may find crucial to stop a terrorist plot. The fact that the Department has used this authority in a judicious manner should not be used as an argument for repealing the provision altogether.

Section 217: Interception of Computer Trespasser Communications

Text of Section 217:

Chapter 119 of title 18, United States Code, is amended--

(1) in section 2510--

(A) in paragraph (18), by striking "and" at the end;

(B) in paragraph (19), by striking the period and inserting a semicolon; and

(C) by inserting after paragraph (19) the following:

"(20) 'protected computer' has the meaning set forth in section 1030; and

"(21) 'computer trespasser'--

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer."; and

(2) in section 2511(2), by inserting at the end the following:

"(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser.".

How Current Law Now Reads:

"18 U.S.C. § 2510. Definitions

...

(20) 'protected computer' has the meaning set forth in section 1030; and

(21) 'computer trespasser'--

(A) means a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer; and

(B) does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer."

"18 U.S.C. § 2511. Interception and disclosure of wire, oral, or electronic communications prohibited

...

(i) It shall not be unlawful under this chapter for a person acting under color of law to intercept the wire or electronic communications of a computer trespasser transmitted to, through, or from the protected computer, if--

(I) the owner or operator of the protected computer authorizes the interception of the computer trespasser's communications on the protected computer;

(II) the person acting under color of law is lawfully engaged in an investigation;

(III) the person acting under color of law has reasonable grounds to believe that the contents of the computer trespasser's communications will be relevant to the investigation; and

(IV) such interception does not acquire communications other than those transmitted to or from the computer trespasser."

Analysis:

Although the criminal wiretap statute ("Title III") allows computer service providers to monitor activity on their machines to protect their rights and property, prior to the passage of the USA PATRIOT Act, it was unclear whether computer owners could obtain law enforcement assistance in conducting such monitoring. This lack of clarity prevented law enforcement from assisting victims in taking reasonable steps in their own

defense that would be entirely legal in the physical world. In the physical world, for example, burglary victims may invite the police into their homes to help them catch burglars in the act of committing the crime. Before the USA PATRIOT Act, however, Title III arguably blocked investigators from responding to similar requests from computer service providers in the electronic context. Because service providers often lacked the expertise, equipment, or financial resources required to monitor hacker attacks, they commonly had no effective way to protect themselves from such attacks. This anomaly in the law created the bizarre result that a computer hacker's supposed "privacy" right trumped the privacy rights of his victims.

To correct this problem, section 217 of the USA PATRIOT Act clarified that victims of computer attacks may authorize persons "acting under color of law" to monitor trespassers on their computer systems. Under section 217, law enforcement can intercept the communications of a computer trespasser transmitted to, through, or from a "protected computer"[34] – basically, a federal government computer or a computer that is used in or affects interstate or foreign commerce or communication – so long as four requirements are met. First, the owner or operator of the protected computer must authorize the interception of the trespasser's communications. 18 U.S.C. § 2511(2)(i)(I). Second, the person who intercepts the communication must be lawfully engaged in an ongoing investigation, but the authority to intercept ceases at the conclusion of the investigation. 18 U.S.C. § 2511(2)(i)(II). Third, the person acting under color of law must have reasonable grounds to believe that the contents of the communication to be intercepted will be relevant to the ongoing investigation. 18 U.S.C. § 2511(2)(i)(III). Fourth, investigators may intercept only the communications sent or received by trespassers. Thus, this section applies only where the configuration of the computer system allows the interception of communications to and from the trespasser, and not the interception of communications to or from non-consenting authorized users. 18 U.S.C. § 2511(2)(i)(IV).

In addition, section 217 amended the wiretap statute to create a definition of "computer trespasser." Pursuant to the provision, a computer trespasser is any person who accesses a protected computer without authorization. The definition, however, explicitly excludes any person "known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator for access to all or part of the computer." 18 U.S.C. § 2510(21). This exemption provides important privacy protections for the customers of Internet service provider ("ISPs"). For example, certain ISPs do not allow their customers to send bulk unsolicited e-mails ("spam"). Customers who send spam would be in violation of the provider's terms of

---

[34] Section 217 adopted the same definition of the term "protected computer" as is specified in 18 U.S.C. § 1030. 18 U.S.C. § 1030(e)(2), in turn, defines "protected computer" to mean a computer—

"(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States."

service, but do not qualify as trespassers – both because they are authorized users and because they have an existing contractual relationship with the provider.

As explained above, these changes simply brought the law relating to cyber-trespassing in line with the law relating to physical trespassing. Just as in the physical world victims of burglary may call the police to enter their home to catch an intruder, so too under section 217 may victims of hacking and cyber-terrorism now obtain law enforcement assistance in catching intruders on their systems.

Section 217 has played a key role to date in sensitive national security matters, including investigations into hackers' attempts to compromise military computer systems. The provision has also been used to uncover serious criminal conduct. For example, in an investigation into an international conspiracy to use stolen credit cards to fraudulently purchase stolen goods and ship them overseas, FBI agents discovered that members of the conspiracy had illegally accessed a computer in Texas and used it to communicate with each other. Pursuant to section 217, the computer owner requested that the agents monitor the trespassers to identify them and determine how they broke in. Monitoring of the criminals' communications revealed useful evidence about the criminal scheme and has led to an indictment for conspiracy to commit fraud.

Section 217 has provoked some opposition from privacy advocates. The Electronic Privacy Information Center, for example, has criticized section 217, claiming that it:

> places the determination [of whether to permit government access to and interception of communications] solely in the hands of law enforcement and the system owner or operator. In those likely instances in which the interception does not result in prosecution, the target of the interception will never have an opportunity to challenge the activity (through a suppression proceeding). Indeed, such targets would never even have notice of the fact that their communications were subject to warrantless interception. However, the USA PATRIOT Act does include an exception prohibiting surveillance of someone who is known by the owner of the protected computer "to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer." The [never-introduced Anti-Terrorism Act bill], which did not contain such an exception, was so vague that the provision could have been applied to users downloading copyrighted materials off the Web. However, even with this fix, the amendment has little, if anything, to do with legitimate investigations of terrorism.[35]

Similarly, EFF claims that the section, which it asserts has "no apparent connection to preventing terrorism," permits "[g]overnment spying on suspected computer trespassers with no need for court order."[36] Finally, CDT has criticized the Department's

---

[35] *See supra* note 3.

[36] *See* "EFF Analysis of USA PATRIOT Act" (Oct. 31, 2001) (available at http://www.eff.org/Privacy/Surveillance/Terrorism/20011031_eff_usa_patriot_analysis.php).

comparison of physical trespassing and computer trespassing, asserting that section 217 "is a far cry from burglary victims being able to invite [police] officers into their homes to catch burglars, as DOJ argues. Under those circumstances, the burglar is well aware that the victim thinks the burglar is trespassing and that the police are investigating - and has the full panoply of protections available in the criminal system. Anyone designated a computer trespasser has no such rights or knowledge."[37]

All of these objections are seriously misplaced. To begin with, when homeowners seek the police's assistance in detecting and apprehending physical trespassers, there is no obligation whatsoever to notify or warn those trespassers that the police have begun an investigation or are physically present on the trespassed property, and the CDT's suggestion to the contrary is simply incorrect. Moreover, a trespasser, whether a computer trespasser or a physical trespasser, has no reasonable expectation of privacy precisely because he or she is a trespasser, and thus has no legitimate privacy rights that merit or receive legal recognition

As stated above, section 217 appropriately places computer owners' privacy rights above the non-existent "privacy" rights of trespassers. Computer operators are not required to involve law enforcement if they detect trespassers on their systems. Section 217 simply gives them the option of doing so. Moreover, it is worth noting that section 217 also preserves the privacy of law-abiding computer users. Officers cannot agree to help a computer owner unless (1) they are intercepting the communications of a computer trespasser; (2) they obtain the permission of the owner or operator of the computer through which the communications have traveled; (3) they are engaged in a lawful investigation; (4) there is reason to believe that the communications will be relevant to that investigation; and (5) their activities will not acquire the communications of non-trespassers.

Section 218: Foreign Intelligence Information

Text of Section 218:

> Sections 104(a)(7)(B) and section 303(a)(7)(B) (50 U.S.C. 1804(a)(7)(B) and 1823(a)(7)(B)) of the Foreign Intelligence Surveillance Act of 1978 are each amended by striking "the purpose" and inserting "a significant purpose".

How Current Law Now Reads:

> **"§ 1804. Applications for court orders**
>
> (a) Submission by Federal officer; approval of Attorney General; contents
>
> Each application for an order approving electronic surveillance under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 1803 of this title. Each application shall require the approval of the Attorney General based

[37] Center for Democracy & Technology, "Setting the Record Straight" (Oct. 27, 2003) (available at http://www.cdt.org/security/usapatriot/031027cdt.shtml).

upon his finding that it satisfies the criteria and requirements of such application as set forth in this subchapter. It shall include—

. . .

