IMPLEMENTATION OF THE USA PATRIOT ACT: SECTION 218—FOREIGN INTELLIGENCE INFORMATION ("THE WALL")

HEARING

BEFORE THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

OF THE

COMMITTEE ON THE JUDICIARY HOUSE OF REPRESENTATIVES

ONE HUNDRED NINTH CONGRESS

FIRST SESSION

APRIL 28, 2005

Serial No. 109–16

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

20–877 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*

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

HOWARD COBLE, North Carolina, *Chairman*

DANIEL E. LUNGREN, California
MARK GREEN, Wisconsin
TOM FEENEY, Florida
STEVE CHABOT, Ohio
RIC KELLER, Florida
JEFF FLAKE, Arizona
MIKE PENCE, Indiana
J. RANDY FORBES, Virginia
LOUIE GOHMERT, Texas

ROBERT C. SCOTT, Virginia
SHEILA JACKSON LEE, Texas
MAXINE WATERS, California
MARTIN T. MEEHAN, Massachusetts
WILLIAM D. DELAHUNT, Massachusetts
ANTHONY D. WEINER, New York

JAY APPERSON, *Chief Counsel*
ELIZABETH SOKUL, *Special Counsel on Intelligence and Homeland Security*
JASON CERVENAK, *Full Committee Counsel*
MICHAEL VOLKOV, *Deputy Chief Counsel*
BOBBY VASSAR, *Minority Counsel*

CONTENTS

APRIL 28, 2005

OPENING STATEMENT

WITNESSES

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

IMPLEMENTATION OF THE USA PATRIOT ACT: SECTION 218—FOREIGN INTELLIGENCE INFORMATION ("THE WALL")

THURSDAY, APRIL 28, 2005

HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON CRIME, TERRORISM,
AND HOMELAND SECURITY
COMMITTEE ON THE JUDICIARY,
Washington, DC.

The Subcommittee met, pursuant to notice, at 2:30 p.m., in Room 2141, Rayburn House Office Building, the Honorable Steve Chabot presiding.

Mr. CHABOT This is the Subcommittee on the Constitution. We'll come to order.

[Discussion off the record.]

Mr. CHABOT. Subcommittee on Crime, I've been informed. [Laughter.]

I'm the Chair of the Subcommittee on the Constitution. I'm so used to saying that. I apologize.

This is the Subcommittee on Crime, Terrorism, and Homeland Security. And the Chair of the Committee, Howard Coble, is unable to attend this afternoon; so he asked me to stand in his place. And I'll try to remember which Committee this is for the rest of the afternoon. So I apologize for that.

This is this Committee's second hearing today on the USA PATRIOT Act. This hearing focuses on section 218 and its effect on "The Wall" that prevented our law enforcement agencies and intelligence community from communicating.

The Foreign Intelligence Surveillance Act limited surveillance and physical search orders to instances where authorities certified that "the purpose" of the order was for foreign intelligence gathering. Subsequent case law and agency guidance interpreted the "purpose" requirement to mean that foreign intelligence gathering had to be the primary purpose. As a result, law enforcement and the intelligence community came to believe that sharing information or coordinating efforts would preclude the ability to obtain court approval for appropriate surveillance.

The effect of this interpretation was that the metaphorical "wall" was built; which prevented vital communications, that some argue contributed to the failure of Government officials to share vital information that could possibly have prevented the 9/11 attacks.

The witnesses this afternoon will examine the effects of section 218 on the Foreign Intelligence Surveillance Act and "The Wall."

With this background on FISA, I look forward to hearing testimony from the witnesses; and now turn to the distinguished Ranking Member of this Committee, Bobby Scott, for his opening statement.

Mr. SCOTT. Thank you. And I thank you for chairing the hearing, and for holding this hearing on the issue that has been foreshadowing much of our discussion about the PATRIOT Act: the extent to which we have dismantled the so-called "wall."

We've broken down the traditional wall between foreign intelligence gathering—particularly foreign intelligence—and criminal proceedings, in order to give Government broad authority to collect and share information, mostly secretly. And so I'm concerned that we have blurred the traditional line between protecting our privacy and freedoms.

While I agree that some lifting of traditional restrictions in this area may be justified for Government to better use the authorities it already has in many instances, I'm also mindful that those restrictions were placed there for a good reason. We have seen, with COINTELPRO, Watergate, FBI spying on Martin Luther King, Jr., and other incidents, what abuses can occur when we do not keep tight enough rein on the Government's use of extraordinary powers. We shouldn't have to experience those problems again to ensure that the abuses do not occur.

When we operate in the foreign intelligence area, we have traditionally given broad latitude for the use of extraordinary investigatory tools abroad, particularly involving non-U.S. persons. But when we turn those tools inward, we run the risk of including U.S. persons in some of the investigative sweeps that occur, unless we have sufficient barriers to prevent unwarranted extensions.

Now, since much of the foreign intelligence side is secretive and ex-parte, with only Government participation, and with no public oversight or review, we don't have the traditional notice, challenge, and public scrutiny oversight that we have on the criminal side. So we've used "The Wall" as protection. That is, if you get something on the foreign intelligence side, you can't use it on the criminal side.

With "The Wall" gone, I believe we should focus on establishing sufficient notice, challenge, and public reporting requirements, to ensure that foreign intelligence operations do not unduly creep into the domestic activities of U.S. persons.

Now, some of our law enforcement officials seem to feel that the mere inclusion of information regarding uninvolved, innocent persons amounts to "no harm, no foul," if they're not arrested or subjected to having to challenge the inclusion—excuse me, the incursion or other process; a sort of "What they don't know won't hurt them" philosophy. Yet if overly broad information is collected, it can also be spread all over town, greatly increasing the likelihood that any of your neighbors, who may happen to be law enforcement, military, or intelligence employees, will know private things about you that you thought were private and known only to those whom you knowingly gave the information.

So the problem with "The Wall" being broken down isn't just the improper acquisition and use of the information; but it's also preventing people from having it in the first place, other than those you gave it to with an expectation of privacy.

So Mr. Chairman, I look forward to the testimony of our witnesses on the extent to which our privacies and freedoms are being protected despite the dismantling of "The Wall" through the USA PATRIOT Act and other measures, and what safeguards are needed to prevent the creep of overly intrusive foreign intelligence operations and powers into the privacy of our homes. Thank you, Mr. Chairman.

Mr. CHABOT. Thank you very much. And it's the practice of the Subcommittee to swear in witnesses who are appearing before it. So if you would, all please rise and raise your right hands.

[Witnesses sworn.]

Mr. CHABOT. Thank you. Let the record show that each of the witnesses answered in the affirmative.

And at this time, I'd like to introduce this afternoon's very distinguished panel. Our first witness is Patrick J. Fitzgerald, United States Attorney for the Northern District of Illinois. Prior to his appointment to this position by President George W. Bush, Mr. Fitzgerald served for 13 years as an Assistant U.S. Attorney in the United States Attorney's Office for the Southern District of New York, General, of the United States. He graduated from Amherst College, Phi Beta Kappa, with a bachelor's degree in economics and mathematics, and from Harvard Law School. We welcome you here this afternoon, Mr. Fitzgerald.

Our second witness is David Kris. David Kris joined the Department of Justice after clerking for U.S. Court of Appeals Judge Stephen S. Strott. For 8 years, he served in the criminal division in the U.S. Attorney's Office for the District of Columbia. In 2000, Mr. Kris was named Associate Deputy Attorney General, with responsibilities for managing the Justice Department's national security programs. He attended Haverford College, and Harvard Law School. In June 2003, Mr. Kris joined Time Warner Inc., as vice president in the legal department. And we welcome you here this afternoon, Mr. Kris.

Our third witness would be Kate Martin. Ms. Martin has been Director of the Center for the National Security Studies since 1992. And prior to assuming her current role, she served as litigation director for the center. She graduated from the University of Virginia Law School, and from Pomona College, with a B.A. in philosophy. And we welcome you here this afternoon, Ms. Martin.

And our fourth and final witness this afternoon will be Peter Swire, a professor of law at the Ohio State University's Morris College of Law. I thank Professor Swire for returning. He has graciously agreed to testify for a second time in this series of PATRIOT Act hearings.

And also, coming from Ohio State, we ought to give you a special recognition for that, as well. Cincinnati's not too far from there.

Prior to joining the faculty at Ohio State University, Mr. Swire served in the Clinton Administration as chief counselor for privacy in the Office of Management and Budget. Professor Swire is a graduate of Princeton University, and Yale Law School. After graduating from law school, he clerked for Judge Ralph K. Winter, Jr., of the United States Court of Appeals for the Second Circuit.

And so we have a very distinguished panel here this afternoon. And as I'm sure you're all aware of, we have a lighting system

here. We'd ask each witness to stay within the 5-minute time frame, if at all possible. There'll be a green light that'll stay on for 4 minutes; a yellow light will tell you you've got about a minute to wrap up; and then, the red light will come on. And we'll give you a little leeway, but if you could stay within that we'd really appreciate it.

And we'll begin this afternoon with you, Mr. Fitzgerald.

TESTIMONY OF PATRICK J. FITZGERALD, UNITED STATES ATTORNEY FOR THE NORTHERN DISTRICT OF ILLINOIS, DEPARTMENT OF JUSTICE

Mr. FITZGERALD. Thank you, Mr. Chairman and Ranking Member Scott. I sit here now, having been working on terrorism cases in the field for about 11 years. And seven of those years, I worked as a terrorism prosecutor while "The Wall" was up; and four I've worked since it has been down. And I can tell you, then, 4 years ago, when "The Wall" was taken down, I could tell you my firm belief that that was the single most important change made, not just in the PATRIOT Act, but in any law that affected our national security. It is extremely valuable. Four years later, I believe that even more.

Let me give you a practical example of how "The Wall" worked. in 1996, when we had an investigation of Osama Bin Laden, there were limits on certain people who we could talk to about certain topics. When we talked to private citizens, New York City police officers, law enforcement generally, even the CIA, there were basically no limits on what we could ask and what we could learn, if we had the clearance.

When we went overseas, we could talk to foreign citizens, foreign police, foreign spies. We could ask whatever we wanted. And if they gave us the answers, we could take it.

When we dealt with Al-Qaeda members, and we did—both overseas and in the United States, as part of our investigation, we talked to Al-Qaeda members and made them witnesses—we not only could ask everything we wanted to, we did. And whatever information we got, we could use.

The people we had limits on speaking to were the FBI agents working the intelligence investigation of Osama Bin Laden right across the street from us in New York, because of "The Wall": the fear we might learn what they had learned from FISA.

In other cases in many other districts, there were prosecutors who did not even know there were intelligence investigations going on, because the people who did those investigations did not even know who the prosecutors were, or never talked to them.

And let me give you a concrete example of how dangerous that could be. After the 1998 bombings of two embassies, American embassies, in Kenya and Tanzania, we had in the grand jury—and it's now public—a person by the name of "Ali Mohamed," a U.S. citizen from California who used to be in the American military and the Egyptian military. At the time, we suspected he had a role in the embassy bombings.

He went into the grand jury; he lied. We believed he lied. We had no link then to the bombings. And we knew from him that if we did not arrest him that day, he was flying overseas. And we were

afraid that we would never see him again. We also knew that a search had happened, under the FISA statute, of Ali Mohamed prior to that. We had no idea what was taken. We didn't know the contents, the results of that search.

We had to make a decision whether to arrest him or not—that night, with many of the cards in our hand unknown to us, although known to the FBI. And my prior boss, Mary Jo White, made the right decision. We arrested Ali Mohamed. He would later plead guilty and admit to us that he had been around for the training of the top Al-Qaeda leadership, including Bin Laden and Ayman Zawahiri. He had trained some of the people who would later be involved in the World Trade Center bombing. He had done the surveillance, the casings, of the American embassies in Tanzania and Kenya. He had shown photographs and sketches of the embassies to Osama Bin Laden himself. And he told us that if we had not arrested him that evening, he would have left the country and rejoined Osama Bin Laden in Afghanistan.

Because of "The Wall," we made a decision only knowing half the facts we needed to know. And we could easily have let him rejoin Osama Bin Laden in a cave, fighting our troops; rather than being in an American prison facility. That, to me, illustrates how crazy "The Wall" was. We could know what Al-Qaeda knew; we couldn't know what the FBI knew.

When the PATRIOT Act included section 218, that wall changed. And now, when we sit down in my district, the Northern District of Illinois, and work together with the FBI, we sit down and talk about our criminal investigations; we talk about the intelligence investigations. And we try to make sure that we're doing the right thing; that we're coordinated. And we move forward.

I, too, am concerned about civil liberties and privacy. In my view, the way we're working, we're doing things coordinated. We're talking things through. We're making sure the law is followed. I do not see abuses of privacy or civil liberties. What I do see is that the right hand knows what the left hand is doing. And I think we do a much better job. Thank you.

[The prepared statement of Mr. Fitzgerald follows:]

PREPARED STATEMENT OF PATRICK J. FITZGERALD

PATRICK J. FITZGERALD

UNITED STATES ATTORNEY

NORTHERN DISTRICT OF ILLINOIS

PREPARED REMARKS FOR THE

SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

COMMITTEE ON THE JUDICIARY

U.S. HOUSE OF REPRESENTATIVES

APRIL 28, 2005

INTRODUCTION

Mr. Chairman, members of the Committee, thank you for asking me here today. I very much look forward to this opportunity to discuss with you how the efforts of the United States Attorney's Offices in the investigation and prosecution of terrorists have changed since the passage of the USA PATRIOT Act ("Patriot Act") and, in particular, section 218 of the Patriot Act which helped to dismantle what was formerly known as "the wall" between intelligence and law enforcement.

I will state up front that I firmly believe that the Patriot Act contained the single most important – and necessary – change in American law as it effects national security over the last decade, and that is section 218, which played a critical role in ending the artificial "wall" between intelligence and law enforcement personnel. As a prosecutor who has worked on terrorism matters for over ten years now, I thank you on behalf of federal prosecutors, FBI agents and the public for that long overdue change that has made America safer.

What was the "wall"? Before the USA PATRIOT Act, applications for FISA orders 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 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 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 such coordination, the more coordination that occurred, the more likely courts would find that law enforcement, rather than foreign intelligence collection, had become the primary purpose of the surveillance or search. The perceived need for a wall was based on the assumption that information about persons and groups seeking to do harm to our country could neatly be separated into "intelligence" information and "evidence."