(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate--

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and

(E) including a statement of the basis for the certification that--

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques."

"§ 1823. Application for order

(a) Submission by Federal officer; approval of Attorney General; contents

Each application for an order approving a physical search under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge of the Foreign Intelligence Surveillance Court. Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements for such application as set forth in this subchapter. Each application shall include--

. . .

(7) a certification or certifications by the Assistant to the President for National Security Affairs or an executive branch official or officials designated by the President from among those executive branch officers employed in the area of national security or defense and appointed by the President, by and with the advice and consent of the Senate-

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the search is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and

(E) includes a statement explaining the basis for the certifications required by subparagraphs (C) and (D);

Analysis:

Before the passage of the USA PATRIOT Act, a metaphorical "wall" largely separated intelligence personnel from law enforcement personnel within the federal government. This "wall" dramatically limited vital information sharing and greatly hindered the Department's counterterrorism efforts.

The origins of this "wall" can be traced back to the pre-USA PATRIOT Act requirement that applications for orders authorizing electronic surveillance or physical searches under FISA had to include a certification from a high-ranking Executive Branch official that "*the* purpose" of the surveillance or search was to gather foreign intelligence information. As interpreted by the courts and later the Justice Department, this requirement meant that the "primary purpose" of the collection had to be to obtain foreign intelligence information rather than evidence of a crime. Over the years, the prevailing interpretation and implementation of the "primary purpose" standard had the effect of sharply limiting coordination and information sharing between intelligence and law enforcement personnel. Because the courts evaluated the government's purpose for using FISA at least in part by examining the nature and extent of coordination between intelligence and law enforcement officials, the more coordination that occurred, the more likely courts would find that law enforcement, rather than foreign intelligence, had become the primary purpose of the surveillance or search.

During the 1980s, the Department operated under a set of largely unwritten rules that limited to some degree information sharing between intelligence and law enforcement officials. In 1995, however, the Department established formal procedures that more clearly separated law enforcement and intelligence investigations and limited the sharing of information between intelligence and law enforcement personnel more than the law required. The promulgation of these procedures was motivated in part by the concern that the use of FISA authorities would not be allowed to continue in particular investigations if criminal prosecution began to overcome intelligence gathering as an investigation's primary purpose. To be sure, the procedures were intended to permit a degree of interaction and information sharing between prosecutors and intelligence officers, while at the same time ensuring that the FBI would be able to obtain or continue FISA coverage and later use the fruits of that coverage in a criminal prosecution. Over time, however, coordination and information sharing between intelligence and law enforcement investigators became even more limited in practice than was allowed in theory under the Department's procedures. Due both to confusion about when sharing was permitted and to a perception that improper information sharing could end a career, a culture developed within the Department sharply limiting the exchange of information between intelligence and law enforcement officials.

Section 218 of the USA PATRIOT Act, however, helped to bring down the perceived "wall" separating intelligence agents from law enforcement agents. It not only

erased the impediment to more robust information sharing between intelligence and law enforcement personnel; it also provided the necessary impetus for the removal of the formal administrative restrictions as well as the informal cultural restrictions on information sharing.

Section 218 did this by eliminating the "primary purpose" requirement. Under section 218 of the USA PATRIOT Act, the government may now conduct FISA surveillance or searches if foreign-intelligence gathering is a "significant" purpose of the surveillance or search, thus eliminating the need for courts to compare the relative weight of the "foreign intelligence" and "law enforcement" purposes of the surveillance or search. This has allowed for significantly more coordination and sharing of information between intelligence and law enforcement personnel.

FISA contains ample safeguards to ensure that innocent Americans are not subject to government surveillance. First, under section 218, the government may conduct a physical search or electronic surveillance under FISA only if a significant purpose of the search is to obtain foreign intelligence information. And second, the government must have probable cause to believe that the target of a FISA physical search or electronic surveillance is a foreign power or agent of a foreign power, such as a terrorist or spy.

The Department has moved aggressively to implement section 218 and bring down "the wall." Following passage of the Act, the Department adopted new procedures designed to increase information sharing between intelligence and law enforcement agents, which were affirmed by the Foreign Intelligence Surveillance Court of Review on November 18, 2002. The Attorney General also instructed every U.S. Attorney to review intelligence files to discover whether there was a basis for bringing criminal charges against the subjects of intelligence investigations. Thousands of files have been reviewed as part of this process. The Attorney General likewise 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 in those investigations.

The increased coordination and information sharing between intelligence and law enforcement personnel facilitated by section 218 has allowed the FBI to approach terrorism investigations not as separate criminal and intelligence investigations, each with separate agents developing separate information and evidence on parallel tracks, but as a single integrated investigation that enables us to "connect the dots." In the course of a terrorism investigation, agents can now use all the tools in the toolbox, utilizing both criminal investigative tools and intelligence tools, as long as the requirements for each are properly met. This approach has yielded extraordinary dividends, enabling the Department to open numerous criminal investigations, disrupt terrorist plots, bring numerous criminal charges, and convict numerous individuals in terrorism cases.

For example, the removal of the "wall" separating intelligence and law enforcement personnel played a crucial role in the Department's successful dismantling of a Portland, Oregon terror cell, popularly known as the "Portland Seven." Members of

this terror cell had attempted to travel to Afghanistan in 2001 and 2002 to take up arms with the Taliban and al Qaeda against United States and coalition forces fighting there. Law enforcement agents investigating that case learned from one member of the terror cell, Jeffrey Battle, through an undercover informant, that before the plan to go to Afghanistan was formulated, at least one member of the cell had contemplated attacking Jewish schools or synagogues and had even been casing such buildings to select a target for such an attack. By the time investigators received this information from the undercover informant, they had information that a number of other persons besides Battle had been involved in the Afghanistan conspiracy. But while several of these other individuals had returned to the United States from their unsuccessful attempts to reach Afghanistan, investigators did not yet have sufficient evidence to arrest them.

Before the USA PATRIOT Act, prosecutors would have faced a dilemma in deciding whether to arrest Battle immediately. If prosecutors had failed to act, lives could have been lost through a terrorist attack. But if prosecutors had arrested Battle in order to prevent a potential attack, the other suspects in the investigation would have undoubtedly scattered or attempted to cover up their crimes. Because of section 218, however, it was clear that the FBI agents could conduct FISA surveillance of Battle to detect whether he had received orders from an international terrorist group to reinstate the domestic attack plan on Jewish targets and keep prosecutors informed as to what they were learning. This gave prosecutors the confidence not to arrest Battle prematurely while they continued to gather evidence on the other members of the cell. Ultimately, prosecutors were able to collect sufficient evidence to charge seven defendants and then to secure convictions and prison sentences ranging from three to eighteen years for the six defendants taken into custody. Without section 218, this case likely would have been referred to as the "Portland One" rather than the Portland Seven.

Likewise, the Department shared information pursuant to section 218 before indicting Sami Al-Arian and several co-conspirators on charges related to their involvement with the Palestinian Islamic Jihad (PIJ). PIJ is alleged to be one of the world's most violent terrorist outfits. It 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. The indictment details that Al-Arian served as the secretary of the Palestinian Islamic Jihad's governing council ("Shura Council"). He was also identified as the senior North American representative of the PIJ.

In this case, section 218 of the USA PATRIOT Act enabled prosecutors to consider all evidence against Al-Arian and his co-conspirators, including evidence obtained pursuant to FISA that provided the necessary factual support for the criminal case. By considering the intelligence and law enforcement information together, prosecutors were able to create a complete history for the case and put each piece of evidence in its proper context. This comprehensive approach was essential to enabling prosecutors to build their case and pursue the proper charges. The trial in this case is currently scheduled to start later this year.

Prosecutors and investigators also used information shared pursuant to section 218 in investigating the defendants in the so-called "Virginia Jihad" case. This

prosecution involved members of the Dar al-Arqam Islamic Center, who trained for jihad in Northern Virginia by participating in paintball and paramilitary training, including eight individuals who traveled to terrorist training camps in Pakistan or Afghanistan between 1999 and 2001. These individuals are associates of a violent Islamic extremist group known as Lashkar-e-Taiba (LET), which operates in Pakistan and Kashmir, and that has ties to the al Qaeda terrorist network. As the result of an investigation that included the use of information obtained through FISA, prosecutors were able to bring charges against these individuals. Six of the defendants have pleaded guilty, and three were convicted in March 2004 of charges including conspiracy to levy war against the United States and conspiracy to provide material support to the Taliban. These nine defendants received sentences ranging from a prison term of four years to life imprisonment.