It is nearly impossible to comprehend the bizarre and dangerous implications that "the wall" caused without reviewing a few examples. While most of the investigations conducted when the wall was in place remain secret, a few matters have become public. For instance, 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 the CIA. We could talk to foreign police officers, foreign citizens, even foreign spies. 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 understood we could not talk to. Who? The FBI agents assigned to a parallel intelligence investigation of Usama Bin Laden and al Qaeda. We understood that we could not learn what information they had gathered from FISA surveillances without prior approvals of other officials. That was "the wall," which a federal court has since agreed was fundamentally flawed – and dangerous.

Let me review some other examples of how the wall played out. On August 7, 1998, al Qaeda struck at the American embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, nearly simultaneously, killing 224 people. The team of FBI agents and prosecutors, which had obtained a sealed indictment of Bin Laden two months earlier, deployed to East Africa and almost immediately learned of al Qaeda's involvement and arrested two bombers in Nairobi. One month later, in September 1998, a man named Ali Mohamed was questioned before a federal grand jury in Manhattan. Ali Mohamed, a California resident, had become a United States citizen in 1989 after serving in the United States Army beginning in 1986. It was believed at the time that Mohamed lied in the grand jury proceeding and that he was involved with the al Qaeda network, but Mohamed had not by then been tied to the bombings. Ali Mohamed left the courthouse to go to his hotel, followed by FBI agents, but not under arrest. He had imminent plans to fly to Egypt. The decision had to be made at that moment whether to charge Mohamed with false statements. If not, Mohamed would leave the country. That difficult decision was made without knowing or reviewing the intelligence information on the other side of the "wall." It was ultimately decided to arrest Mohamed that night in his hotel room. As described below, the team got lucky, but we

never should have had to rely on luck. The prosecution team later obtained access to the intelligence information, including documents obtained from an earlier search of Mohamed's home by the intelligence team on the other side of "the wall." (The search had been a FISA search under authority that pre-existed the Patriot Act.) Those documents included direct written communications with al Qaeda members and a library of al Qaeda training materials that would have made the decision far less difficult. The criminal case gathered additional evidence through further investigation. Mohamed later pleaded guilty in federal court admitting that he was a top trainer to the leadership of al Qaeda and Egyptian Islamic Jihad, and that he had participated in the surveillance of a number of overseas American targets, including the American embassy in Nairobi, Kenya, and had later shown the sketches of that embassy to Bin Laden himself. Mohamed further admitted he had trained some of the persons in New York who had been responsible for the 1993 World Trade Center bombing. Mohamed stated that had he not been arrested on that day in September 1998, he had intended to travel to Afghanistan to rejoin Usama Bin Laden. Thus, while the right decision to arrest was made partly in the dark, the "wall" could easily have caused a different decision that September evening that would have allowed a key player in the al Qaeda network to escape justice for the embassy bombing in Kenya and rejoin Usama Bin Laden in a cave in Afghanistan, instead of going to federal prison.

What is ironic is that this is an example of where the wall came into play where both criminal and intelligence investigations existed. In most cases, the wall prevented criminal cases from being opened or pursued at all. In 1993, for example, after the World Trade Center bombing, conspirators, including Sheik Omar Abdel Rahman, planned to bomb the Holland and Lincoln tunnels, the FBI building, the United Nations and the George Washington Bridge.

Prosecutors, however, were in the dark about the details of the plot until very late in the day for fear that earlier prosecutorial involvement – even mere knowledge by the prosecutors of what was happening – would breach the wall. Later, during the investigation of the planned Millenium attacks, criminal prosecutors were forced to observe the wall while the intelligence community dealt with al Qaeda planned attacks on our soil and overseas. Criminal prosecutors received information only in part and with lag time so as not to breach the wall. The persons who determined what could be shared with the prosecutors were on the other side of the wall, making their best guess as to what would be helpful. This was no way to defend our country from imminent attack. Moreover, the above examples occurred in New York where the working relationship between prosecutors and agents in the field was strong. In many other areas in the country, the wall was so high that criminal agents and prosecutors simply had no idea what intelligence investigators were doing, and often even who they were.

When I heard over the last several years from critics of the Patriot Act that the law was passed in haste and ought simply be repealed, I think back to the days when prosecutors and agents made decisions about national security – life and death decisions – while only looking at half the cards in their hand and know that the change came a decade too late, not a moment too soon.

Prior to the Patriot Act, there was also concern with a prosecutor's uncertain ability to share grand jury testimony affecting national security with the intelligence community, a problem that was fixed by section 203(a) of the Patriot Act. In 1997, Wadih el Hage, a key member of the al Qaeda cell in Nairobi, Kenya, had his Nairobi residence searched and his telephone wiretapped with the participation of the intelligence community. He thereafter departed Kenya en route to

Dallas, Texas, in September 1997, changing flights in New York City. At that point, el Hage was subpoenaed from the airport to a federal grand jury in Manhattan where he was questioned about Bin Laden, al Qaeda and his associates in Kenya, including among others his close associate "Harun." El Hage chose to lie repeatedly to the grand jury, but even in his lies he provided some information of potential use to the intelligence community – including potential leads as to the location of his confederate Harun and the location of Harun's files in Kenya. Unfortunately, as el Hage left the grand jury room, we knew that we could not then prove el Hage's lies in court. And we also knew that the law did not clearly provide for sharing grand jury information with the intelligence community. We did not want, however, to withhold information of intelligence value. Fortunately, we found a way to address the problem that in most other cases would not work. Upon request, el Hage voluntarily agreed to be debriefed by an FBI agent outside of the grand jury when it was explained that the FBI agent was not allowed in the grand jury but was also interested in what el Hage wanted to say. El Hage then repeated the essence of what he told the grand jury to the FBI agent, including his purported leads on the location of Harun and his files. The FBI then lawfully shared that information with others in the intelligence community. In essence, we solved the problem only by obtaining the consent of a since convicted terrorist. We should not have to rely on the generosity of al Qaeda terrorists to address the gaps in our national security.

As I mentioned earlier, the American Embassy in Nairobi, Kenya, was bombed in August 1998. Investigation in Kenya quickly determined that Harun (described above) was responsible for the bombing. (Harun had left Kenya in 1997 after the search of el Hage's Nairobi home, correctly fearing that American officials were looking for him. Harun returned in 1998 to

carry out the bombing.) Harun's missing files were uncovered in the investigation of the bombing, stored at a charity office in Nairobi. (Harun remains a fugitive today and an important al Qaeda operative.) The point here is that had el Hage provided truthful information about the al Qaeda cell in Kenya a year before the embassy attacks, the rules then in existence did not provide for the sharing of that grand jury material had the team not used the FBI interview to work around the problem. This example should not be written off as "no harm, no foul": we should not have to wait for people to die with no other explanation than the law blocked the sharing of specific information that provably would have saved those lives before acting. The Patriot Act addressed that problem of separating the dots from those charged with connecting them.

These concrete examples demonstrate that the need to tear down the wall between criminal and intelligence investigations was real and compelling and not abstract. Section 218 did this by eliminating the "primary purpose" requirement discussed above. Under section 218, the government may now conduct FISA surveillance or searches if the gathering of foreign intelligence is a "significant" purpose of the surveillance or search, thus eliminating the need for courts to compare the relative weight of the "intelligence" and "law enforcement purposes" of the surveillance or search. This means that law enforcement and intelligence personnel can now share information without worrying that by doing so they will be jeopardizing the government's ability to continue ongoing FISA surveillance or introduce evidence in court. It is important to point out, however, that section 218 did nothing to alter the requirement that the Foreign Intelligence Surveillance Court may only authorize surveillance or searches under FISA when it finds that there is probable cause to believe that the target is a foreign power or an agent of a foreign

power, such as a terrorist or spy, and that section 218 was found to be constitutional in a unanimous decision of the FISA Court of Review in 2002.

I can tell you from personal experience that section 218 has made a huge difference in the way we approach national security. Today, as United States Attorney in Chicago, the prosecutors in my office enjoy a good working relationship with the FBI agents in Chicago. We are aware of the intelligence investigations they do and they are aware of our criminal cases and we coordinate to make sure that the law is followed and that all information is shared appropriately. In simple terms, we are making sure that if people who pose a threat to our country *can* be arrested, my office knows about it. Then together with the FBI we decide what, if any, national security sources and methods would be exposed by a prosecution and make an informed decision whether it is in the interest of our country's national security to proceed. It sounds simple and logical. It is. But it was not that way before the Patriot Act.

Let me give you a concrete example. In 2003, FBI agents had for several years been conducting an intelligence investigation regarding Khaled Dumeisi's activities on behalf of the Government of Iraq. Dumeisi had been living in the Chicago area and publishing a newspaper. However, Dumeisi had been gathering information (including telephone records) on Iraqi opposition figures in the Chicago area and transmitting the information to the Iraqi Intelligence Service. Dumeisi also provided Iraqi spies with false press credentials and recorded conversations with Iraqi opposition figures through the use of hidden microphones. In the past, such an espionage investigation would be conducted with little interaction with prosecutors. However, because of the ability in 2003 to share information which had both intelligence value and constituted evidence of a federal crime without compromising the ability to conduct FISA

surveillance, the intelligence agents worked together with prosecutors in my office to assemble a case against Dumeisi for serving as an unregistered agent of a foreign power, as well as for perjury. Dumeisi was convicted after trial in January 2004, and sentenced to 46 months in prison.

The Dumeisi case is far from unique. Efforts to increase coordination and information sharing between intelligence and law enforcement officers have been undertaken nationwide.

CLOSING

Mr. Chairman, I thank you for inviting me here and giving me the opportunity to explain in concrete terms how the Patriot Act has changed the way we fight terrorism. I would like to thank this Committee for its continued leadership and support. I also wish to assure this Committee that the men and women of the Northern District of Illinois, and the U.S. Attorney's Offices elsewhere in the country, appreciate the Constitution and the values it represents as we go about out work. With your support we will continue to make great strides in keeping both our country and our Constitution safe.

I will be happy to respond to any questions you may have.

Mr. CHABOT. Thank you very much.
Mr. Kris, you're recognized for 5 minutes.

TESTIMONY OF DAVID S. KRIS, VICE PRESIDENT FOR CORPORATE COMPLIANCE, TIME WARNER CORPORATION

Mr. KRIS. Mr. Chairman, Ranking Member Scott, thank you for the opportunity to testify about the FISA "wall" and the role of the PATRIOT Act in tearing it down.

As you know, I worked on these matters when I was at the Department of Justice. And although I've been out of Government since May of 2003, I have maintained an interest in national security issues. And I need to emphasize at the very outset that, in appearing before you today, I'm doing so only as an individual, and not as a representative of any former or current employer, including the Department and Time Warner.

My written testimony lays out in detail the legal background and the history of the FISA "wall." And subject to your questions, I don't intend to repeat any of that material here. Instead, in keeping with the 5-minute rule, I would like to make two brief points.

The first is that, regardless of your views on "The Wall" or the PATRIOT Act, whether you think it's a good thing or a bad thing, you should do something about the upcoming sunset of section 218.

[Sound of buzzer.]

Mr. CHABOT. Go ahead.

Mr. KRIS. I thought maybe my time had run out.

Mr. CHABOT. No. That just means that the House is going back into session. So there could be votes at some point from here on.

Mr. KRIS. Right.

Mr. CHABOT. But don't worry about it.

Mr. KRIS. The reason that you should do something is because, if you do nothing and just allow the sun to set, I predict that you will thereby expand, rather than contract, Governmental power in this area. And the reasons for that are laid out in detail in my written testimony.

Mr. SCOTT. Say that again.

Mr. KRIS. I predict that, if you allow the sun to set on section 218, you will thereby expand the Government's power in this area, for the reasons that are in my testimony. And I don't hear Mr. Fitzgerald asking for any broader authority. And indeed, even if he were, I don't think that the gains from that would be——

[Repeated sounds of buzzer.]

Mr. KRIS. This is——

Mr. CHABOT. Now they're just doing that to annoy us. So go ahead.

Mr. KRIS. I don't think the gains would be worth the attendant confusion. So my first point is that you should do something. And I guess that's why you're holding these hearings.

My second point is one that I think will strike you as perhaps a little strange, because it, I think, flies in the face of conventional wisdom. But nonetheless, I believe there is substantial reason to think that civil liberties are better protected with "The Wall" down, than they are with "The Wall" up.

And here's why: With "The Wall" down, DOJ prosecutors—and there are a lot of them; like Mr. Fitzgerald, they're smart and ener-

getic—enjoy full legal access to domestic national security investigations and matters. And from that lawyer access, if it's done right, comes lawyer oversight of these investigations. And lawyer oversight is how this country has protected civil liberties in the area of national security since at least the Church Commission report in the 1970's. And obviously, it is today the civil liberties backbone of Executive Order 12333.

So tearing down "The Wall" has the effect of opening up these investigations to a substantially larger pool of lawyers. And I think that is a good thing for civil liberties.

On the other hand, if "The Wall" is up, DOJ prosecutors lose a substantial amount of that access and, in particular, their ability to recommend law enforcement solutions to national security problems. That, after all, is the very essence of "The Wall."

And yet, I think there will always be some cases in which a national security threat must be dealt with through incarceration or detention of one or more individuals. That is just the nature of the business: Sometimes you have to lock somebody up. And in those cases, "The Wall" has a tendency to channel the Government toward methods of achieving that kind of detention and incarceration that do not require the involvement of civilian law enforcement personnel.

And regardless of what the alternatives to civilian prosecution were in 1978, today, obviously, one of the alternatives is military detention, or tribunals. Now, I hasten to state that I am not saying there's anything wrong with military justice, one way or the other. I'm not taking any position on that matter. But I am saying, I think, that from a pure civil liberties perspective, at least after the Supreme Court's decision in Hamdi, it's clear that military justice need not involve all of the same due process protections as civilian justice. And so I think for that reason as well, there is a good basis for expecting that civil libertarians should prefer "The Wall" to be down.

One last caveat. I see my time has almost expired. I don't mean to raise the specter of mass enemy combatant designations if "The Wall" is rebuilt. That would be silly. But I do mean to say this. "The Wall" has a tendency to deprive prosecutors of their seat at the table when the Government comes together in an inter-agency forum to decide what to do in a case—let's say, the Moussaoui case or something like it. And anyone who has ever been through a contentious inter-agency meeting in the Executive Branch, as I have, knows one iron-clad rule of the bureaucracy. And that is that the absent agency rarely prevails. Thank you very much.

[The prepared statement of Mr. Kris follows:]

PREPARED STATEMENT OF DAVID S. KRIS

Written Testimony of David S. Kris before the
House Committee on the Judiciary,
Subcommittee on Crime, Terrorism, and Homeland Security
April 28, 2005

Mr. Chairman, Ranking Member Scott, and Members of the Subcommittee: Thank you for the opportunity to testify about the Foreign Intelligence Surveillance Act (FISA) "wall" between intelligence and law enforcement, and the role of the USA Patriot Act in tearing it down.[1] As you know, I worked on this issue when I was at the Department of Justice (DOJ), and while I have been out of government since May 2003, I maintain an active interest in national security matters. Of course, in appearing before you today, I speak only for myself, and not for any former or current employer, including DOJ and Time Warner Inc.

My written testimony begins by looking backward, describing in some detail the rise and fall of the FISA wall. To understand the wall, it is necessary first to understand FISA: As the Foreign Intelligence Surveillance Court of Review observed in November 2002, the wall "emerges from [an] implicit interpretation of FISA."[2] Accordingly, Part 1 of my testimony summarizes the provisions of FISA that gave rise to the wall – those requiring that electronic surveillance and physical searches be motivated (at least in part) by a "purpose" to obtain "foreign intelligence information." Part 2 explains how interpretation of those provisions led to limits on coordination between intelligence and law enforcement, and also describes efforts by the Department to overcome those limits both before and after September 11, 2001. Thus, for example, Part 2 discusses internal DOJ procedures from July 1995 and thereafter, Sections 218 and 504 of the Patriot Act, and the government's first appeal from the Foreign Intelligence Surveillance Court (FISC) to the Court of Review.

Part 3 of my testimony looks forward, and tries to predict what will happen according to whether the sun is allowed to set on Section 218.[3] I do not pretend to be neutral on these matters, and so my written testimony also offers recommendations about what should be done. But caveat emptor: my recommendations arise from my experience, which is now nearly two years out of date; the government witnesses, including Mr. Fitzgerald, will surely have more current information available to them.

1. FISA's "Purpose" and "Foreign Intelligence Information" Provisions.

As you know, FISA governs electronic surveillance and physical searches of foreign powers and their agents inside the United States. Applications for FISC orders authorizing searches or surveillance must contain two important statements that bear on the FISA wall. First, each application must identify or describe the target of the search or surveillance, and must establish that the target is either a "foreign power" or an "agent of a foreign power" – terms that are defined in the statute.[4] To approve the application, a judge of the FISC must find "probable cause" to believe that the target of the search or surveillance is a foreign power or an agent of a foreign power.[5]

Second, each FISA application must include a certification from a high-ranking Executive Branch official, such as the Director of the FBI, concerning the purpose of the search or surveillance. As enacted in 1978, FISA required the official to certify that "the purpose" of a surveillance was to obtain "foreign intelligence information."[6] In October 2001, Section 218 of the USA Patriot Act amended FISA by replacing "the purpose" with "a significant purpose" in the required certification. To approve the FISA application where the target of the search or surveillance is a "United States person" – *e.g.*, a U.S. citizen or permanent resident alien – the FISC must find that the government's certification is not "clearly erroneous."[7]

a. The "Primary Purpose" Test.

The FISA wall emerged from interpretations of FISA's purpose requirements. Before the Patriot Act, those requirements raised two legal questions. First, how much purpose to obtain foreign intelligence information does the statute require? Must obtaining foreign intelligence information be the government's sole purpose, the primary purpose, a substantial purpose, a significant purpose, or merely a non-trivial purpose for conducting a search or surveillance? Following a 1980 decision,[8] every federal court of appeals to decide the issue before the Patriot Act held that the government's "primary purpose" must be to obtain foreign intelligence information.[9]

The second question is definitional: What, exactly, is "foreign intelligence information"? Since 1978, FISA has defined that term to include "information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against" attack, sabotage, international terrorism, or espionage committed by a foreign power or an agent of a foreign power.[10] As this language makes clear, "foreign intelligence information" must be relevant or necessary to "protect" against foreign threats to national security, but FISA does not prescribe how the information may or must be used to achieve that protection. In other words, FISA does not discriminate between protection through intelligence, diplomatic, economic, military, or law enforcement efforts, other than to require that those efforts be "lawful."[11] The 1978 legislative history of FISA confirms the statute's plain language.[12]

Nonetheless, beginning in the 1980s, the federal courts generally either implicitly assumed or concluded that "foreign intelligence information" excludes information relevant or necessary to protect national security using law enforcement methods.[13] Under this approach, information needed to recruit an international terrorist as a double agent was foreign intelligence information, because recruitment is a method of protecting against terrorism that does not involve law enforcement. However, information needed to indict and prosecute an international terrorist was not foreign intelligence information. Although prosecution clearly can protect against terrorism – by deterring, incapacitating, or encouraging cooperation from terrorists in exchange for leniency – prosecution is a law enforcement method.[14] By drawing this distinction, courts created a dichotomy between law enforcement methods and all other methods (including intelligence methods) of protecting national security.[15]

In keeping with these judicial interpretations of FISA, prosecution of an international terrorist could be a secondary purpose of FISA surveillance, but not the primary purpose. If prosecution became – or was perceived to have become – the primary purpose of FISA surveillance, then the surveillance would have to stop, and any evidence thereafter obtained or derived from FISA would be suppressed.[16]

In their oversight capacities, the House and Senate Intelligence Committees expressed support for this restrictive approach. For example, the Senate Intelligence Committee opined in a 1984 report that "the Justice Department should" not use FISA "when it is clear that the main concern with respect to a terrorist group is domestic law enforcement and criminal prosecution."[17] The House Intelligence Committee announced a similar opinion that same year, arguing that "the wiser course" is not to use FISA "once prosecution is contemplated, unless articulable reasons of national security dictate otherwise."[18]

b. Application of the "Primary Purpose" Test.

To determine the government's primary purpose for using FISA in particular cases, courts could not rely on who was being targeted, or even on what information the government obtained or tried to obtain from the search or surveillance. That is because a FISA wiretap conducted for a law enforcement purpose – such as prosecuting a spy for espionage – would typically be indistinguishable on those grounds from a FISA wiretap conducted for a traditional intelligence purpose – such as recruiting the spy as a double agent. By and large, the same individuals would be targeted, and the same facilities would be monitored to the same degree, in both cases. As the FISC acknowledged, "most information intercepted or seized" under FISA is of interest to both law enforcement and intelligence officials alike – "*e.g.*, the identity of a spy's handler; his/her communications signals and deaddrop locations; the fact that a terrorist is taking flying lessons, or purchasing explosive chemicals."[19]

Unable to rely on who or what was being searched or surveilled, courts instead determined the government's purpose by reviewing consultations between intelligence and law enforcement officials. The more consultations that occurred concerning an intelligence investigation, or the use of FISA within that investigation, the more likely courts were to find an improper law enforcement purpose. Although there are relatively few published cases in this area, in an important decision issued in 1980, a federal appeals court determined the government's primary purpose by examining the consultations between intelligence agents (who were conducting the surveillance) and prosecutors (who eventually brought espionage charges against the defendant).[20] The court of appeals agreed with the district court's decision to suppress evidence obtained from electronic surveillance after consultations and coordination had shifted the government's "primary purpose" to prosecution:

> In this case, the district court concluded that on July 20, 1977, the investigation of [the defendant] had become primarily a criminal investigation. Although the Criminal Division of the Justice Department had been aware of the investigation

> from its inception, until summer the Criminal Division had not taken a central role in the investigation. On July 19 and July 20, however, several memoranda circulated between the Justice Department and the various intelligence and national security agencies indicating that the government had begun to assemble a criminal prosecution. On the facts of this case, the district court's finding that July 20 was the critical date when the investigation became primarily a criminal investigation was clearly correct.[21]

In February 1995, the Department of Justice's Office of Legal Counsel (OLC) prepared a memorandum summarizing the law in this area. After discussing the relevant cases, the OLC memorandum concluded that "courts are more likely to adopt the 'primary purpose' test than any less stringent formulation," and that "the greater the involvement of prosecutors in the planning and execution of FISA searches, the greater is the chance that the government could not assert in good faith that the 'primary purpose' was the collection of foreign intelligence."[22]

2. The FISA Wall.

The foundations of the FISA wall lie in the "primary purpose" test as described above. The history of the wall – its rise and subsequent fall – can be divided into several discrete periods: (a) from FISA's enactment in 1978 to the investigation of Aldrich Ames in 1993 and 1994; (b) July 1995, when DOJ adopted new internal coordination procedures; (c) DOJ's efforts to overcome limits on coordination associated with the July 1995 procedures before September 11, 2001; (d) the USA Patriot Act, which was signed into law by the President in October 2001; (e) efforts to implement the Patriot Act with the FISC, culminating in the FISC's decision in May 2002; and (f) the government's appeal to the Court of Review, culminating in the Court of Review's decision in November 2002. Each of these periods is described below.

a. From FISA's Enactment to the *Ames* Case.

In response to court decisions adopting the "primary purpose" test (and perhaps also in light of Congressional preferences), the Department of Justice limited coordination between its intelligence and law enforcement officials. The early history of the FISA wall is recounted in an authoritative report issued in May 2000 by the Attorney General's Review Team (AGRT) – a group directed by Attorney General Janet Reno to evaluate the handling of the espionage investigation of Wen Ho Lee. According to the AGRT Report, from 1984 to 1993, under unwritten rules, the Criminal Division was regularly briefed by the FBI about ongoing intelligence investigations concerning espionage, and was allowed to assert that an intelligence investigation should be transformed into a criminal investigation. However, prosecutors "knew [they] were not to 'direct' the [intelligence] investigation or to suggest the use of FISA for criminal investigative purposes."[23] Thus, the Department of Justice's Criminal Division played only a "defensive role" in coordinating with intelligence officials of that era.[24]

In 1993 and early 1994, during the investigation of Aldrich Ames, coordination between intelligence and law enforcement officials apparently became quite robust. As explained in the AGRT Report, this troubled the then-Counsel for Intelligence Policy, who heads the Office of Intelligence Policy and Review (OIPR), a Department of Justice component that represents the government before the FISC. The Counsel "raised concerns with the Attorney General that the FISA statute had been violated by these contacts" between intelligence and law enforcement officials.[25] The Counsel believed that coordination "during the Ames investigation could be used by defense counsel to cast doubt upon the 'primary purpose' of the FISA surveillance and thereby jeopardize the prosecution."[26] There may also have been concerns about whether the FISC would continue to grant FISA applications. Thereafter, according to the AGRT Report, the "'backdoor' channel between the FBI and [the Criminal Division] was * * * closed. Because of the perceived threat to obtaining FISA coverage, [FBI] Deputy Director Bryant made it clear to the agents that this was a 'career-stopper' if they violated this rule."[27]

b. The July 1995 Procedures.

On July 19, 1995, following discussions among various Department of Justice components growing out of the aftermath of the *Ames* case, Attorney General Reno approved FISA coordination procedures that applied in most cases.[28] By their terms, the July 1995 Procedures required a certain level of coordination. For example, they directed the FBI to notify prosecutors when information developed in an intelligence investigation "reasonably indicate[d]" the commission of a "significant federal crime."[29] Moreover, where FISA was being used in an intelligence investigation, the July 1995 Procedures allowed the Criminal Division to give "guidance to the FBI aimed at preserving the option of a criminal prosecution," a standard understood to permit advice designed to avoid a "'screw up'" of the potential criminal case.[30]

In practice under the July 1995 Procedures, however, coordination was limited in three important ways. First, although the Procedures allowed advice aimed at "preserving" the possibility of prosecution, by negative implication the Criminal Division was understood not to be authorized to give advice aimed at "enhancing" the possibility of a prosecution. In practice, it turned out, the line between preserving and enhancing advice was so murky that advice-giving was substantially curtailed.[31] Indeed, the July 1995 Procedures warned the FBI and the Criminal Division to "ensure that advice intended to preserve the option of a criminal prosecution does not inadvertently result in either fact or the appearance of the Criminal Division's directing or controlling the [intelligence] investigation toward law enforcement objectives,"[32] a standard that encouraged reticence in the face of uncertainty about what was authorized. Second, concerns about limits on advice-giving also inhibited information-sharing.[33] As the AGRT Report explains, OIPR sought to limit advice-giving between intelligence and law enforcement, and its "presence at meetings between the FBI and the Criminal Division" was characterized as "'intimidating' because of concerns about jeopardizing FISA coverage by asking for advice."[34] Thus, meetings between intelligence and law enforcement officials did not include "ordinary interaction between agents and prosecutors"; instead, these meetings were "'surreal' and 'weird,'" with "an OIPR attorney present to hear the [FBI's] briefing and [the Criminal Division] acting like a 'potted plant.'"[35]

Third, although the July 1995 Procedures did not expressly require OIPR to attend meetings between the FBI and the Criminal Division, OIPR's desire to attend created "substantial delays in scheduling" the meetings.[36] OIPR understood that it was limiting coordination, but it believed that such limits were necessary to avoid violations.[37]

c. Efforts to Improve Coordination Before September 11, 2001.