Moreover, the information sharing between intelligence and law enforcement personnel made possible by section 218 was useful in the investigation of two Yemeni citizens, Mohammed Ali Hasan Al-Moayad and Mohshen Yahya Zayed, who were charged in 2003 with conspiring to provide material support to al Qaeda and HAMAS. The complaint against these two individuals alleges that an FBI undercover operation developed information that Al-Moayad boasted that he had personally handed Usama Bin Laden $20 million from his terrorist fund-raising network and that Al-Moayad and Zayed flew from Yemen to Frankfurt, Germany in 2003 with the intent to obtain $2 million from a terrorist sympathizer (portrayed by a confidential informant) who wanted to fund al Qaeda and HAMAS. During their meetings, Al-Moayad and Zayed specifically promised the donor that his money would support HAMAS, al Qaeda, and any other mujahideen, and "swore to Allah" that they would keep their dealings secret. Following their indictment, Al-Moayad and Zayed were extradited to the United States from Germany, and both were convicted in March 2005 of conspiring to provide material support to a foreign terrorist organization.

In addition, the Department used section 218 to gain access to intelligence, which facilitated the indictment of Enaam Arnaout, the Executive Director of the Illinois-based Benevolence International Foundation (BIF). Arnaout conspired to fraudulently obtain charitable donations in order to provide financial assistance to Chechen rebels and organizations engaged in violence and terrorism. Arnaout had a long-standing relationship with Usama Bin Laden and used his charity organization both to obtain funds illicitly from unsuspecting Americans for terrorist organizations, such as al Qaeda, and to serve as a channel for people to contribute money knowingly to such groups. Arnaout ultimately pleaded guilty to a racketeering charge, admitting that he diverted thousands of dollars from BIF to support Islamic militant groups in Bosnia and Chechnya. He was sentenced to over 11 years in prison.

The broader information sharing made possible by section 218 also assisted the prosecution in San Diego of several persons involved in an al Qaeda drugs-for-weapons plot, which culminated in two guilty pleas. Two defendants, Muhamed Abid Afridi and Ilyas Ali, admitted that they conspired to distribute approximately five metric tons of hashish and 600 kilograms of heroin originating in Pakistan to undercover United States law enforcement officers. Additionally, they admitted that they conspired to receive, as

partial payment for the drugs, four "Stinger" anti-aircraft missiles that they then intended to sell to the Taliban, an organization they knew at the time to be affiliated with al Qaeda. Afridi and Ali pleaded guilty to the felony charges of conspiracy to provide material support to terrorists and conspiracy to distribute heroin and hashish The lead defendant in the case is currently awaiting trial.

Finally, section 218 was critical in the successful prosecution of Khaled Abdel Latif Dumeisi, who was convicted by a jury in January 2004 of illegally acting as an agent of the former government of Iraq as well as two counts of perjury. Before the Gulf War, Dumeisi passed information on Iraqi opposition members located in the United States to officers of the Iraqi Intelligence Service stationed in the Iraqi Mission to the United Nations. During this investigation, intelligence agents conducting surveillance of Dumeisi pursuant to FISA coordinated and shared information with law enforcement agents and prosecutors investigating Dumeisi for possible criminal violations. Because of this coordination, law enforcement agents and prosecutors learned from intelligence agents of an incriminating telephone conversation that took place in April 2003 between Dumeisi and a co-conspirator. This phone conversation corroborated other evidence that Dumeisi was acting as an agent of the Iraqi government and provided a compelling piece of evidence at his trial.

As evidenced by these examples and many others, section 218 has been crucial to the success of the Department's efforts in the war against terrorism by allowing for the full coordination between intelligence and law enforcement that is necessary to conduct an integrated counterterrorism effort.

Notwithstanding section 218's importance to the fight against terrorism, this provision has been the subject of criticism. The ACLU, for example, has complained that section 218 allows the FBI to circumvent constitutional safeguards by conducting a search or wiretap for the purpose of investigating a crime without demonstrating probable cause that a crime has been committed.[38] That is incorrect. In 2002, the FISA Court of Review found that section 218 was constitutional; that Court squarely held "that FISA as amended [by the USA PATRIOT Act] is constitutional because the surveillances it authorizes are reasonable." *In re Sealed Case*, 310 F.3d 717, 746 (FISCR 2002).

The ACLU also predicted at the time of the USA PATRIOT Act's passage: "courts will exclude the evidence gathered from surveillance conducted under [s]ection 218 because the probable cause of crime requirement was not met for a search conducted primarily to gather evidence of crime."[39] Experience, however, has revealed that this criticism of section 218 is without merit. In the first place, the Department is unaware of a single case where evidence gathered from FISA surveillance authorized pursuant to section 218 has been excluded from any criminal case on the grounds identified by the

[38] "How the Anti-Terrorism Bill Enables Law Enforcement to Use Intelligence Authorities to Circumvent the Privacy Protections Afforded in Criminal Cases", (Oct. 23, 2001) (available at http://www.asata.org/resources/articles/civil_rights/ACLU_loss_of_privacy.pdf).
[39] *Id.*

ACLU. Indeed, such evidence has been extremely important at trial in many of the criminal cases discussed above.

Many of the criticisms of section 218 are based on a false dichotomy, which strictly separates obtaining foreign intelligence information from gathering evidence for use in a criminal trial. Such a dichotomy, however, represents the same pre-9/11 mindset that led to the creation of the "wall" separating intelligence and law enforcement personnel, which prevented the sharing of valuable information. As the FISA Court of Review noted, for instance, "the definition of foreign intelligence information includes evidence of crimes such as espionage, sabotage or terrorism." *In re Sealed Case*, 310 F.3d 717, 723 (FISCR 2002). The Court therefore concluded that it is "virtually impossible" to read FISA "to exclude from its purpose the prosecution of foreign intelligence crimes." *Id* at 724. Indeed, the Court explained that "arresting and prosecuting terrorist agents of, or spies for, a foreign power may well be the best technique to prevent them from successfully continuing their terrorist or espionage activity." *Id.* The government after all does not obtain intelligence for the sake of gathering intelligence. Rather, it gathers intelligence, among other reasons, to disrupt terrorist plots, and one of the best ways to prevent terrorist acts is to arrest and prosecute terrorists before they are able to strike.

Section 220: Out-of-District Service of Search Warrants for Electronic Evidence

Text of Section 220:

> (a) IN GENERAL- Chapter 121 of title 18, United States Code, is amended--
>
> > (1) in section 2703, by striking "under the Federal Rules of Criminal Procedure" every place it appears and inserting "using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation"; and
> >
> > (2) in section 2711--
> >
> > > (A) in paragraph (1), by striking "and";
> > >
> > > (B) in paragraph (2), by striking the period and inserting "; and"; and
> > >
> > > (C) by inserting at the end the following:
> > >
> > > "(3) the term `court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation.".

How Current Law Now Reads:

"§ 2703. Required disclosure of customer communications or records

(a) Contents of wire or electronic communications in electronic storage.--A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, **only pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation** or equivalent State warrant. A governmental entity may require the disclosure by a provider of electronic communications services of the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than one hundred and eighty days by the means available under subsection (b) of this section.

(b) Contents of wire or electronic communications in a remote computing service.—

(1) A governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication to which this paragraph is made applicable by paragraph (2) of this subsection--

(A) without required notice to the subscriber or customer, if the governmental entity obtains **a warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation** or equivalent State warrant; or

(B) with prior notice from the governmental entity to the subscriber or customer if the governmental entity--

(i) uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena; or

(ii) obtains a court order for such disclosure under subsection (d) of this section; except that delayed notice may be given pursuant to section 2705 of this title.

(2) Paragraph (1) is applicable with respect to any wire or electronic communication that is held or maintained on that service--

(A) on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such remote computing service; and

(B) solely for the purpose of providing storage or computer processing services to such subscriber or customer, if the provider is not authorized to access the contents of any such communications for purposes of providing any services other than storage or computer processing.

(c) Records concerning electronic communication service or remote computing service.—

(1) A governmental entity may require a provider of electronic communication service or remote computing service to disclose a record or other information pertaining to a

subscriber to or customer of such service (not including the contents of communications) only when the governmental entity--

(A) obtains a **warrant issued using the procedures described in the Federal Rules of Criminal Procedure by a court with jurisdiction over the offense under investigation** or equivalent State warrant;

(B) obtains a court order for such disclosure under subsection (d) of this section;

(C) has the consent of the subscriber or customer to such disclosure; or

(D) submits a formal written request relevant to a law enforcement investigation concerning telemarketing fraud for the name, address, and place of business of a subscriber or customer of such provider, which subscriber or customer is engaged in telemarketing (as such term is defined in section 2325 of this title); or

(E) seeks information under paragraph (2).