The Department of Justice was aware of problems arising from limits on coordination well before the September 11, 2001 attacks, and it made efforts to overcome the limits, but with only modest success.[38] The AGRT Report describes unsuccessful efforts to deal with coordination issues in 1996 and 1997, including a memo clarifying the July 1995 Procedures that was never sent, and a working group that disbanded without making a written recommendation for change.[39] In January 2000, Attorney General Reno directed the FBI to provide the Criminal Division with all of its annual "letterhead memoranda" (LHMs) summarizing espionage investigations of U.S. persons.[40] Also in 2000, the Department created several high-level working groups to consider the recommendations set forth in the AGRT Report, including one group that submitted several proposed revisions to the July 1995 Procedures that were never acted upon.[41]

During the spring and summer of 2001, DOJ implemented other changes to the FISA program, including some measures designed to ensure coordination and compliance with the July 1995 Procedures.[42] On August 6, 2001, the July 1995 Procedures were clarified and modified in a memo issued by Deputy Attorney General Larry Thompson.[43] The August 2001 memo was the product of two conflicting concerns: the Department's understanding of problems resulting from the wall, and its inability to tear down the wall unilaterally.[44] The memo began by observing that the July 1995 Procedures "remain in effect today."[45] It maintained the important requirement that law enforcement be notified when facts or circumstances developed in the intelligence investigation "reasonably indicate that a significant federal crime has been, is being, or may be committed." But the August 2001 memo also clarified several important elements from the July 1995 Procedures – that the notification requirement is mandatory; that a "reasonable indication" is less than probable cause but more than a mere hunch; that "significant federal crime" includes any federal felony; and that when notification is required it is required without delay. The August 2001 memo prescribed monthly briefings of the Criminal Division by the FBI on all intelligence cases that meet the notification standards. In an apparent bow to the FISC, the memo required the FBI to notify OIPR before contacting the Criminal Division, and to give OIPR a "reasonable opportunity to be present for such contacts," not merely to be notified of them.[46] The August 2001 memorandum did not change the advice-giving standards in the July 1995 Procedures.

d. The USA Patriot Act.

In early September 2001, shortly after the attacks, DOJ sent Congress an amendment to FISA designed to permit greater coordination between intelligence and law enforcement. The amendment, which ultimately became Section 218 of the Patriot Act, was based on the 1995 OLC memorandum discussed above, and would have replaced "the purpose" with "a purpose" in the

certification provisions of 50 U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B). This amendment did not challenge the courts' interpretation of "foreign intelligence information" to exclude information sought for law enforcement efforts to protect national security. Instead, it made clear that law enforcement may nevertheless be the primary purpose of FISA searches or surveillance as long as "a purpose" remains that does not involve law enforcement. Eventually, the Department of Justice acceded to Congressional preferences, and "a purpose" was changed to a "significant purpose" in the final version of Section 218.[47] The basic approach and effect of the amendment, however, remained unchanged.

A second wall-related amendment in the Patriot Act came from Senator Leahy. In its final form as Section 504 of the Patriot Act, this amendment provided:

> (1) Federal officers who conduct [electronic surveillance or physical searches] to acquire foreign intelligence information under this title may consult with Federal law enforcement officers to coordinate efforts to investigate or protect against –
>
> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.
>
> (2) Coordination authorized under paragraph (1) shall not preclude the certification required by [50 U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B)] or the entry of an order under [50 U.S.C. §§ 1805 and 1824].[48]

Section 504 took a different approach than Section 218. Rather than changing the amount of "purpose" required for a FISA search or surveillance, it seemed to reflect an understanding that "foreign intelligence information" included information sought for law enforcement efforts to protect national security. That is because, in defining the scope of authorized consultation and coordination, Section 504 incorporated verbatim the foreign threats to national security that are specified in the definition of "foreign intelligence information" – attack, sabotage, terrorism, and espionage committed by foreign powers or their agents.[49] It authorized consultations to coordinate the government's "law enforcement" and intelligence "efforts to investigate or protect" against such threats. Thus, the amendment seemed to recognize that law enforcement investigations and efforts, as well as intelligence investigations and efforts, can "protect" against the threats, in keeping with the original meaning of "foreign intelligence information."

Moreover, Section 504 provided that authorized coordination "shall not preclude" the statutorily required certification or finding of a purpose to obtain foreign intelligence information.

That aspect of the amendment followed logically from its basic tenet: By definition, coordination authorized by Section 504 must be in furtherance of a purpose to protect against the threats specified in the definition of "foreign intelligence information"; accordingly, authorized coordination cannot "preclude" a purpose to obtain foreign intelligence information – on the contrary, it is affirmative evidence of that purpose. In any event, that was the meaning the Department of Justice ultimately ascribed to the amendment; others did not always agree.[50]

e. Implementation of the Patriot Act in the FISC.

Even armed with Sections 218 and 504, Department of Justice initially could not tear down the wall. In November 2001, in the first FISA applications filed after the Patriot Act, the FISC blocked efforts to implement the Act. In the words of the Court of Review, the FISC "took portions of the Attorney General's augmented 1995 Procedures – adopted to deal with the primary purpose standard – and imposed them generically as minimization procedures" in all cases.[51] Thereafter, components within the Department of Justice considered how to respond to the FISC's order.[52]

On March 6, 2002, Attorney General Ashcroft adopted new coordination procedures to replace the July 1995 Procedures. The March 2002 Procedures generally permitted the total exchange of information and advice between intelligence and law enforcement officials, emphasizing that "[t]he overriding need to protect the national security from foreign threats compels a full and free exchange of information and ideas."[53] Part II.A of the Procedures, which governs information-sharing, provided that with minor exceptions, prosecutors "shall have access to all information developed in full field [intelligence] investigations" that are conducted by the FBI, including investigations in which FISA is being used.[54] Correspondingly, the FBI was essentially required to keep prosecutors "apprised of all information" from such investigations.[55] Part II.B of the Procedures, which governs advice-giving, allowed prosecutors to provide advice to the FBI about "all issues"[56] in an intelligence investigation, including advice about the use of FISA.[57] It directed the FBI, OIPR, and prosecutors to meet regularly, and as needed, to conduct consultations.[58] The March 2002 Procedures explicitly permitted consultations directly between prosecutors and the FBI, without OIPR present.[59]

In an order issued in May 2002, the FISC accepted some aspects of the March 2002 Procedures and rejected others.[60] The FISC accepted in full the information-sharing provisions of the Procedures, Part II.A. Thus, the FISC approved the Department's standards generally allowing wholesale dissemination of information from intelligence investigations to law enforcement officials, subject to specific limits imposed in particular cases.[61] This was an evolutionary change, not a revolutionary change, from the July 1995 Procedures as modified in January 2000 and August 2001.

However, the FISC rejected much of Part II.B of the March 2002 Procedures, which allows law enforcement officials to give advice to intelligence officials. Instead of allowing consultation and coordination on "all issues" necessary to protect the United States from foreign

threats to national security, the FISC held that prosecutors and intelligence agents may consult on certain specified matters,[62] and imposed three limits on advice-giving. First, it held that law enforcement officials may "not make recommendations to intelligence officials concerning the initiation, operation, continuation or expansion of FISA searches or surveillances," and warned law enforcement officials not to "direct or control the use of FISA procedures to enhance criminal prosecution."[63] Second, the FISC instructed the FBI and prosecutors to "ensure that advice designed to preserve the option of a criminal prosecution does not inadvertently result in [prosecutors'] directing or controlling the investigation using FISA searches and surveillances toward law enforcement objectives."[64] Third, the FISC imposed a "chaperone" requirement, holding that prosecutors may not consult with intelligence agents unless they first invite OIPR to participate in the consultation, and that OIPR must participate unless it is "unable" to do so. If OIPR does not participate, the FISC held, it "shall be apprised of the substance of the meetings forthwith in writing so that the [FISC] may be notified at the earliest opportunity."[65]

f. The FISA Appeal.

Dissatisfied with the FISC's decision, the Department of Justice decided to appeal to the Foreign Intelligence Surveillance Court of Review, a court that had never before been convened.[66] The Department of Justice submitted two briefs to the Court of Review, and the American Civil Liberties Union and the National Association of Criminal Defense Lawyers each submitted an amicus brief in support of the FISC's decision (though they did not participate in oral argument).[67]

In November 2002, the Court of Review reversed the FISC's decision and upheld in full the March 2002 Procedures. It held that FISA allows complete coordination between intelligence and law enforcement officials, even if such coordination results in what might be characterized as law enforcement "direction" or "control" of an investigation.[68] Under the Court of Review's decision, FISA may be used primarily for the purpose of obtaining evidence to prosecute a foreign spy or terrorist, and prosecutors may provide any advice, including advice on the use of FISA itself, in furtherance of such a purpose.[69] The Court found "simply no basis" for the FISC's decision "to limit criminal prosecutors' ability to advise FBI intelligence officials on the initiation, operation, continuation, or expansion of FISA surveillances to obtain foreign intelligence information, even if such information includes evidence of a foreign intelligence crime."[70] Indeed, the Court of Review stated that in doing so the FISC "may well have exceeded the constitutional bounds that restrict an Article III court."[71] There are three important aspects to the Court of Review's decision, each of which is discussed below: (i) its interpretation of FISA as enacted in 1978; (ii) its interpretation of Sections 218 and 504 of the Patriot Act; and (iii) its conclusions about the nature and scope of judicial review of the government's purpose for using FISA.

i. The Court of Review began by analyzing FISA as enacted in 1978. Reviewing the statutory definitions of "foreign power," "agent of a foreign power," and "foreign intelligence information," the Court of Review concluded that the latter term "includes evidence of crimes such as espionage, sabotage or terrorism."[72] Reviewing the House and Senate Reports, the Court found that they "cast [no] doubt on the obvious reading of the statutory language." Thus, the

"FISA passed by Congress in 1978 clearly did not preclude or limit the government's use or proposed use of foreign intelligence information, which included evidence of certain kinds of criminal activity, in a criminal prosecution."[73] Indeed, the Court concluded, "it is virtually impossible to read the 1978 FISA to exclude from its purpose the prosecution of foreign intelligence crimes."[74]

In light of the text and legislative history of FISA, the Court of Review found it "quite puzzling that the Justice Department, at some point during the 1980s, began to read the statute as limiting the Department's ability to obtain FISA orders if it intended to prosecute the targeted agents [of a foreign power] – even for foreign intelligence crimes."[75] By 1995, however, the Court of Review understood that the Department was hemmed in, acknowledging that the Procedures issued in July of that year limited coordination "[a]pparently to avoid running afoul of the primary purpose test used by some courts."[76] The Court of Review stated: "We certainly understand the 1995 Justice Department's effort to avoid difficulty with the [FISC], or other courts; and we have no basis to criticize any organization of the Justice Department that an Attorney General desires."[77]

The Court of Review's analysis meant that, as enacted in 1978, FISA could have been used not just primarily, but exclusively to obtain evidence needed to prosecute a spy or terrorist, because such evidence was itself "foreign intelligence information." Accordingly, there was never any need to build a wall between intelligence and law enforcement. To be sure, FISA could not be used against ordinary criminals, because they posed no foreign threat to national security. Thus, Bonnie and Clyde, John Gotti, and corrupt Wall Street traders were immune from FISA surveillance. The same was true of Timothy McVeigh – as a domestic terrorist, evidence of his crimes was not (and is not) "foreign intelligence information."[78] But international spies, terrorists, and saboteurs whom the government intended to prosecute were fair game for FISA surveillance and searches.

ii. Had that been the end of the Court's opinion, it would have been a clean theoretical win for the government. In an unusual twist, however, the Court of Review took its analysis of the Patriot Act one step further. Having criticized the misreading of FISA that prevailed since the 1980s, the Court acknowledged that the misreading had also prevailed when Congress passed Section 218 of the Patriot Act – because DOJ had decided not to challenge it – and so the Court concluded that the Act implicitly codified the misreading into law. The Court explained: "even though we agree that the original FISA did not contemplate the 'false dichotomy' [between intelligence and law enforcement], the Patriot Act actually did – which makes it no longer false."[79] Thus, the Court of Review concluded, FISA today cannot be used exclusively to gather evidence for prosecution – even prosecution of a terrorist. Under the "significant purpose" amendment, it can be used primarily for such a prosecution, as long as a significant non-law enforcement purpose remains. According to the Court of Review, therefore, Section 218 of the USA Patriot Act actually reduced the government's authority under FISA.[80]

The Court of Review also imposed a second limit on the use of FISA. It held that FISA may be used primarily to obtain evidence for a criminal prosecution, but only if the prosecution concerns an offense related to a foreign intelligence threat. The Court divided crimes into two categories: "foreign intelligence crimes" and "ordinary crimes." A foreign intelligence crime is any crime "referred to in section 1801(a)-(e)" of FISA – i.e., espionage and international terrorism, unlawful clandestine intelligence activities, sabotage, identity fraud offenses committed for or on behalf of a foreign power, and aiding and abetting or conspiring to commit these offenses.[81] Moreover, any crime inextricably intertwined with foreign intelligence activity – such as a bank robbery committed to finance terrorist activity, or credit card fraud designed to maintain the cover of a sleeper spy – is also a foreign intelligence crime.[82] By contrast, an ordinary crime is one "'totally unrelated to intelligence matters,'"[83] such as when a foreign spy murders his wife to be with his mistress, or when an international terrorist is also a consumer of child pornography. The Court held that FISA may be used primarily to obtain evidence of a foreign intelligence crime, but not of an ordinary crime.[84]

iii. The Court of Review also changed the nature and scope of judicial inquiry into the government's purpose for using FISA. Under prior law, as noted above, the FISC (and other courts) determined the government's purpose by reviewing consultations and coordination between line attorneys and agents, and compared intelligence and law enforcement purposes to find which one was primary. The Court of Review flatly rejected that approach. It held that the Patriot Act "eliminated any justification for the [FISC] to balance the relative weight the government places on criminal prosecution as compared to other counterintelligence responses."[85] Thus, the significance of a foreign intelligence purpose is judged on its own terms, and does not vary according to the significance of a law enforcement purpose.

More importantly, the Court of Review also held that the government's purpose is determined by the high-level certification that is a part of every FISA application, not the coordination between line attorneys and agents in the field. Thus, the Court held, the significant purpose test is "not a standard whose application the [FISC] legitimately reviews by seeking to inquire into which Justice Department officials" – law enforcement or intelligence – "were instigators of an investigation" or a request to use FISA.[86] Rather, "the government's purpose * * * is to be judged by the national security official's articulation [in the FISA certification], and not by a [FISC] inquiry into the origins of an investigation nor an examination of the personnel involved."[87] The "relevant purpose is that of those senior officials in the Executive Branch who have the responsibility of appraising the government's national security needs," and if the Attorney General "wishes a particular investigation to be run by an officer of any division, that is his prerogative."[88] Where the FISC has doubts, "it can demand further inquiry into the certifying officer's purpose," but an inquisition of line attorneys and agents would be inappropriate because the certification represents the government's purpose regardless of "whatever may be the subjective intent of the investigators or lawyers who initiate an investigation."[89]

3. The Future.

The rise and fall of the FISA wall is a case study in our Constitutional system of divided government. It took all three branches of the national government to build the wall: Congress had to express a policy preference for separating law enforcement and intelligence; courts had to issue opinions implicitly reading FISA to require such separation; and the Department of Justice had to accede to those interpretations and apply them internally. Correspondingly, it took all three branches of government to tear down the wall: Congress had to pass the Patriot Act (and the President had to sign it); the Justice Department had to take an unprecedented appeal advancing novel legal arguments; and the Court of Review had to issue its decision substantially agreeing with those arguments.

Future progress will also require cooperation among the branches of government. Set out below are (a) several predictions about what will happen depending on how Congress and the President respond to the upcoming Patriot Act sunset; and (b) my recommendations for how best to move forward.

a. Predictions.

The Subcommittee is holding these hearings because Congress now faces the question whether to renew Section 218 of the Patriot Act (Section 504 is not subject to the sunset provisions).[90] In practical terms, Congress must choose among three possibilities: (i) do nothing, and allow Section 218 to sunset; (ii) renew Section 218, and maintain the status quo; or (iii) explicitly rebuild the wall. Each of these three possibilities is discussed below.

i. If Congress does nothing, Section 218 will generally sunset at the end of this year. Ironically, I believe the sunset will probably expand the government's authority. As explained above, the Court of Review concluded that, as enacted in 1978, FISA could be used exclusively, not just primarily, to gather evidence for use in a criminal prosecution of a spy or terrorist. In other words, Section 218 actually reduced the government's authority by requiring a "significant" non-law enforcement purpose where no such purpose was required before. If Section 218 sunsets, the government will almost surely argue that the original (newly discovered) meaning of FISA has been restored. I have not made a detailed study of the law in this area, but my sense is that DOJ may well prevail in that argument. And you may be confident that DOJ will base its argument in part on the idea that Congress implicitly endorsed broader governmental power because, although it was on notice – through briefings I gave in 2002 and today's hearings – it did not act to stop the sun from setting.[91]

ii. If Congress renews Section 218, it will effectively endorse the status quo. If you decide to do this – as I believe you should for reasons explained below – it makes sense not only to lift the sunset, but also explicitly to endorse the reasoning and result of the Court of Review. Whether or not you agree with its outcome, the Court of Review's opinion is a very sophisticated and technically sound interpretation of a complex statute. If Congress were to adopt its reasoning, it would provide guidance that is equally sophisticated and sound. That, above all, is what the country needs in this area. This could be done either through explicit legislative history

endorsing the Court of Review's decision, or (perhaps better) through a "sense of the Congress" provision that is actually passed.

iii. Finally, if you prefer to rebuild the wall, and return to the "primary purpose" test, then you should change "significant" to "primary" in the certification provisions of 50 U.S.C. §§ 1804(a)(7)(B) and 1823(a)(7)(B), repeal Section 504, and amend the definition of "foreign intelligence information" by adding the phrase, "not including protection against the foregoing using law enforcement methods, such as criminal prosecution," immediately after 50 U.S.C. § 1801(e)(1)(C). Obviously, I believe this would be a grave error.

b. Recommendations.

In my view, Congress should eliminate the sunset on Section 218 and explicitly endorse the reasoning and decision of the Court of Review. That approach has three main virtues: (i) it makes us safer because it improves the efficiency and effectiveness of the government's efforts to protect against foreign threats to national security; (ii) it enhances protections for civil liberties; and (iii) it offers much-needed stability in a vital area of law.

i. Keeping the wall down will make us safer. For those with little experience in law enforcement or national security investigations, the harm caused by limits on coordination may not be obvious. But the harm is real. To protect national security effectively, domestic intelligence and law enforcement must closely coordinate their operational activities. Properly understood, they are separate but similar tools in the President's national security toolbox – far more similar to each other than either one is to other tools like diplomacy, military strikes, covert paramilitary action, or economic initiatives. They seek much the same information about foreign spies and terrorists, particularly within the United States, and they use many of the same investigative techniques to collect and process that information – for example, judicially approved, targeted searches and wiretaps (*e.g.*, under FISA or Title III); undercover agents and recruited informants; and lures or "honeypots" to attract would-be perpetrators (though law enforcement is here somewhat circumscribed by entrapment doctrine).[92] These similarities apply not only to investigations of espionage and terrorism themselves, but also to investigations of ordinary crimes committed to finance or otherwise facilitate espionage and terrorism.[93]

The similarities between intelligence and law enforcement make coordination essential. As I testified before the Senate Judiciary Committee in September 2002 (as a government witness):

> When we identify a spy or a terrorist, we have to pursue a coordinated, integrated, coherent response. We need all of our best people, intelligence and law enforcement alike, working together to neutralize the threat. In some cases, the best protection is prosecution – like the recent prosecution of Robert Hanssen for espionage. In other cases, prosecution is a bad idea, and another method – such as recruitment – is called for. Sometimes you need to use both methods. But we

can't make a rational decision until everyone is allowed to sit down together and brainstorm about what to do.[94]

Law enforcement officials can add value to an intelligence investigation by bringing perspective, expertise, and certain investigative tools. By and large, as a result of their training and experience, prosecutors and other law enforcement officials are able and inclined to address national security threats through law enforcement efforts.[95] By bringing that perspective to bear, law enforcement officials may identify ways to neutralize a national security threat that do not occur to counterintelligence officials. For example, an Assistant United States Attorney may be better than an FBI intelligence agent or an OIPR lawyer at identifying a viable prosecution for providing material support to a terrorist organization.[96] If such a prosecution puts a stop to fundraising by terrorists, it protects national security.

Law enforcement officials also have expertise in conducting complex investigations and assembling cases generally, and there is a growing cadre of federal prosecutors with extensive expertise in espionage and terrorism cases. Law enforcement officials can offer assistance to intelligence agents in formulating an interview strategy to obtain leads to additional or corroborating information. They can also help to ensure that undercover operations are designed to avoid entrapment or other legal problems. Law enforcement officials experienced in national security cases can provide valuable strategic and tactical guidance on a variety of issues that may aid in protecting sensitive sources and methods and other classified information from exposure in future litigation. Such expertise helps to ensure the success of any prosecution that may occur and also helps even if no prosecution ever occurs. Many law enforcement officials have expertise in financial review and analysis, and can assist intelligence agents in reviewing complex money trails. In that respect, particularly, their expertise may assist the investigation even if no prosecution is ever brought. Of course, intelligence officials also have expertise in certain of these areas; adding law enforcement officials to the mix can only enhance that expertise.

Finally, prosecutors and other law enforcement officials provide certain investigative tools that are not available to counterintelligence officials. Prosecutors can use the grand jury not only to obtain documents, but to compel testimony in furtherance of a lawful criminal investigation.[97] National security letters, which may be issued by FBI agents, and FISA tangible things orders, which may be issued by the FISC, are not as powerful, primarily because they cannot compel the attendance of witnesses.[98] Prosecutors can invoke mutual legal assistance treaties with other nations. And, of course, prosecutors can offer immunity from prosecution or motions for reduction in sentence in exchange for cooperation,[99] which may in certain cases produce extraordinary foreign intelligence information.[100]

In my 2002 testimony before your Senate counterparts, I offered a medical analogy, comparing terrorism to cancer. Both involve cells that are hidden in a larger organism and that attempt to kill the organism. In some cases, cancer is best treated with surgery as terrorism is best treated with prosecution. In other cases, however, cancer is best treated with chemotherapy as terrorism is best treated with intelligence methods. In some cases, both approaches are

required. But no rational patient would seek treatment at a hospital where the surgeons and oncologists cannot coordinate about how best to stop the disease. Or, to be more precise and carry the analogy one step further, no rational patient would go to a hospital where, if the surgeons and oncologists do coordinate, they will be forbidden from using their most effective diagnostic tool – in medicine, an X-ray or MRI machine; in national security, FISA.[101]

ii. Although conventional wisdom says otherwise, I believe that keeping the wall down will, if anything, enhance protections for civil liberties. To understand why, it is important to remember that the wall does not prevent the use in criminal trials of evidence obtained or derived from FISA; such use has always been permitted.[102] Nor does the wall prevent any search or surveillance from occurring – as long as the intelligence officials using FISA are careful to eschew any contact with law enforcement officials. The only direct function of the wall is to prevent coordination – it is explicitly designed to stop the government from connecting the dots. Its secondary effect may be to prevent use of FISA information in criminal trials, but only because prosecutors don't have timely knowledge of, or input into, intelligence investigations.

With the wall down, more DOJ lawyers may become more involved in national security investigations, as they are now involved in ordinary criminal investigations. More lawyers means more oversight, and lawyer oversight of intelligence matters is how this country has protected civil liberties for more than 30 years – since the Church Committee report, as currently embodied in Executive Order 12333, and as recently endorsed by the WMD Commission. Civil libertarians ought to oppose the wall because its main effect is to keep lawyers out of intelligence investigations.

Some fear that prosecutors may push national security investigations towards law enforcement remedies. As a complaint about civil liberties (rather than effectiveness), however, this strikes me as quite misguided. If the government confronts a national security threat, and determines that the best way to protect against the threat is to incarcerate someone, civilian prosecution is one obvious option. With the wall down, and prosecutors at the table, civilian prosecution becomes a real possibility. By contrast, with the wall up, and prosecutors excluded from discussions, civilian prosecution is much less likely to prevail as the remedy of choice. In a case where detention is required, other methods may therefore be used, including immigration or military detention.[103] I am not saying there is anything wrong with those approaches, but the Supreme Court has held that "the full protections that accompany challenges to detentions in other settings may prove unworkable and inappropriate in the enemy-combatant setting," at least when the U.S. citizen involved was captured on the battlefield abroad.[104] Let me be clear: I do not mean to raise the specter of mass military detentions if the wall is rebuilt. I mean only to say that civil libertarians generally support lawyer oversight of national security activities, and they generally prefer civilian to military justice, and that they therefore ought to welcome the involvement of prosecutors in national security investigations, and oppose the wall.

iii. Finally, endorsing the Court of Review's decision yields stability. Although the Court of Review's decision binds the FISC, and the government, it is not the last word in this area

because it does not control any other federal court. Any district court, or court of appeals, may have to interpret the statute in the context of a criminal case in which information obtained or derived from FISA is used.[105] If Congress explicitly adopts or endorses the Court of Review's decision, and makes corresponding legislative changes, however, the statutory question will be resolved universally. On the constitutional front, the Court of Review's analysis is quite persuasive, and will be even more persuasive with an explicit Congressional endorsement. From the perspective of safety, and the perspective of civil liberties, this country needs a clear and stable articulation of the law. Congress is now in a position to provide that.

To offer one practical example illustrating the need for clarity and stability, consider the training of DOJ and FBI personnel. Following the Court of Review's decision in November 2002, Attorney General Ashcroft and Deputy Attorney General Thompson ordered extensive training for all Department personnel who work on national security matters. This order culminated in multiple training sessions, of several days' duration, for thousands of FBI agents and DOJ lawyers in the spring and summer of 2003. The training included instructors from the Criminal Division, U.S. Attorneys' Offices, OIPR, FBI, CIA, Department of Homeland Security, and other agencies. The highlight of the training was a hypothetical exercise that unfolded in 12 discrete segments and required participants to use the legal and practical knowledge they had gained to protect the country from a dirty bomb attack, with emphasis on coordination and information-sharing. The training, and particularly the hypothetical exercise, was generally well received. If the wall is later rebuilt, however, the Department of Justice will have to expend equal time and energy to re-train its personnel – this time, to avoid coordination. It will take months, or years, for that re-training to take hold.

c. National Security Division.

At the risk of exceeding my mandate, I would like to close with one more recommendation. If the legal wall between intelligence and law enforcement remains down, as I believe it should, then Congress should also discuss a corresponding organizational change. I agree with the WMD Commission that Congress and the President should at least consider creating a National Security Division inside the Department of Justice. A National Security Division would make us safer in three important ways, and it would also help safeguard civil liberties. It answers the long-standing question of whether to create an American version of Britain's MI-5, with a solution tailored to the counter-intelligence training, culture, and traditions of our country.[106]

First, a National Security Division would quickly improve coordination within the Department of Justice itself. At a time when the national security mission is preeminent, DOJ is structured as if national security were an afterthought. Its principal responsibilities in this area – searches and surveillance, law enforcement, economic security, information security, and emergency planning – are scattered far and wide within the agency. Moreover, apart from a few high-level staffers in the Department's front offices, there is no real umbrella structure to hold the

pieces together. A National Security Division would streamline the current hodgepodge, foster coherent operational and policy development, and help establish a distinct DOJ national security culture.

Second, a National Security Division would facilitate coordination between DOJ and other federal, state, and private-sector entities. The Department today has no single, central point of contact for national security matters. As a result, when other members of the U.S. Intelligence Community want to coordinate with DOJ, they literally may not know where to call. Worse, when they don't want to coordinate, they can forum shop (without breaching inter-agency protocol) by contacting the DOJ component least likely to oppose their desires, hoping that DOJ doesn't connect the dots in time to bring its other national security components to the table.

Third – and most important – a National Security Division would make the FBI more effective. For more than 50 years, the Bureau has trained its agents to work closely with DOJ lawyers. Particularly in complex cases, lawyers and agents coordinate from the beginning, in part because many of the most effective investigative techniques – including subpoenas, search warrants, electronic surveillance, and certain undercover operations – require DOJ's participation. Experience shows unequivocally that agents and lawyers working together produce better results than either group working alone, whether or not a case ends up being litigated in court.

In national security matters, however, the FBI and DOJ continue to operate as if it were 1940, with agents and lawyers working apart rather than together. Until November 2002, when a federal court dismantled the legal wall between counter-intelligence and law enforcement, prosecutors were kept away from national security investigations and programs, and other elements of DOJ lacked the personnel to participate fully in them. A National Security Division would have the authority, resources, focus, and clout to work closely with the FBI, both at headquarters and in the field. It would modernize the FBI by taking advantage of the agent-lawyer cooperative model that works so well in other contexts. It would represent the best American analogue to MI-5.