(2) A provider of electronic communication service or remote computing service shall disclose to a governmental entity the--

(A) name;

(B) address;

(C) local and long distance telephone connection records, or records of session times and durations;

(D) length of service (including start date) and types of service utilized;

(E) telephone or instrument number or other subscriber number or identity, including any temporarily assigned network address; and

(F) means and source of payment for such service (including any credit card or bank account number),

of a subscriber to or customer of such service when the governmental entity uses an administrative subpoena authorized by a Federal or State statute or a Federal or State grand jury or trial subpoena or any means available under paragraph (1).

(3) A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer."

"§ 2711. Definitions for chapter

As used in this chapter--

. . .

(3) the term 'court of competent jurisdiction' has the meaning assigned by section 3127, and includes any Federal court within that definition, without geographic limitation."

Analysis:

Federal law requires investigators to use a search warrant to compel an Internet service provider to disclose unopened e-mail messages that are less than six months old.

See 18 U.S.C. § 2703(a). But because Rule 41 of the Federal Rules of Criminal Procedure requires that the "property" to be obtained through a search warrant be located "within the district" of the issuing court, some courts, prior to the passage of the USA PATRIOT Act, declined to issue warrants for e-mail stored on computer servers located in other judicial districts. For example, in a murder investigation centered in Massachusetts, law enforcement officials, in order to obtain e-mail stored on an ISP's server in the Silicon Valley, were not allowed to obtain a search warrant from a judge in Massachusetts but rather were forced to seek a search warrant in California.

Not only did this requirement deprive the judges most knowledgeable about a particular case of the ability to evaluate search warrant requests, forcing judges and prosecutors with little or no knowledge of an investigation to process search warrants, but it also placed an enormous administrative burden on those districts in which major ISPs are located, such as the Northern District of California and the Eastern District of Virginia. Before the USA PATRIOT Act, these districts were inundated with search warrant requests for electronic evidence. For example, before the enactment of the USA PATRIOT Act, the U.S. Attorney's Office in Alexandria, Virginia was receiving approximately 10 applications each month from United States Attorney's Offices in other districts for search warrants for records from a particular ISP. For each of these applications, an Assistant United States Attorney in Virginia and a law enforcement agent in the district had to learn all of the details of another district's investigation to present an affidavit to the court in support of the application for the search warrant. The result was that agents and attorneys spent many hours each month processing applications for investigations conducted in other districts rather than working on cases involving crimes occurring within their district. In addition, requiring investigators to go through the aforementioned process of seeking warrants to obtain electronic evidence in distant jurisdictions often slowed time-sensitive investigations.

Section 220 of the USA PATRIOT Act solved these problems by allowing courts with jurisdiction over a particular investigation to order the release of stored communications relevant to that investigation through a search warrant valid in another specified judicial district. Therefore, for example, in the investigation of a murder occurring in Pennsylvania, a federal judge in Pennsylvania now may issue a search warrant for e-mail messages pertaining to the investigation that are stored on a server in California.

This enhanced ability to obtain electronic evidence efficiently has been used by the Department on a frequent basis and proved helpful in several terrorism investigations as well as time-sensitive criminal investigations. For example, as Assistant Attorney General Chris Wray testified before the Senate Judiciary Committee on October 21, 2003, section 220 was useful in the Portland terror cell case because "the judge who was most familiar with the case was able to issue the search warrants for the defendants' e-mail accounts from providers in other districts, which dramatically sped up the investigation and reduced all sorts of unnecessary burdens on other prosecutors, agents and courts." Section 220 was also helpful in the investigations of a Northern Virginia terror cell and the infamous "shoebomber" Richard Reid.

The provision was also used in a time-sensitive investigation involving a fugitive, who after abducting his estranged wife and sexually assaulting her, fled West Virginia in a stolen car to avoid capture armed with a sawed-off shotgun. While in flight, he continued to contact cooperating individuals by e-mail using an ISP located in California. Using the authority provided by section 220, investigators in West Virginia were able to quickly obtain an order from a federal court in West Virginia for the disclosure of information regarding the armed fugitive's e-mail account, rather than wasting additional time obtaining such an order from a California court. Within a day of the order being issued, the ISP had released information to the government revealing that the fugitive had contacted individuals from a public library in a small town in South Carolina. The very next day, Deputy U.S. Marshals went to the town and arrested the fugitive. In this case, the fast turn-around on the order for information related to the fugitive's e-mail account made possible by section 220 was crucial to capturing the fugitive.

In addition to allowing law enforcement to gain access to information quickly in time-sensitive investigations, section 220 has significantly improved the Justice Department's ability to mount large-scale child-pornography investigations. The ability to obtain search warrants in the jurisdiction of a child-pornography investigation rather than in the jurisdiction of the Internet service provider is critical to the success of a complex, multi-jurisdictional child-pornography case. In the absence of section 220, law enforcement agents would either have to spend hours briefing other agents across the country to obtain warrants or travel hundreds or thousands of miles to present a warrant application to a local magistrate judge. In practice, one of two things would often occur in light of limited law enforcement resources: either the scope of the investigation would be narrowed or the case would be deemed impractical at the outset and dropped.

Finally, section 220 has eased the administrative burden on U.S. Attorney's Offices and courts that are located in districts that are home to ISPs. Now, investigators and prosecutors in those districts, such as the Northern District of California and Eastern District of Virginia, can spend their time handling cases involving crimes committed in their home districts rather than spending their time getting up to speed and handling requests for search warrants necessary to obtain electronic evidence pertaining to investigations being conducted by other U.S. Attorney's Offices.

While section 220 has not generated a significant amount of criticism, some privacy advocates have opposed its renewal for two reasons. First, they claim that the provision allows law enforcement officers to pick and choose the courts in which they will seek warrants, thus allowing them to "shop" for judges with a pro-law enforcement bias.[40] This criticism, however, reflects a fundamental misunderstanding of section 220. Section 220 does not allow investigators to seek search warrants for electronic evidence from any court in the country. Rather, it allows investigators to seek a search warrant only in a court with jurisdiction over the offense under investigation. Thus, for example,

[40] *See* Electronic Frontier Foundation, "Let the Sun Set on PATRIOT - Section 220: 'Nationwide Service of Search Warrants for Electronic Evidence" (Mar. 16, 2004) (available at http://www.eff.org/Privacy/Surveillance/Terrorism/PATRIOT/sunset/220.php).

while a court in Ohio may issue a search warrant for electronic evidence stored in California in the investigation of a murder committed in Ohio, a judge located in a district with no connection to the investigation, such as North Dakota, is not allowed to issue such a warrant. In practice, judges and prosecutors with the most knowledge of a particular investigation are now permitted to process requests for search warrants to obtain electronic evidence in that investigation.

Second, critics such as the EPIC allege that section 220 reduces the chances that Internet service providers will seek to challenge search warrants for electronic evidence.[41] According to them, a Virginia ISP is less likely to go through the additional time and expense of challenging a search warrant issued by a judge in Oregon than one issued by a judge in Virginia. This argument is flawed for several reasons. To begin with, the nationwide reach of search warrants issued pursuant to section 220 is no different than the nationwide reach of grand jury subpoenas that are issued in federal criminal investigations. Therefore, just as a Virginia company receiving a subpoena from an Oregon grand jury must challenge that subpoena in Oregon, so too must a Virginia ISP receiving a search warrant issued by a federal judge in Oregon challenge that warrant in Oregon. The latter case, in fact, should be far less troubling to privacy advocates as grand jury subpoenas do not require prior judicial approval while search warrants do require such approval. Moreover, since the passage of section 220, the Justice Department has not observed any noticeable decrease in the frequency of instances in which search warrants for electronic evidence have been challenged by ISPs, which rarely challenged such warrants prior to the passage of the Act. This is not surprising as the most popular ISPs are sufficiently large that any additional expense from challenging a search warrant issued by a judge in another district does not constitute a significant deterrent. Indeed, the Justice Department is not aware of any complaints from Internet service providers regarding section 220.

Section 223: Civil Liability for Certain Unauthorized Disclosures

Text of Section 223:

> (a) Section 2520 of title 18, United States Code, is amended--
>
> (1) in subsection (a), after "entity", by inserting ", other than the United States,";
>
> (2) by adding at the end the following:
>
> "(f) ADMINISTRATIVE DISCIPLINE- If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector

[41] *See id.*

General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination."; and

(3) by adding a new subsection (g), as follows:

"(g) IMPROPER DISCLOSURE IS VIOLATION- Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a)."