Last, but not least, as discussed above, a National Security Division could only enhance protection of civil liberties by bringing lawyers – with their legal expertise and perspective – into national security operations as they now participate in law enforcement operations. Thus, for example, just as DOJ lawyers have long sat on the committee that reviews risky FBI undercover operations in criminal cases, so they would now sit on its national security counterpart.

The principal argument against creating a National Security Division is that it would separate national security lawyers from other prosecutors, and thereby reduce the synergies between them. This is not a trivial argument. But DOJ has specialized prosecutors in its Antitrust, Civil Rights, Environmental, and Tax Divisions because of a belief that greater synergies arise from grouping employees by mission rather than by the legal technique designed to achieve that mission. Thus it was that the civil rights section of the Department's Criminal Division became the criminal section of its Civil Rights Division when the latter was created in

1957. In that era, the move reflected a belief that prosecution would be most effective as part of a single, coordinated effort using all available methods to protect civil rights. Today, I believe, the same is true of national security.

The *New York Times* reported recently that DOJ is considering the creation of a National Security Division.[107] It makes eminent sense for Congress to give DOJ the first crack at this issue, and the opportunity to write either a proposal for creating a National Security Division or an explanation of why it should not be created. Congress need not take the lead on this, but could require a report from DOJ within 180 days.

Thank you for the opportunity to testify on these important and interesting matters.

Notes

1. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA Patriot Act), Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001). This testimony is based primarily on the November 2002 decision of the Foreign Intelligence Surveillance Court of Review (FISCR or Court of Review), *In re Sealed Case*, 310 F.3d 717 (per curiam); the Brief and Supplemental Brief for the United States filed in connection with that decision; and the May 2000 *Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation* (AGRT Report). In places, the statement uses portions of the government's briefs verbatim, without quotation marks (I was the principal author of those briefs). Other sources are cited and quoted in the traditional manner. An earlier version of this document, containing certain client confidences as authorized by the Department of Justice, was submitted to the National Commission on Terrorist Attacks Upon the United States. This testimony contains no client confidences and was approved for publication by the Department of Justice under 28 C.F.R. § 17.18.

2. *In re Sealed Case*, 310 F.3d at 721.

3. See Patriot Act Section 224. Section 224 provides generally for a December 31, 2005 sunset for several provisions of the Patriot Act, including Section 218. There is no sunset provision for Section 504 of the Patriot Act.

4. 50 U.S.C. §§ 1804(a)(3), 1804(a)(4)(A), 1823(a)(3), 1823(a)(4)(A). A "foreign power" is defined by FISA to include, among other things, a "foreign government or any component thereof," and a "group engaged in international terrorism." 50 U.S.C. §§ 1801(a)(1), (4). The statute defines "agent of a foreign power" to include any person who "knowingly engages in * * * international terrorism * * * for or on behalf of a foreign power," and any person "other than a United States person" – *e.g.*, someone other than a U.S. citizen or permanent resident alien – who is a "member" of a group engaged in international terrorism. 50 U.S.C. §§ 1801(b)(1)(A), (b)(2)(C), (i). "International terrorism" is defined by FISA to require activities that (1) involve violent or dangerous acts that violate U.S. law (or would do so if committed here); (2) appear to be intended to "intimidate or coerce" a civilian population, to "influence" government policy through "intimidation or coercion," or to "affect the conduct of government by assassination or kidnapping"; and (3) either "occur totally outside the United States, or transcend national boundaries" in various ways. 50 U.S.C. § 1801(c).

5. 50 U.S.C. §§ 1805(a)(3)(A), 1824(a)(3)(A).

6. 50 U.S.C. § 1804(a)(7)(B).

7. 50 U.S.C. §§ 1805, 1824; H.R. Rep. No. 95-1283, Part I, 95th Cong., 2d Sess. 80-81 (1978) [hereinafter House Report].

8. *United States* v. *Truong Dinh Hung*, 629 F.2d 908 (4th Cir. 1980). *Truong* applied pre-FISA law because the surveillance in question took place before enactment of the statute, *id.* at 914 n.4, but it exerted a profound influence on later decisions applying FISA. See *In re Sealed Case*, 310 F.3d at 725 (noting that the "origin of * * * the * * * dichotomy between foreign intelligence information that is evidence of foreign intelligence crimes and that which is not appears to have been" *Truong*).

9. See *United States* v. *Duggan*, 743 F.2d 59, 78 (2d Cir. 1984); *United States* v. *Badia*, 827 F.2d 1458, 1464 (11th Cir. 1987); *United States* v. *Pelton*, 835 F.2d 1067, 1075 (4th Cir. 1987); *United States* v. *Johnson*, 952 F.2d 565, 572 (1st Cir. 1992).

10. The threats specified in the definition of "foreign intelligence information" are:

> (A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;
>
> (B) sabotage or international terrorism by a foreign power or an agent of a foreign power; or
>
> (C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

50 U.S.C. § 1801(e)(1). A second definition of "foreign intelligence information," in 50 U.S.C. § 1801(e)(2), includes information relevant or necessary to "the national defense of the United States" or "the conduct of the foreign affairs of the United States." This definition, which generally involves information referred to as "affirmative" or "positive" foreign intelligence rather than "protective" foreign intelligence or "counterintelligence" information, is rarely the object of surveillances in which purpose issues arise, because affirmative intelligence information is usually not evidence of a crime. See S. Rep. No. 95-701, 95th Cong., 2d Sess. 11 & n.4 (1978) [hereinafter Senate Intelligence Report].

11. 50 U.S.C. §§ 1806(a), 1825(a). The statute provides that no "information acquired pursuant to" a search or surveillance may be "disclosed for law enforcement purposes" or "used in a criminal proceeding" absent the Attorney General's permission. 50 U.S.C. §§ 1806(b), 1825(c). This provision is designed to ensure that an aggrieved party receives notice that he was subject to FISA searches or surveillance so that he may seek suppression of evidence obtained or derived from FISA before it is used in a "trial" or other proceeding. 50 U.S.C. §§ 1806(c) and (e), 1825(d) and (f). See House Report at 88-90.

12. The House Report on the 1978 version of FISA provides:

> Finally, the term "foreign intelligence information," especially as defined in [50 U.S.C. §§ 1801(e)(1)(B) and (e)(1)(C)], can include evidence of certain crimes relating to sabotage, international terrorism, or clandestine intelligence activities.

> With respect to information concerning U.S. persons, foreign intelligence information includes information necessary to protect against clandestine intelligence activities of foreign powers or their agents. Information about a spy's espionage activities obviously is within this definition, and it is most likely at the same time evidence of criminal activities. How this information may be used to "protect" against clandestine intelligence activities is not prescribed by the definition of foreign intelligence information, although of course, how it is used may be affected by minimization procedures, *see* [50 U.S.C. § 1801(h)]. And no information acquired pursuant to this bill could be used for other than lawful purposes, *see* [50 U.S.C. § 1806(a)]. Obviously, use of "foreign intelligence information" as evidence in a criminal trial is one way the Government can lawfully protect against clandestine intelligence activities, sabotage, and international terrorism. The bill, therefore, explicitly recognizes that information which is evidence of crimes involving clandestine intelligence activities, sabotage, and international terrorism can be sought, retained, and used pursuant to this bill.

House Report at 49 (emphasis added).

The Senate Intelligence Committee's report on the 1978 version of FISA contains similar language:

> Electronic surveillance for foreign counterintelligence and counterterrorism purposes requires different standards and procedures. U.S. persons may be authorized targets, and the surveillance is part of an investigative process often designed to protect against the commission of serious crimes such as espionage, sabotage, assassination, kidnaping, and terrorist acts committed by or on behalf of foreign powers. Intelligence and criminal law enforcement tend to merge in this area.

Senate Intelligence Report at 10-11 (emphasis added, footnote omitted). As noted in the government's principal brief on appeal to the Court of Review (pages 38-39 & n.13), and in the Court's opinion (310 F.3d at 725), there are some contrary indications in the legislative history, but they are not sufficient to overcome the clear meaning of the language quoted above (as well as other, similar language elsewhere in the legislative history).

13. In *Duggan*, 743 F.2d at 78, the court affirmed a conviction because "the purpose of the surveillance in this case, both initially and throughout, was to secure foreign intelligence information and was not, as [the] defendants assert, directed towards criminal investigation or the institution of a criminal prosecution." In *Badia*, 827 F.2d at 1464, the court relied on a finding that the surveillance "did not have as its purpose the primary objective of investigating a criminal act. Rather, surveillance was sought for the valid purpose of acquiring foreign intelligence information, as defined by § 1801(e)(1)." Similarly, in *Pelton*, 835 F.2d at 1075, the court "reject[ed] Pelton's claim that the 1985 FISA surveillance was conducted primarily for the purpose of his criminal prosecution, and not primarily 'for the purpose of obtaining foreign

intelligence information' as required by" FISA. And in *Johnson*, 952 F.2d at 572, the court relied on its conclusion that the "primary purpose" of the surveillance, "from the first authorization in July 1988, to July 1989, when appellants were arrested, was to obtain foreign intelligence information, not to collect evidence for any criminal prosecution of appellants."

14. As the government argued in its principal brief on appeal to the Court of Review (page 33):

> Prosecution is often a most effective means of protecting national security. For example, the recent prosecution of Ahmed Ressam, who was charged with attempting to destroy Los Angeles International Airport, protected the United States by incapacitating Ressam himself from committing further attacks, and by deterring others who might have contemplated similar action. Moreover, as a result of his conviction and sentence, Ressam agreed to cooperate with the government and provided information about the training that he received at an al Qaeda camp overseas. That kind of prosecution thus protects the United States directly, by neutralizing a threat, and indirectly, by generating additional foreign intelligence information. The same is true of the recent prosecution of Robert Hanssen: By far the best source of intelligence on Hanssen's espionage activities is Hanssen himself; and the government gained access to Hanssen only as a result of his capture, prosecution, and plea agreement.

The Court of Review agreed (310 F.3d at 724): "The government argues persuasively 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."

15. In some ways, this dichotomy goes back at least to the law enforcement proviso of the National Security Act of 1947, which prescribed the jurisdiction of the CIA and the FBI, and prohibited the CIA from engaging in domestic law enforcement. The proviso states that the CIA "shall have no police, subpoena, or law enforcement powers or internal security functions." 50 U.S.C. § 403-3(d)(1). The purposes of this proviso are to prevent the CIA from exercising the kind of combined internal security and external intelligence functions that have been characteristic of intelligence agencies in police states and to prevent jurisdictional conflicts between the CIA and the FBI.

The law enforcement proviso has generally not been interpreted to exclude the CIA from all domestic law enforcement-related activities. Rather (setting aside Section 105A of the Act), the proviso has been applied in accordance with the "principal purpose" test. See, *e.g.*, William C. Banks & M.E. Bowman, *Executive Authority for National Security Surveillance*, 50 Am. U. L. Rev. 1, 32-34 (2000) (discussing the Commission on CIA Activities Within the United States, more commonly known as the Rockefeller Commission). Under this interpretation, CIA may provide assistance requested by a law enforcement agency if CIA's principal purpose in doing so is a foreign intelligence or counterintelligence purpose. Prior to the enactment of Section 105A, the practical application of the test generally meant that CIA would provide a requesting law enforcement agency with previously collected or pre-existing CIA data, product, or equipment,

and would provide law enforcement agencies with information of "incidental" law enforcement value that CIA lawfully acquired during its authorized foreign intelligence activities. However, the CIA might well have been reluctant to undertake a new collection at the request of a law enforcement agency because of the risk that such a collection would be deemed inconsistent with the principal purpose test.

A request by a law enforcement agency for CIA to undertake a new collection directed against a United States person (inside or outside the United States) or directed against someone inside the United States (whether or not the proposed target is a U.S. person) raises issues under the "principal purpose" test. Any such request must be assessed on an individual basis to determine whether an independent, "principal" foreign intelligence purpose would be served by performing the collection. If the answer to that question is "No," the collection may not be undertaken. (Whether or not the principal purpose test is actually required by law, it is the standard actually used by the agencies in question – at least as far as I know.)

16. See 50 U.S.C. §§ 1806(e), 1825(f).

17. *The Foreign Intelligence Surveillance Act of 1978: The First Five Years*, S. Rep. No. 98-660, 98th Cong., 2d Sess. 15 (1984) [hereinafter Senate Five Year Report].

18. *Implementation of the Foreign Intelligence Surveillance Act*, H.R. Rep. No. 98-738, 98th Cong., 2d Sess. 6 (1984) [hereinafter House Five Year Report].

19. *In re All Matters Submitted to Foreign Intelligence Surveillance Court*, 218 F. Supp. 611, 617 (FISC 2002), rev'd, *In re Sealed Case*, 310 F.3d 717 (FISCR 2002).

20. *Truong*, *supra*, 629 F.2d 908. As mentioned above, note 8, *supra*, *Truong* was decided under pre-FISA standards, *id.* at 914 n.4, but it exerted a profound influence on later decisions applying FISA.

21. *Id.* at 916.

22. OLC Memo at 1.

23. IV *Final Report of the Attorney General's Review Team on the Handling of the Los Alamos National Laboratory Investigation*, Chapter 20, at 711 (May 2000) [hereinafter AGRT Report]. According to the AGRT Report (page 711), there were no written FISA guidelines or procedures governing coordination during this period. Prior versions of the Attorney General Guidelines for FBI Foreign Intelligence Collection and Foreign Counterintelligence Investigations [hereinafter FCI Guidelines] provided that "information obtained from [FISA] electronic surveillance and physical searches" could be disseminated under "[FISA] court ordered minimization procedures." FCI Guidelines, Part VII.B.3 (May 1995). See <<http://www.usdoj.gov/ag/readingroom/terrorismintel2.pdf>>. (Earlier and later versions of the FCI Guidelines, from 1983 and 1999, were substantially similar. See AGRT Report at 714 n. 948.) FISA's statutory minimization provisions require the government to follow procedures in

conducting a search or surveillance that are "reasonably designed" to "minimize" the acquisition of nonpublic information concerning unconsenting U.S. persons "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. §§ 1801(h)(1), 1821(4)(A). The minimization provisions also provide, "notwithstanding" the rules governing foreign intelligence information, for retention and dissemination (but not acquisition) of "evidence of a crime" for "law enforcement purposes." 50 U.S.C. §§ 1801(h)(3), 1821(4)(C). Minimization procedures are discussed at length in the government's principal brief on appeal to the Court of Review (pages 6, 27-30, 41-45) and in the Court's opinion (310 F.3d at 730-732 and 728 n.16). In November 2003, the FCI Guidelines were substantially modified and renamed the Attorney General's Guidelines for FBI National Security Investigations and Foreign Intelligence Collection [hereinafter NSI Guidelines]. See <<http://www.usdoj.gov/olp/nsifactsheet.pdf>>.