(b) Section 2707 of title 18, United States Code, is amended--

(1) in subsection (a), after "entity", by inserting ", other than the United States,";

(2) by striking subsection (d) and inserting the following:

"(d) ADMINISTRATIVE DISCIPLINE- If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination."; and

(3) by adding a new subsection (g), as follows:

"g) IMPROPER DISCLOSURE- Any willful disclosure of a 'record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter.".

(c)(1) Chapter 121 of title 18, United States Code, is amended by adding at the end the following:

"Sec. 2712. Civil actions against the United States

(a) IN GENERAL- Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages--

(1) actual damages, but not less than $10,000, whichever amount is greater; and

(2) litigation costs, reasonably incurred.

(b) PROCEDURES-

(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.'.

(3) Any action under this section shall be tried to the court without a jury.

(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

(c) ADMINISTRATIVE DISCIPLINE- If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the possible violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(d) EXCLUSIVE REMEDY- Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

(e) STAY OF PROCEEDINGS-

(1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

(2) In this subsection, the terms `related criminal case' and `related investigation' mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall

consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.

(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party.'"

(2) The table of sections at the beginning of chapter 121 is amended to read as follows:

"2712. Civil action against the United States.".

How Current Law Now Reads:

"18 U.S.C. § 2520. Recovery of civil damages authorized

...

(a) In general.--Except as provided in section 2511(2)(a)(ii), any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

...

(f) Administrative discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(g) Improper disclosure is violation.--Any willful disclosure or use by an investigative or law enforcement officer or governmental entity of information beyond the extent permitted by section 2517 is a violation of this chapter for purposes of section 2520(a)."

"18 U.S.C. § 2707. Civil action

(a) Cause of action.--Except as provided in section 2703(e), any provider of electronic communication service, subscriber, or other person aggrieved by any violation of this chapter in which the conduct constituting the violation is engaged in with a knowing or intentional state of mind may, in a civil action, recover from the person or entity, other than the United States, which engaged in that violation such relief as may be appropriate.

...

(d) Administrative discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved

determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

...

(g) Improper disclosure.--Any willful disclosure of a 'record', as that term is defined in section 552a(a) of title 5, United States Code, obtained by an investigative or law enforcement officer, or a governmental entity, pursuant to section 2703 of this title, or from a device installed pursuant to section 3123 or 3125 of this title, that is not a disclosure made in the proper performance of the official functions of the officer or governmental entity making the disclosure, is a violation of this chapter. This provision shall not apply to information previously lawfully disclosed (prior to the commencement of any civil or administrative proceeding under this chapter) to the public by a Federal, State, or local governmental entity or by the plaintiff in a civil action under this chapter."

"**18 U.S.C. § 2712. Civil actions against the United States**

(a) In general.--Any person who is aggrieved by any willful violation of this chapter or of chapter 119 of this title or of sections 106(a), 305(a), or 405(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.) may commence an action in United States District Court against the United States to recover money damages. In any such action, if a person who is aggrieved successfully establishes such a violation of this chapter or of chapter 119 of this title or of the above specific provisions of title 50, the Court may assess as damages--

(1) actual damages, but not less than $10,000, whichever amount is greater; and

(2) litigation costs, reasonably incurred.

(b) Procedures.—

(1) Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

(2) Any action against the United States under this section shall be forever barred unless it is presented in writing to the appropriate Federal agency within 2 years after such claim accrues or unless action is begun within 6 months after the date of mailing, by certified or registered mail, of notice of final denial of the claim by the agency to which it was presented. The claim shall accrue on the date upon which the claimant first has a reasonable opportunity to discover the violation.

(3) Any action under this section shall be tried to the court without a jury.

(4) Notwithstanding any other provision of law, the procedures set forth in section 106(f), 305(g), or 405(f) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.) shall be the exclusive means by which materials governed by those sections may be reviewed.

(5) An amount equal to any award against the United States under this section shall be reimbursed by the department or agency concerned to the fund described in section 1304 of title 31, United States Code, out of any appropriation, fund, or other account (excluding any part of such appropriation, fund, or account that is available for the enforcement of any Federal law) that is available for the operating expenses of the department or agency concerned.

(b) Administrative discipline.--If a court or appropriate department or agency determines that the United States or any of its departments or agencies has violated any provision of this chapter, and the court or appropriate department or agency finds that the circumstances surrounding the

violation raise serious questions about whether or not an officer or employee of the United States acted willfully or intentionally with respect to the violation, the department or agency shall, upon receipt of a true and correct copy of the decision and findings of the court or appropriate department or agency promptly initiate a proceeding to determine whether disciplinary action against the officer or employee is warranted. If the head of the department or agency involved determines that disciplinary action is not warranted, he or she shall notify the Inspector General with jurisdiction over the department or agency concerned and shall provide the Inspector General with the reasons for such determination.

(d) Exclusive remedy.--Any action against the United States under this subsection shall be the exclusive remedy against the United States for any claims within the purview of this section.

(e) Stay of proceedings.--(1) Upon the motion of the United States, the court shall stay any action commenced under this section if the court determines that civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case. Such a stay shall toll the limitations periods of paragraph (2) of subsection (b).

(2) In this subsection, the terms "related criminal case" and "related investigation" mean an actual prosecution or investigation in progress at the time at which the request for the stay or any subsequent motion to lift the stay is made. In determining whether an investigation or a criminal case is related to an action commenced under this section, the court shall consider the degree of similarity between the parties, witnesses, facts, and circumstances involved in the 2 proceedings, without requiring that any one or more factors be identical.

(3) In requesting a stay under paragraph (1), the Government may, in appropriate cases, submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the Government makes such an ex parte submission, the plaintiff shall be given an opportunity to make a submission to the court, not ex parte, and the court may, in its discretion, request further information from either party."

Analysis:

Prior to the passage of the USA PATRIOT Act, individuals were permitted only in limited circumstances to file a cause of action and collect money damages against the United States if government officials unlawfully disclosed sensitive information collected through wiretaps and electronic surveillance. Thus, while those engaging in illegal wiretapping or electronic surveillance were subject to civil liability, those illegally disclosing communications lawfully intercepted pursuant to a court order generally could not be sued. Section 223 of the USA PATRIOT Act remedied this inequitable situation; it created an important mechanism for deterring the improper disclosure of sensitive information and providing redress for individuals whose privacy might be violated by such disclosures.

Section 223 permits persons harmed by willful violations of the criminal wiretap statute or the prohibitions on the improper use and disclosure of information contained in FISA to file a claim against the United States for at least $10,000 in damages, plus costs. Section 223 also broadened the circumstances under which administrative discipline could be imposed upon a federal official who improperly handled sensitive information; now, if the relevant court or agency finds a (possible) legal violation, section 223

requires the agency to initiate a proceeding in order to determine the appropriate disciplinary action.

To date, no complaints have been filed against Department employees pursuant to section 223. This is a reflection of the professionalism of the Department's employees as well as their commitment to the rule of law. The Department believes, however, that it is important that section 223 remain on the books in order to provide an important disincentive to those who would unlawfully disclose intercepted communications as well as give compensation to those whose privacy is compromised by any such unlawful disclosure.

The Justice Department does not believe that section 223 has generated any significant criticism. For instance, CDT lists the section as one of the USA PATRIOT Act provisions scheduled to sunset that is not controversial.[42] Indeed, EPIC has even praised section 223 as "serv[ing] to limit misuse of communications captured through lawful surveillance,"[43] and EFF has stated that the provision contains "valuable tools and should certainly be renewed."[44]

Section 225: Immunity for Compliance with FISA Wiretap

Text of Section 225:

> Section 105 of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1805) is amended by inserting after subsection (g) the following:
>
> "(h) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act.".

How Current Law Now Reads:

> **"§ 1805. Issuance of Order**
>
> (a) Necessary findings
>
> Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that--
>
> (1) the President has authorized the Attorney General to approve applications for electronic surveillance for foreign intelligence information;
>
> (2) the application has been made by a Federal officer and approved by the Attorney General;

---

[42] See *supra* note 2.
[43] Electronic Privacy Information Center, "The USA PATRIOT Act," (available at http://www.epic.org/privacy/terrorism/usapatriot).
[44] Electronic Frontier Foundation, "Let the Sun Set on PATRIOT – Section 223 "Civil Liability for Certain Unauthorized Disclosures", *EFFector* (Nov. 19, 2004) (available at http://eff.org/effector/17/43.php#IV).

(3) on the basis of the facts submitted by the applicant there is probable cause to believe that--

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: Provided, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(4) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and

(5) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

. . .

(i) No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this Act."

Analysis:

Pursuant to FISA, the United States may obtain electronic surveillance and physical search orders from the FISA Court concerning an entity or individual whom the court finds probable cause to believe is an agent of a foreign power. Generally, however, as in the case of criminal wiretaps and electronic surveillance, the United States requires the assistance of private communications providers to carry out such court orders.

In the criminal and civil contexts, those who disclose information pursuant to a subpoena or court order are generally exempted from liability. For example, those assisting the government in carrying out criminal investigative wiretaps are provided with immunity from civil liability. *See* 18 U.S.C. § 2511(2)(a)(ii) ("No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, or agents, landlord, custodian, or other specified person for providing information, facilities, or assistance in accordance with the terms of a court order, statutory authorization, or certification under this chapter."). This immunity is important because it helps to secure the prompt cooperation of private parties with law enforcement officers to ensure the effective implementation of court orders.

Prior to the passage of the USA PATRIOT Act, however, while those assisting in the implementation of criminal wiretaps were provided with immunity, no similar immunity protected those companies and individuals assisting the government in carrying

out surveillance orders issued by the FISA Court under FISA. Section 225 ended this anomaly in the law by immunizing from civil liability communications service providers and others who assist the United States in the execution of such FISA orders, thus helping to ensure that such entities and individuals will comply with orders issued by the FISA Court without delay. For example, in the investigation of an espionage subject, the FBI was able to convince a company to assist in the installation of technical equipment pursuant to a FISA order by providing a letter outlining the immunity from civil liability associated with complying with the FISA order.

Because section 225 simply extends to the FISA context the exemption long applied in the civil and criminal contexts, where individuals who disclose information pursuant to a subpoena or court order generally are immune from liability for disclosure, it has not provoked any significant opposition. For example, CDT has taken the position that section 225 is not controversial.[45] Moreover, the provision has been praised for protecting those companies and individuals who are simply fulfilling their legal obligations.[46]

[45] *See supra* note 2.

[46] *See* Ronald L. Plesser, James J. Halpert & Emilio W. Cividanes, "USA PATRIOT Act for Internet and Communications Companies," Computer and Internet Lawyer, March 2002 (calling section 225 "a very important expansion of service provider immunity for compliance with FISA").

CHAPTER I OF *On Liberty* by John Stuart Mill, submitted for the Record by the Honorable Sheila Jackson Lee

ON LIBERTY

by
John Stuart Mill
(1859)

CHAPTER I
INTRODUCTORY

THE subject of this Essay is not the so-called Liberty of the Will, so unfortunately opposed to the misnamed doctrine of Philosophical Necessity; but Civil, or Social Liberty: the nature and limits of the power which can be legitimately exercised by society over the individual. A question seldom stated, and hardly ever discussed, in general terms, but which profoundly influences the practical controversies of the age by its latent presence, and is likely soon to make itself recognized as the vital question of the future. It is so far from being new, that, in a certain sense, it has divided mankind, almost from the remotest ages, but in the stage of progress into which the more civilized portions of the species have now entered, it presents itself under new conditions, and requires a different and more fundamental treatment. The struggle between Liberty and Authority is the most conspicuous feature in the portions of history with which we are earliest familiar, particularly in that of Greece, Rome, and England. But in old times this contest was between subjects, or some classes of subjects, and the government. By liberty, was meant protection against the tyranny of the political rulers. The rulers were conceived (except in some of the popular governments of Greece) as in a necessarily antagonistic position to the people whom they ruled. They consisted of a governing One, or a governing tribe or caste, who derived their authority from inheritance or conquest; who, at all events, did not hold it at the pleasure of the governed, and whose supremacy men did not venture, perhaps did not desire, to contest, whatever precautions might be taken against its oppressive exercise. Their power was regarded as necessary, but also as highly dangerous; as a weapon which they would attempt to use against their subjects, no less than against external enemies. To prevent the weaker members of the community from being preyed upon by innumerable vultures, it was needful that there should be an animal of prey stronger than the rest, commissioned to keep them down. But as the king of the vultures would be no less bent upon preying upon the flock than any of the minor harpies, it was indispensable to be in a perpetual attitude of defence against his beak and claws. The aim, therefore, of patriots, was to set limits to the power which the ruler should be suffered to exercise over the community; and this limitation was what they meant by liberty. It was attempted in two ways. First, by obtaining a recognition of certain immunities, called political liberties or rights, which it was to be regarded as a breach of duty in the ruler to infringe, and which, if he did infringe, specific resistance, or general rebellion, was held to be justifiable. A second, and generally a later expedient, was the establishment of constitutional checks; by which the consent of the community, or of a body of some sort supposed to represent its interests, was made a necessary condition to some of the more important acts of the governing power. To the first of these modes of limitation, the ruling power, in most European countries, was compelled, more or less, to submit. It was not so with the second; and to attain this, or when already in some degree possessed, to attain it more completely, became everywhere the principal object of the lovers of liberty. And so long as mankind were content to combat one enemy by another, and to be ruled by a master, on condition of being guaranteed more

or less efficaciously against his tyranny, they did not carry their aspirations beyond this point.

A time, however, came in the progress of human affairs, when men ceased to think it a necessity of nature that their governors should be an independent power, opposed in interest to themselves. It appeared to them much better that the various magistrates of the State should be their tenants or delegates, revocable at their pleasure. In that way alone, it seemed, could they have complete security that the powers of government would never be abused to their disadvantage. By degrees, this new demand for elective and temporary rulers became the prominent object of the exertions of the popular party, wherever any such party existed; and superseded, to a considerable extent, the previous efforts to limit the power of rulers. As the struggle proceeded for making the ruling power emanate from the periodical choice of the ruled, some persons began to think that too much importance had been attached to the limitation of the power itself. That (it might seem) was a resource against rulers whose interests were habitually opposed to those of the people. What was now wanted was, that the rulers should be identified with the people; that their interest and will should be the interest and will of the nation. The nation did not need to be protected against its own will. There was no fear of its tyrannizing over itself. Let the rulers be effectually responsible to it, promptly removable by it, and it could afford to trust them with power of which it could itself dictate the use to be made. Their power was but the nation's own power, concentrated, and in a form convenient for exercise. This mode of thought, or rather perhaps of feeling, was common among the last generation of European liberalism, in the Continental section of which, it still apparently predominates. Those who admit any limit to what a government may do, except in the case of such governments as they think ought not to exist, stand out as brilliant exceptions among the political thinkers of the Continent. A similar tone of sentiment might by this time have been prevalent in our own country, if the circumstances which for a time encouraged it had continued unaltered.

But, in political and philosophical theories, as well as in persons, success discloses faults and infirmities which failure might have concealed from observation. The notion, that the people have no need to limit their power over themselves, might seem axiomatic, when popular government was a thing only dreamed about, or read of as having existed at some distant period of the past. Neither was that notion necessarily disturbed by such temporary aberrations as those of the French Revolution, the worst of which were the work of an usurping few, and which, in any case, belonged, not to the permanent working of popular institutions, but to a sudden and convulsive outbreak against monarchical and aristocratic despotism. In time, however, a democratic republic came to occupy a large portion of the earth's surface, and made itself felt as one of the most powerful members of the community of nations; and elective and responsible government became subject to the observations and criticisms which wait upon a great existing fact. It was now perceived that such phrases as "self-government," and "the power of the people over themselves," do not express the true state of the case. The "people" who exercise the power, are not always the same people with those over whom it is exercised, and the "self-government" spoken of, is not the government of each by himself, but of each by all the rest. The will of the people, moreover, practically means, the will of the most numerous or the most active part of the people; the majority, or those who succeed in making themselves accepted as the majority; the people, consequently, may desire to oppress a part of their number; and precautions are as much needed against this, as against any other abuse of power. The limitation, therefore, of the power of government over individuals, loses none of its importance when the holders of power are regularly accountable to the community, that is, to the strongest party therein. This view of things, recommending itself equally to the intelligence of thinkers and to the inclination of those important classes in European society to whose real or supposed interests democracy is

adverse, has had no difficulty in establishing itself; and in political speculations "the tyranny of the majority" is now generally included among the evils against which society requires to be on its guard.

Like other tyrannies, the tyranny of the majority was at first, and is still vulgarly, held in dread, chiefly as operating through the acts of the public authorities. But reflecting persons perceived that when society is itself the tyran--society collectively, over the separate individuals who compose it--its means of tyrannizing are not restricted to the acts which it may do by the hands of its political functionaries. Society can and does execute its own mandates: and if it issues wrong mandates instead of right, or any mandates at all in things with which it ought not to meddle, it practises a social tyranny more formidable than many kinds of political oppression, since, though not usually upheld by such extreme penalties, it leaves fewer means of escape, penetrating much more deeply into the details of life, and enslaving the soul itself. Protection, therefore, against the tyranny of the magistrate is not enough; there needs protection also against the tyranny of the prevailing opinion and feeling; against the tendency of society to impose, by other means than civil penalties, its own ideas and practices as rules of conduct on those who dissent from them; to fetter the development, and, if possible, prevent the formation, of any individuality not in harmony with its ways, and compel all characters to fashion themselves upon the model of its own. There is a limit to the legitimate interference of collective opinion with individual independence; and to find that limit, and maintain it against encroachment, is as indispensable to a good condition of human affairs, as protection against political despotism.