24. AGRT Report at 712. The AGRT Report also states that this system, with the Criminal Division in a "defensive" role, "appears to have worked quite satisfactorily * * * both from the perspective of the Criminal Division and from that of the FBI." *Ibid.*

25. *Id.* at 713.

26. *Ibid.*

27. *Id.* at 714.

28.The Southern District of New York operated under a different set of rules, known as the SDNY Annex, and the investigation of the first World Trade Center bombing was also subject to a separate set of rules articulated in a memorandum issued by Deputy Attorney General Gorelick. Among other things, the Gorelick Memo directed the assignment of (1) an Assistant United States Attorney who had "knowledge of, but no active involvement in, the ongoing criminal investigations" to review information developed in the intelligence investigation, and (2) an FBI agent from the criminal investigation who would "remain involved in the on-going trial" but would "otherwise be assigned to the foreign counterintelligence investigation."

29. July 1995 Procedures, Part A, at ¶ 1.

30. *Id.* Part A, at ¶ 6; AGRT Report at 727. The July 1995 Procedures also cautioned the Criminal Division and the FBI to "ensure" that any advice given did "not inadvertently result in either the fact or the appearance of the Criminal Division's directing or controlling the [intelligence] investigation toward law enforcement objectives." July 1995 Procedures, Part A, at ¶ 6. They directed the FBI to maintain "a log of all contacts with the Criminal Division," and required all FISA renewal applications to "apprise the FISC of the existence of, and basis for, any contacts among the FBI, the Criminal Division, and a U.S. Attorney's Office, in order to keep the FISC informed of the criminal justice aspects of the ongoing investigation." *Id.* Part A, at ¶¶ 4, 7.

31. See AGRT Report at 721-734; General Accounting Office, *FBI Intelligence Investigations: Coordination Within Justice on Counterintelligence Criminal Matters is Limited* (July 2001)

(GAO-01-780) [hereinafter GAO Report].

32. July 1995 Procedures, Part A, ¶ 6.

33. AGRT Report at 732.

34. *Id.* at 733.

35. *Id.* at 732.

36. *Id.* at 733.

37. *Ibid.* In its July 2001 report, the General Accounting Office suggested that regardless of the July 1995 Procedures, the Department of Justice was limiting coordination between intelligence and law enforcement officials to adhere to what it believed was the FISC's requirements. The GAO found that a "key factor inhibiting * * * coordination [between the FBI and the Criminal Division] is the concern over how the Foreign Intelligence Surveillance Court or another federal court might rule on the primary purpose of the surveillance or search in light of such coordination." GAO Report at 3. As discussed below, subsequent events proved that right. Even after the Patriot Act, the FISC did not allow the full range of coordination between intelligence and law enforcement, and insisted that OIPR continue to chaperone such coordination.

38. In May 2000, the AGRT Report recounted much of the history set forth in the text, and concluded (page 706) that "[i]t was predictable and, perhaps, inevitable that, sooner or later, a price would have to be paid for the Department's failure to fix this 'broken' and 'dysfunctional' relationship" between the FBI and the Criminal Division.

39. *Id.* at 709, 721-722. I am less familiar with these efforts because I was not involved in national security matters at this time. Officials in OIPR or other DOJ components would be more able to describe this period, including the ability of the Department to work with the FISA wall in particular investigations or periods, such as the weeks and months preceding January 1, 2000.

40. This sharing of LHMs did not implicate the concerns that arose from in-person meetings, where a conversation designed to share information from an investigation could easily morph into a conversation containing advice about how to conduct the investigation. However, it is fair to say, that directive and other efforts did not produce the desired results. As the GAO concluded, "Criminal Division officials opined that these procedures had helped to improve coordination," but that they were not enough. GAO Report at 4.

41. As the July 2001 GAO Report explains (at page 4):

> a [FISA] coordination working group headed by the Principal Associate Deputy Attorney General developed a decision memorandum in late 2000. The memorandum, which required the Attorney General's approval, recommended

> revisions to the 1995 procedures and detailed several options, including a preferred option, to address the differing interpretations on the advice issue. However, as of the completion of our review [in July 2001], no decision had been made on the memorandum. Consequently, these issues continue to be impediments to coordination. According to working group officials, among those issues discussed in the decision memorandum were (1) the type of advice the Criminal Division should be permitted to provide the FBI and (2) varying interpretations as to whether certain criminal violations are considered "significant violations" and, thus, trigger the Attorney General's 1995 coordination procedures.

As staff to the Deputy Attorney General, I worked on this decision memo, and subsequent decision memos on the same topic.

42. On April 4, 2001, the FBI adopted the so-called "Woods Procedures" (named after the FBI lawyer who was their principal author) to ensure coordination between FBI Headquarters and FBI field offices, and the accuracy of FISA applications. On May 18, 2001, Attorney General John Ashcroft issued a memorandum mandating direct contact between OIPR and FBI field offices; streamlined and standardized FISA applications; regular meetings to coordinate FISA priorities; training for FBI agents on the use of FISA and the July 1995 Procedures (which training was to be conducted jointly by law enforcement and intelligence officials); and a report on the feasibility of a classified e-mail system linking FBI Headquarters, FBI field offices, and the Main Justice Building. In June 2001, the Counsel for Intelligence Policy issued a memo to all OIPR staff prescribing measures to ensure that the Criminal Division would be advised if OIPR learned of information that met the July 1995 Procedures' notification standards. At around the same time, the Deputy Attorney General ordered the FBI to expand its inspections program to verify compliance with the July 1995 Procedures; the FBI established a "Foreign Intelligence/Counterintelligence Audit" inspections program in August 2001. As staff to the Deputy Attorney General, I worked on many of these matters.

43. As staff to Deputy Attorney General Thompson, I worked on drafting the August 2001 memo.

44. See note 37, *supra*. Confidential deliberations within the Executive Branch pertaining to the August 2001 memo, and confidential communications between DOJ and the FISC, are not discussed here.

45. August 2001 Memo at 1.

46. *Id*. at 3.

47. As a practical matter, that change was determined during a colloquy between Senator Feinstein and Attorney General Ashcroft during the latter's testimony before the Senate Judiciary Committee on September 25, 2001:

> Senator Feinstein: * * * I'd like to ask the same question I asked yesterday of Mr. [Kris], with the intention of really brining this to your attention. And this is on section 153, the Foreign Intelligence Information and that section aims to clarify that the certification of a FISA request is supportable where foreign intelligence-gathering is, quote, "A purpose of the investigation." Now, the primary purpose test, as you well know, has often been cited as one of the reasons that FISA meets the constitutional requirements under the Fourth Amendment, and we're concerned that the elimination of the test might place FISA in danger of being struck down by a court.
>
> Now, Mr. [Kris] testified that the department does not believe that will be the case. But I would like to ask this question; what would your view be if instead of adopting the attorney general's proposal, FISA was amended to allow for a substantial or significant purpose?

After turning to consult with his staff, Attorney General Ashcroft gave the following answer:

> I think if I were forced to say if we're going to make a change here, I think we would move toward thinking to say that if "a purpose" isn't satisfactory, saying "a significant purpose" reflects a considered judgment that would be the kind of balancing that I think we're all looking to find. If I were having to choose one of your words I think that's the one I would chose.

Thereafter, Senator Feinstein thanked the Attorney General, and all that remained to be done was the drafting by Senate legislative counsel. That is the essential story of the Patriot Act's "significant purpose" amendment. 2001 WL 1132689.

48. 50 U.S.C. §§ 1806(k), 1825(k) (emphasis added).

49. Compare 50 U.S.C. §§ 1806(k)(1)(A)-(C) and 1825(k)(1)(A)-(C), with 50 U.S.C. § 1801(e)(1)(A)-(C).

50. Here is how Senator Leahy described Section 504 at the time it was enacted (147 Cong. Rec. S11004 (Oct. 25, 2001) (emphasis added)):

> In addition, I proposed and the Administration agreed to an additional provision in Section 505 [later changed to Section 504] that clarifies the boundaries for consultation and coordination between officials who conduct FISA search and surveillance and Federal law enforcement officials including prosecutors. Such consultation and coordination is authorized for the enforcement of laws that protect against international terrorism, clandestine intelligence activities of foreign agents, and other grave foreign threats to the nation. Protection against these foreign-based threats by any lawful means is within the scope of the definition of 'foreign intelligence information,' and the use of FISA to

> gather evidence for the enforcement of these laws was contemplated in the enactment of FISA. The Justice Department's opinion cites relevant legislative history from the Senate Intelligence Committee's report in 1978, and there is comparable language in the House report.

Indeed, Senator Leahy and other Senators seemed to repeat this same argument – that "foreign intelligence information" includes information sought for use in prosecutions of foreign spies and terrorists – in a publicly available letter they sent to the FISC on July 31, 2002 (2002 WL 1949260):

> We appreciate that "foreign intelligence information" sought under FISA may be evidence of a crime that will be used for law enforcement purposes to protect against international terrorism, sabotage, and clandestine intelligence activities by foreign powers. * * * * [Quoting the 1978 House Report, the letter states that FISA] "explicitly recognizes that information which is evidence of crimes involving clandestine intelligence activities, sabotage, and international terrorism can be sought, retained, and used pursuant to this bill." * * * * Coordination between FBI Agents and prosecutors is essential to ensure that the information sought and obtained under FISA contributed most effectively to protecting the national security against such threats.

In its appeal to the Court of Review, the Department of Justice advanced this same argument – i.e., that Section 504 supported its (new) interpretation of FISA as enacted in 1978, because "foreign intelligence information" had always included information sought for law enforcement efforts to protect national security (*e.g.*, prosecuting a spy or terrorist). I testified before the Senate Judiciary Committee in September 2002 that Section 504 and Senator Leahy's letter to the FISC "corresponds exactly" to the government's arguments in the Court of Review. 2002 WL 31033656. (The Department itself did not assert this interpretation of Section 504, or the 1978 version of FISA, until its appeal to the Court of Review. To explain why would require revealing client confidences.)

At the September 2002 hearings, however, Senator Leahy himself strongly disagreed with that interpretation of Section 504:

> I was surprised to learn that as, quote "The drafter of the coordination amendment" close quote, of the USA Patriot Act, the [Department of Justice] cites my statement – cites a Leahy statement to support its argument that there is no longer a distinction between using FISA for a criminal prosecution and using it to collect foreign intelligence. Had the Department of Justice taken the time to pick up a phone and call me, and incidentally I have a listed phone number, both home and at the office, I would have told them that was not, and is not, my belief.

2002 WL 31031849. (This statement by Senator Leahy was included as footnote 7 of the

government's supplemental brief in the Court of Review.)

As explained in more detail in the text, the Court of Review concluded that the Patriot Act did not reinforce the original definition of "foreign intelligence information" to include information sought for the prosecution of a spy or terrorist. Indeed, the Court concluded that, despite Section 504, the Patriot Act did exactly the opposite, and affirmatively codified into law the historical misreading of the 1978 version of the statute. *In re Sealed Case*, 310 F.3d at 734-735.

51. *Id.* at 730.

52. Confidential deliberations within the Executive Branch are not discussed here.

53. March 2002 Procedures at 1.

54. *Id.* at 2-3.

55. *Id.* at 3.

56. *Ibid.*

57. *Id.* at 4.

58. *Ibid.*

59. *Ibid.*

60. *In re All Matters Submitted to Foreign Intelligence Surveillance Court*, 218 F.Supp.2d 611 (2002).

61. *Ibid.*

62. *Ibid.* The specified matters were:

> [1] exchanging information already acquired; [2] identifying categories of information needed and being sought; [3] preventing either [the law enforcement or intelligence] investigation or interest from obstructing or hindering the other; [4] [preventing the] compromise of either investigation; and [5] [formulating] long term objectives and overall strategy of both investigations in order to ensure that the overlapping intelligence and criminal interests of the United States are both achieved.

63. *Ibid.* Thus, for example, law enforcement officials could not nominate targets for FISA searches or surveillance. Nor could they recommend that an existing FISA search or surveillance be conducted in a particular way or seek particular information.

The FISC's only significant reliance on the USA Patriot Act was to make the new procedures arguably more restrictive than procedures that governed prior to the Act. As explained in the government's principal brief to the Court of Review, prior written intelligence sharing procedures governed consultations between intelligence agents and prosecutors, but not consultations between intelligence agents and law enforcement agents. The FISC's order, however, applied at least in part to law enforcement agents because it used the term "law enforcement officials" rather than "prosecutors." In response to a motion for clarification filed by the government, the FISC explained that "[t]he Court uses, and intended to use, the term 'law enforcement officials'" in its opinion and order "in conjunction with the source and context from which it originated, i.e., the recent amendments to the FISA." The FISC stated that "[t]he new minimization procedures apply to the minimization process in FISA electronic surveillances and physical searches, and to those involved in the process – including both FBI agents and criminal prosecutors."

64. *Ibid.* The FISC's approval of advice designed to "preserve" the option of a criminal prosecution, and its ban on advice amounting to prosecutorial "direction or control" of an investigation, led the government to file a motion for clarification. The motion inquired whether the FISC intended to permit advice designed to "enhance," rather than merely to "preserve," a criminal prosecution, a distinction addressed at length in the AGRT Report from May 2000. The motion asked the FISC either to delete the reference to "preserv[ing]" advice or to explain in more detail the scope of any ban on "enhancing" advice. The FISC did neither. This history is recounted on pages 18-20 of the government's principal brief in the Court of Review.

65. The FISC also adopted a new rule to the same effect: "All FISA applications shall include informative descriptions of any ongoing criminal investigations of FISA targets, as well as the substance of any consultations between the FBI and criminal prosecutors at the Department of Justice or a United States Attorney's Office." FISC Rule 11 (later vacated).