But though this proposition is not likely to be contested in general terms, the practical question, where to place the limit--how to make the fitting adjustment between individual independence and social control--is a subject on which nearly everything remains to be done. All that makes existence valuable to any one, depends on the enforcement of restraints upon the actions of other people. Some rules of conduct, therefore, must be imposed, by law in the first place, and by opinion on many things which are not fit subjects for the operation of law. What these rules should be, is the principal question in human affairs; but if we except a few of the most obvious cases, it is one of those which least progress has been made in resolving. No two ages, and scarcely any two countries, have decided it alike; and the decision of one age or country is a wonder to another. Yet the people of any given age and country no more suspect any difficulty in it, than if it were a subject on which mankind had always been agreed. The rules which obtain among themselves appear to them self-evident and self-justifying. This all but universal illusion is one of the examples of the magical influence of custom, which is not only, as the proverb says a second nature, but is continually mistaken for the first. The effect of custom, in preventing any misgiving respecting the rules of conduct which mankind impose on one another, is all the more complete because the subject is one on which it is not generally considered necessary that reasons should be given, either by one person to others, or by each to himself. People are accustomed to believe and have been encouraged in the belief by some who aspire to the character of philosophers, that their feelings, on subjects of this nature, are better than reasons, and render reasons unnecessary. The practical principle which guides them to their opinions on the regulation of human conduct, is the feeling in each person's mind that everybody should be required to act as he, and those with whom he sympathizes, would like them to act. No one, indeed, acknowledges to himself that his standard of judgment is his own liking; but an opinion on a point of conduct, not supported by reasons, can only count as one person's preference; and if the reasons, when given, are a mere appeal to a similar preference felt by other people, it is still only many people's liking instead of one. To an ordinary man, however, his own preference, thus supported, is not only a perfectly satisfactory reason, but the only one he generally has for any of his notions of morality, taste, or propriety,

which are not expressly written in his religious creed; and his chief guide in the interpretation even of that. Men's opinions, accordingly, on what is laudable or blamable, are affected by all the multifarious causes which influence their wishes in regard to the conduct of others, and which are as numerous as those which determine their wishes on any other subject. Sometimes their reason--at other times their prejudices or superstitions: often their social affections, not seldom their anti-social ones, their envy or jealousy, their arrogance or contemptuousness: but most commonly, their desires or fears for themselves--their legitimate or illegitimate self-interest. Wherever there is an ascendant class, a large portion of the morality of the country emanates from its class interests, and its feelings of class superiority. The morality between Spartans and Helots, between planters and negroes, between princes and subjects, between nobles and roturiers, between men and women, has been for the most part the creation of these class interests and feelings: and the sentiments thus generated, react in turn upon the moral feelings of the members of the ascendant class, in their relations among themselves. Where, on the other hand, a class, formerly ascendant, has lost its ascendency, or where its ascendency is unpopular, the prevailing moral sentiments frequently bear the impress of an impatient dislike of superiority. Another grand determining principle of the rules of conduct, both in act and forbearance which have been enforced by law or opinion, has been the servility of mankind towards the supposed preferences or aversions of their temporal masters, or of their gods. This servility though essentially selfish, is not hypocrisy; it gives rise to perfectly genuine sentiments of abhorrence; it made men burn magicians and heretics. Among so many baser influences, the general and obvious interests of society have of course had a share, and a large one, in the direction of the moral sentiments: less, however, as a matter of reason, and on their own account, than as a consequence of the sympathies and antipathies which grew out of them: and sympathies and antipathies which had little or nothing to do with the interests of society, have made themselves felt in the establishment of moralities with quite as great force.

The likings and dislikings of society, or of some powerful portion of it, are thus the main thing which has practically determined the rules laid down for general observance, under the penalties of law or opinion. And in general, those who have been in advance of society in thought and feeling, have left this condition of things unassailed in principle, however they may have come into conflict with it in some of its details. They have occupied themselves rather in inquiring what things society ought to like or dislike, than in questioning whether its likings or dislikings should be a law to individuals. They preferred endeavouring to alter the feelings of mankind on the particular points on which they were themselves heretical, rather than make common cause in defence of freedom, with heretics generally. The only case in which the higher ground has been taken on principle and maintained with consistency, by any but an individual here and there, is that of religious belief: a case instructive in many ways, and not least so as forming a most striking instance of the fallibility of what is called the moral sense: for the *odium theologicum*, in a sincere bigot, is one of the most unequivocal cases of moral feeling. Those who first broke the yoke of what called itself the Universal Church, were in general as little willing to permit difference of religious opinion as that church itself. But when the heat of the conflict was over, without giving a complete victory to any party, and each church or sect was reduced to limit its hopes to retaining possession of the ground it already occupied; minorities, seeing that they had no chance of becoming majorities, were under the necessity of pleading to those whom they could not convert, for permission to differ. It is accordingly on this battle-field, almost solely, that the rights of the individual against society have been asserted on broad grounds of principle, and the claim of society to exercise authority over dissentients openly controverted. The great writers to whom the world owes what religious liberty it possesses, have mostly asserted freedom of conscience as an indefeasible right, and denied absolutely that a human being

is accountable to others for his religious belief. Yet so natural to mankind is intolerance in whatever they really care about, that religious freedom has hardly anywhere been practically realized, except where religious indifference, which dislikes to have its peace disturbed by theological quarrels, has added its weight to the scale. In the minds of almost all religious persons, even in the most tolerant countries, the duty of toleration is admitted with tacit reserves. One person will bear with dissent in matters of church government, but not of dogma; another can tolerate everybody, short of a Papist or an Unitarian; another, every one who believes in revealed religion; a few extend their charity a little further, but stop at the belief in a God and in a future state. Wherever the sentiment of the majority is still genuine and intense, it is found to have abated little of its claim to be obeyed.

In England, from the peculiar circumstances of our political history, though the yoke of opinion is perhaps heavier, that of law is lighter, than in most other countries of Europe; and there is considerable jealousy of direct interference, by the legislative or the executive power with private conduct; not so much from any just regard for the independence of the individual, as from the still subsisting habit of looking on the government as representing an opposite interest to the public. The majority have not yet learnt to feel the power of the government their power, or its opinions their opinions. When they do so, individual liberty will probably be as much exposed to invasion from the government, as it already is from public opinion. But, as yet, there is a considerable amount of feeling ready to be called forth against any attempt of the law to control individuals in things in which they have not hitherto been accustomed to be controlled by it; and this with very little discrimination as to whether the matter is, or is not, within the legitimate sphere of legal control; insomuch that the feeling, highly salutary on the whole, is perhaps quite as often misplaced as well grounded in the particular instances of its application.

There is, in fact, no recognized principle by which the propriety or impropriety of government interference is customarily tested. People decide according to their personal preferences. Some, whenever they see any good to be done, or evil to be remedied, would willingly instigate the government to undertake the business; while others prefer to bear almost any amount of social evil, rather than add one to the departments of human interests amenable to governmental control. And men range themselves on one or the other side in any particular case, according to this general direction of their sentiments; or according to the degree of interest which they feel in the particular thing which it is proposed that the government should do; or according to the belief they entertain that the government would, or would not, do it in the manner they prefer; but very rarely on account of any opinion to which they consistently adhere, as to what things are fit to be done by a government. And it seems to me that, in consequence of this absence of rule or principle, one side is at present as often wrong as the other; the interference of government is, with about equal frequency, improperly invoked and improperly condemned.

The object of this Essay is to assert one very simple principle, as entitled to govern absolutely the dealings of society with the individual in the way of compulsion and control, whether the means used be physical force in the form of legal penalties, or the moral coercion of public opinion. That principle is, that the sole end for which mankind are warranted, individually or collectively in interfering with the liberty of action of any of their number, is self-protection. That the only purpose for which power can be rightfully exercised over any member of a civilized community, against his will, is to prevent harm to others. His own good, either physical or moral, is not a sufficient warrant. He cannot rightfully be compelled to do or forbear because it will be better for him to do so, because it will make him happier, because, in the opinions of others, to do so would be wise, or

even right. These are good reasons for remonstrating with him, or reasoning with him, or persuading him, or entreating him, but not for compelling him, or visiting him with any evil, in case he do otherwise. To justify that, the conduct from which it is desired to deter him must be calculated to produce evil to some one else. The only part of the conduct of any one, for which he is amenable to society, is that which concerns others. In the part which merely concerns himself, his independence is, of right, absolute. Over himself, over his own body and mind, the individual is sovereign.

It is, perhaps, hardly necessary to say that this doctrine is meant to apply only to human beings in the maturity of their faculties. We are not speaking of children, or of young persons below the age which the law may fix as that of manhood or womanhood. Those who are still in a state to require being taken care of by others, must be protected against their own actions as well as against external injury. For the same reason, we may leave out of consideration those backward states of society in which the race itself may be considered as in its nonage. The early difficulties in the way of spontaneous progress are so great, that there is seldom any choice of means for overcoming them; and a ruler full of the spirit of improvement is warranted in the use of any expedients that will attain an end, perhaps otherwise unattainable. Despotism is a legitimate mode of government in dealing with barbarians, provided the end be their improvement, and the means justified by actually effecting that end. Liberty, as a principle, has no application to any state of things anterior to the time when mankind have become capable of being improved by free and equal discussion. Until then, there is nothing for them but implicit obedience to an Akbar or a Charlemagne, if they are so fortunate as to find one. But as soon as mankind have attained the capacity of being guided to their own improvement by conviction or persuasion (a period long since reached in all nations with whom we need here concern ourselves), compulsion, either in the direct form or in that of pains and penalties for non-compliance, is no longer admissible as a means to their own good, and justifiable only for the security of others.

It is proper to state that I forego any advantage which could be derived to my argument from the idea of abstract right as a thing independent of utility. I regard utility as the ultimate appeal on all ethical questions; but it must be utility in the largest sense, grounded on the permanent interests of man as a progressive being. Those interests, I contend, authorize the subjection of individual spontaneity to external control, only in respect to those actions of each, which concern the interest of other people. If any one does an act hurtful to others, there is a prima facie case for punishing him, by law, or, where legal penalties are not safely applicable, by general disapprobation. There are also many positive acts for the benefit of others, which he may rightfully be compelled to perform; such as, to give evidence in a court of justice; to bear his fair share in the common defence, or in any other joint work necessary to the interest of the society of which he enjoys the protection; and to perform certain acts of individual beneficence, such as saving a fellow-creature's life, or interposing to protect the defenceless against ill-usage, things which whenever it is obviously a man's duty to do, he may rightfully be made responsible to society for not doing. A person may cause evil to others not only by his actions but by his inaction, and in neither case he is justly accountable to them for the injury. The latter case, it is true, requires a much more cautious exercise of compulsion than the former. To make any one answerable for doing evil to others, is the rule; to make him answerable for not preventing evil, is, comparatively speaking, the exception. Yet there are many cases clear enough and grave enough to justify that exception. In all things which regard the external relations of the individual, he is *de jure* amenable to those whose interests are concerned, and if need be, to society as their protector. There are often good reasons for not holding him to the responsibility; but these reasons must arise from the special expediencies of the case: either because it is a kind of case in which he is on the whole likely to act better, when left to his own discretion, than when

controlled in any way in which society have it in their power to control him; or because the attempt to exercise control would produce other evils, greater than those which it would prevent. When such reasons as these preclude the enforcement of responsibility, the conscience of the agent himself should step into the vacant judgment-seat, and protect those interests of others which have no external protection; judging himself all the more rigidly, because the case does not admit of his being made accountable to the judgment of his fellow-creatures.

But there is a sphere of action in which society, as distinguished from the individual, has, if any, only an indirect interest; comprehending all that portion of a person's life and conduct which affects only himself, or, if it also affects others, only with their free, voluntary, and undeceived consent and participation. When I say only himself, I mean directly, and in the first instance: for whatever affects himself, may affect others through himself; and the objection which may be grounded on this contingency, will receive consideration in the sequel. This, then, is the appropriate region of human liberty. It comprises, first, the inward domain of consciousness; demanding liberty of conscience, in the most comprehensive sense; liberty of thought and feeling; absolute freedom of opinion and sentiment on all subjects, practical or speculative, scientific, moral, or theological. The liberty of expressing and publishing opinions may seem to fall under a different principle, since it belongs to that part of the conduct of an individual which concerns other people; but, being almost of as much importance as the liberty of thought itself, and resting in great part on the same reasons, is practically inseparable from it. Secondly, the principle requires liberty of tastes and pursuits; of framing the plan of our life to suit our own character; of doing as we like, subject to such consequences as may follow; without impediment from our fellow-creatures, so long as what we do does not harm them even though they should think our conduct foolish, perverse, or wrong. Thirdly, from this liberty of each individual, follows the liberty, within the same limits, of combination among individuals; freedom to unite, for any purpose not involving harm to others: the persons combining being supposed to be of full age, and not forced or deceived.

No society in which these liberties are not, on the whole, respected, is free, whatever may be its form of government; and none is completely free in which they do not exist absolute and unqualified. The only freedom which deserves the name, is that of pursuing our own good in our own way, so long as we do not attempt to deprive others of theirs, or impede their efforts to obtain it. Each is the proper guardian of his own health, whether bodily, or mental or spiritual. Mankind are greater gainers by suffering each other to live as seems good to themselves, than by compelling each to live as seems good to the rest.

Though this doctrine is anything but new, and, to some persons, may have the air of a truism, there is no doctrine which stands more directly opposed to the general tendency of existing opinion and practice. Society has expended fully as much effort in the attempt (according to its lights) to compel people to conform to its notions of personal, as of social excellence. The ancient commonwealths thought themselves entitled to practise, and the ancient philosophers countenanced, the regulation of every part of private conduct by public authority, on the ground that the State had a deep interest in the whole bodily and mental discipline of every one of its citizens, a mode of thinking which may have been admissible in small republics surrounded by powerful enemies, in constant peril of being subverted by foreign attack or internal commotion, and to which even a short interval of relaxed energy and self-command might so easily be fatal, that they could not afford to wait for the salutary permanent effects of freedom. In the modern world, the greater size of political communities, and above all, the separation between the spiritual and temporal authority (which placed the direction of men's consciences in

other hands than those which controlled their worldly affairs), prevented so great an interference by law in the details of private life; but the engines of moral repression have been wielded more strenuously against divergence from the reigning opinion in self-regarding, than even in social matters; religion, the most powerful of the elements which have entered into the formation of moral feeling, having almost always been governed either by the ambition of a hierarchy, seeking control over every department of human conduct, or by the spirit of Puritanism. And some of those modern reformers who have placed themselves in strongest opposition to the religions of the past, have been nowhere behind either churches or sects in their assertion of the right of spiritual domination: M. Compte, in particular, whose social system, as unfolded in his *Trait de Politique Positive*, aims at establishing (though by moral more than by legal appliances) a despotism of society over the individual, surpassing anything contemplated in the political ideal of the most rigid disciplinarian among the ancient philosophers.

Apart from the peculiar tenets of individual thinkers, there is also in the world at large an increasing inclination to stretch unduly the powers of society over the individual, both by the force of opinion and even by that of legislation: and as the tendency of all the changes taking place in the world is to strengthen society, and diminish the power of the individual, this encroachment is not one of the evils which tend spontaneously to disappear, but, on the contrary, to grow more and more formidable. The disposition of mankind, whether as rulers or as fellow-citizens, to impose their own opinions and inclinations as a rule of conduct on others, is so energetically supported by some of the best and by some of the worst feelings incident to human nature, that it is hardly ever kept under restraint by anything but want of power; and as the power is not declining, but growing, unless a strong barrier of moral conviction can be raised against the mischief, we must expect, in the present circumstances of the world, to see it increase.

It will be convenient for the argument, if, instead of at once entering upon the general thesis, we confine ourselves in the first instance to a single branch of it, on which the principle here stated is, if not fully, yet to a certain point, recognized by the current opinions. This one branch is the Liberty of Thought: from which it is impossible to separate the cognate liberty of speaking and of writing. Although these liberties, to some considerable amount, form part of the political morality of all countries which profess religious toleration and free institutions, the grounds, both philosophical and practical, on which they rest, are perhaps not so familiar to the general mind, nor so thoroughly appreciated by many even of the leaders of opinion, as might have been expected. Those grounds, when rightly understood, are of much wider application than to only one division of the subject, and a thorough consideration of this part of the question will be found the best introduction to the remainder. Those to whom nothing which I am about to say will be new, may therefore, I hope, excuse me, if on a subject which for now three centuries has been so often discussed, I venture on one discussion more.

some utilitarian terms

E-mail
info@utilitarianism.com

HOME
HedWeb
Future Opioids
BLTC Research
Wirehead Hedonism
Paradise-Engineering
Critique of *Brave New World*