66. Due to jurisdictional limits, the Department did not appeal the order of the FISC that modified the March 2002 Procedures. Instead, it identified a particular case, applied to the FISC for an order in that case allowing it conduct surveillance while following the Attorney General's March 2002 Procedures (rather than the FISC-approved version of those procedures), and then appealed from the FISC's order in that particular case. See *In re Sealed Case*, 310 F.3d at 720-721.

67. *Id.* at 737.

68. *Id.* at 733-734.

69. *Ibid.*

70. *Id.* at 731.

71. *Ibid.*

72. *Id.* at 723.

73. *Id.* at 727 (emphasis in original).

74. *Id.* at 723. This interpretation of FISA may have been "impossible," but it did in fact prevail for nearly 25 years, during the tenure of several Attorneys General from both major political parties. Confidential deliberations within the Executive Branch are not discussed here.

75. *Ibid.*

76. *Id.* at 727.

77. *Id.* at 727 n.14.

78. Indeed, all of these criminals are and always have been safe from FISA for another, more fundamental reason – they are not "agents of a foreign power" as defined by FISA, and therefore not lawful FISA targets regardless of the government's purpose. See 50 U.S.C. § 1801(a)-(b).

79. *In re Sealed Case*, 310 F.3d at 735.

80. As a practical matter, this limitation is unlikely to inhibit necessary coordination between intelligence and law enforcement officials. Even when the government's prosecutorial purpose is at its zenith, there will still always (or almost always) be a "significant" non-prosecutorial purpose for conducting a FISA search or surveillance. For example, detection of espionage or terrorist communications networks, taskings, and other tradecraft will invariably assist in developing appropriate diplomatic, military, economic, or other non-law enforcement countermeasures. Use of these or other non-law enforcement countermeasures almost always is at least a significant purpose for conducting a search or surveillance under FISA. Indeed, the Court of Review itself recognized that this requirement "may not make much practical difference." *In Re Sealed Case*, 310 F.3d at 735. As the Court explained, if the FISA application "articulates a broader objective than criminal prosecution – such as stopping an ongoing conspiracy – and includes other potential non-prosecutorial responses, the government meets the statutory test." *Ibid.* The government should be able to meet that test, even when prosecution is its dominant motive.

81. *Id.* at 723 & n.10.

82. *Id.* at 736.

83. *Id.* at 731 (quoting FISA's 1978 legislative history).

84. The Court of Review did not make much effort to tie that limitation to the text of the statute. See 310 F.3d at 736 ("[W]e see not the slightest indication that Congress meant to give that power [to use FISA primarily to obtain information for the prosecution of an ordinary crime] to the Executive Branch. Accordingly, the manifestation of such a purpose, it seems to us, would continue to disqualify an application."). Of course, evidence of <u>any</u> crime obtained or derived from a lawful FISA search or surveillance may be used in a subsequent prosecution; the limit applies only to the government's purpose and intent to use information at the time it seeks and

conducts the search or surveillance. See 50 U.S.C. §§ 1801(h)(3) and 1821(4)(C).

The limitation should not inhibit necessary coordination. As a practical matter, it becomes an issue only when an intelligence investigation reveals a serious crime that is not related to foreign intelligence. That does not often occur, because most serious crimes committed by agents of foreign powers are in fact related to their foreign intelligence activities – *e.g.*, international terrorists tend to commit terrorism-related offenses (including crimes committed to fund or facilitate terrorism), and foreign spies tend to commit espionage-related offenses (including crimes committed to fund or facilitate espionage). When the issue does arise, it may be appropriate for the FISA application to explain why prosecution of that unrelated crime is not the primary purpose of the search or surveillance. That should not be difficult to establish.

85. *In re Sealed Case*, 310 F.3d at 735.

86. *Id.* at 736.

87. *Ibid.*

88. *Ibid.*

89. *Ibid.* In keeping with that analysis, the Court of Review rejected the FISC's Rule 11. Rule 11 required every FISA application to include "informative descriptions of any ongoing criminal investigations of FISA targets, as well as the substance of any consultations between the FBI and criminal prosecutors at the Department of Justice or a United States Attorney's Office." *Id.* at 729, 746. Descriptions of ongoing criminal investigations are unnecessary, the Court of Review concluded, because the significant purpose test does not require a comparison between intelligence and law enforcement motives. Descriptions of consultations among agents and prosecutors are unnecessary because the relevant purpose under FISA is determined by the certifying official and the Attorney General.

90. See Patriot Act Section 224.

91. If you decide that you want to expand DOJ's authority along these lines, and remove any statutory doubt, you should amend the definition of "foreign intelligence information" by adding the phrase "including protection against the foregoing using law enforcement methods, such as criminal prosecution," immediately after 50 U.S.C. § 1801(e)(1)(C).

92. For example, see "We Can Trap More Crooks With a Net Full of Honey," by Michael Schrage, *Washington Post*, Sunday, January 11, 2004, Outlook Section, pages B1 and B5 (noting government use of fake child pornography Internet sites known as "honeypots": "In fact, Operation Pin [a multi-national effort to crack down on child pornography using fake sites] and its honeypots – a term of art in espionage referring to female spies skilled in seduction and betrayal – reflects an emerging trend with enormous policy implications for the law, national security, commerce, and culture.").

93. That is not to minimize the important differences between intelligence and law enforcement. Much of law enforcement (particularly domestic law enforcement) has nothing to do with national security, and much of foreign intelligence (particularly affirmative intelligence) has nothing to do with law enforcement. Law enforcement remedies are always overt and serve many different goals – punishment, deterrence, incapacitation, and in some eras, rehabilitation – whereas intelligence remedies are often covert and are always focused on protection. The training, skills, perspective, and culture of government professionals in each area is necessarily somewhat different: George Smiley (or James Bond) would not be effective investigating crack cocaine dealers, and Dirty Harry would not be a good spycatcher.

94. Testimony of David S. Kris before the Senate Committee on the Judiciary, September 10, 2002. 2002 WL 31033656.

95. To be sure, that is not always the case, especially as the Department of Justice continues to move from a reactive to a proactive model of law enforcement. As a general matter, however, prosecutors have an ability to view counterintelligence investigations with a law enforcement perspective.

96. See 18 U.S.C. § 2339B.

97. See generally, *United States* v. *R. Enterprises, Inc.*, 498 U.S. 292 (1991).

98. See, *e.g.*, 15 U.S.C. § 1681u (national security letter); 50 U.S.C. § 1861 (FISA subpoena).

99. See, *e.g.*, 18 U.S.C. §§ 6001-6005 (immunity); United States Sentencing Guidelines § 5K1.1 (reduction in sentence).

100. Pages 701 to 706 of the AGRT Report provide some concrete examples of harm resulting from a lack of coordination in the investigation of Wen Ho Lee (also noting, however, the necessarily "speculative quality" of the analysis). Among the consequences of the wall in that case were the fact that "the Computer Crime Section of the Criminal Division was unable to serve as a critical resource for the FBI in 1996 when it was examining the issue of access to Wen Ho Lee's computer." The AGRT also describes the following contributions the Criminal Division could have made (assuming that there were no legal barriers): (1) Verification of the predicate for the investigation. (2) Authentication of [certain materials provided by a source]. (3) Establishing the case against Wen Ho Lee, particularly his motive and intent to commit espionage. (4) Preparation in the event that "Wen Ho Lee had headed for the airport." In particular, the AGRT Report poses the following questions the Criminal Division might have helped to answer: "Could he have been arrested? What about Sylvia [his wife]? And, if arrested, how exactly were the Criminal Division and a United States Attorney's Office supposed to put themselves in a position, essentially overnight, to even comprehend – let alone communicate to a court – the substance of an investigation that had been going on, to one extent or another, for more than four years?" (5) The interview and polygraph of Wen Ho Lee, and in particular "identification of matters to be addressed in a subject interview" and avoiding possible claims of coercion based on requirements

to cooperate stemming from Lee's status as a government employee.

101. This medical analogy, and my testimony in general, has been criticized. See, *e.g.*, William C. Banks, *And the Wall Came Tumbling Down: Secret Surveillance After the Terror*, 57 U. Miami L. Rev. 1147, 1172-1174 (2003).

102. See, *e.g.*, 50 U.S.C. §§ 1801(h), 1806.

103. See, *e.g.*, *Hamdi* v. *Rumsfeld*, 124 S. Ct. 2633 (2004).

104. *Id.* at 2650.

105. See 50 U.S.C. §§ 1806(3), 1825(f).

106. As understood by most Americans engaged in the current debate, MI-5 is a domestic security agency separate from law enforcement. Thus, creating an American MI-5 would require separating the FBI's national security elements from its law enforcement elements. The main argument in favor of such a proposal is cultural: Domestic intelligence professionals can prosper, and work effectively, only if they are freed from the shackles of a law enforcement mindset. An excessive focus on discrete "cases" rather than national "threats," and on law enforcement solutions rather than other solutions to these threats, makes the FBI ill-suited to the domestic intelligence mission. On the other hand, the main argument against splitting the FBI is that, culture aside, law enforcement and domestic intelligence must work together if they are to function effectively. Having dismantled the legal wall to permit operational coordination between intelligence and law enforcement, it makes no sense to replace it with a bureaucratic wall that inhibits such coordination. If these opposing arguments are in equipoise – I am not sure that they are – the tremendous transition costs associated with splitting the FBI counsel against such radical surgery.

107. See Eric Lichtblau, *A New Antiterror Agency is Considered*, New York Times page A13, March 25, 2005.

Mr. CHABOT. Thank you.
Ms. Martin, you're recognized for 5 minutes.

TESTIMONY OF KATE MARTIN, DIRECTOR, CENTER FOR NATIONAL SECURITY STUDIES

Ms. MARTIN. Thank you, Mr. Chairman and Ranking Member Scott, for the opportunity to testify here before you today. I first of all want to make clear that, as civil libertarians, we're not in favor of "The Wall"; and indeed, have never been in favor of "The Wall." In the 2 weeks after September 11th, we testified before the Congress in favor of more and better information sharing between intelligence and law enforcement communities.

I do think, though, it's important to note that the effect of section 218 is slightly more complicated, I think, than simply to say that it tore down "The Wall." Section 218—I'm sorry, the purpose requirement, which was changed by section 218, was interpreted by the Justice Department before September 11th as prohibiting contact between prosecutors and the FBI; an interpretation, by the way, which the FISA Court of Appeals after September 11th said was wrong.

The PATRIOT Act contains another section, 504, which explicitly provides that all FISA information may be shared with all law enforcement. And one of the things that I think is necessary in the current effort to find out about the use of the PATRIOT Act is to ask the question of the Justice Department about why section 218 is necessary, given section 504. What is it that section 218 adds in dismantling "The Wall" that 504 doesn't already give?

And the reason why it's important to ask that question is that section 218 doesn't simply tear down "The Wall." It makes FISA surveillance much more broadly available than it was before the passage of the PATRIOT Act. And it is that aspect of section 218 that I'd like to briefly focus on today.

Section 218—before September 11, it was understood that if the Government started out with the primary purpose of making a criminal case against an individual, it must use the criminal surveillance authorities; not the Foreign Intelligence Surveillance Act. Section 218 changed that, and allows the Government to now use the broad and secret authorities of the FISA when its primary purpose is not to obtain foreign intelligence information.

I suggest that one of the questions we don't yet have the answer to is how and why and when the Justice Department and the FBI decide to use the secret FISA authorities instead of the regular criminal authorities. And that's an important question to obtain the answer to.

Most importantly, I think that in looking at section 218 it's important for this Committee to look more broadly at the use, and possible abuse, of the FISA authorities; especially given the recent revelations about the secret FISA search of Brandon Mayfield, the Muslim lawyer in Portland, Oregon.

As the Committee knows, the FISA authorizes secret searches and secret wiretaps, not delayed-notice searches of the kind that are authorized under section 213 of the PATRIOT Act. It authorizes such secret searches and secret wiretaps with less probable

cause of criminal activity than is authorized in the fourth amendment in criminal investigations.

But there are two additional key features of FISA surveillance. The first is that in most instances, when Americans are targeted for secret searches and secret wiretaps under the FISA, they are never informed by the Government that the FBI has been inside their house, has copied their computer drives or, in some instances, seized their DNA. They are never informed that the FBI has been listening to their telephone conversations.

The second key difference between FISA surveillance and criminal surveillance is that when individuals are indicted, after having been targeted by FISA surveillance, then they are in fact informed. That's the only time they are informed of FISA surveillance. But even then, they are never provided with any kind of opportunity to look at any portion of the original application for the FISA warrant.

And the effect of that means that there is no adversarial judicial review of the propriety of a FISA search. It is true, of course, that a FISA judge initially approves a FISA surveillance. But on the criminal side, what we rely on to make sure that the fourth amendment was in fact complied with is after-the-fact judicial review of the search and the probable cause, in which the target of the search has a fair chance to participate and challenge whether or not there was in fact probable cause to begin with. That opportunity is missing in the FISA context.

And I would suggest that this Committee look into two possible amendments to address the problem of the searches being secret forever, and the second problem of no adequate chance to challenge the legality of the search when someone is indicted using FISA evidence.

[The prepared statement of Ms. Martin follows:]

PREPARED STATEMENT OF KATE MARTIN

Thank you, Mr. Chairman, for the honor and opportunity to testify today on behalf of the Center for National Security Studies. The Center is a civil liberties organization, which for 30 years has worked to insure that civil liberties and human rights are not eroded in the name of national security. The Center is guided by the conviction that our national security can and must be protected without undermining the fundamental rights of individuals guaranteed by the Bill of Rights. In our work on matters ranging from national security surveillance to intelligence oversight, we begin with the premise that both national security interests and civil liberties protections must be taken seriously and that by doing so, solutions to apparent conflicts can often be found without compromising either. The Center has worked for more than twenty years to protect the Fourth Amendment rights of Americans to be free of unreasonable searches and seizures, especially when conducted in the name of national security. For example, the Center, then affiliated with the American Civil Liberties Union, was asked to testify before Congress when the Foreign Intelligence Surveillance Act was first enacted. In 1994, when Congress amended the Act to include physical searches, we were again asked to testify about the civil liberties and constitutional implications of that legislation.

We appreciate the role this Committee has taken in connection with the USA Patriot Act, beginning with the work that was done before its enactment to build in protections for civil liberties while the government's surveillance powers were increased. Since its enactment, the Committee has vigorously pursued information from the Justice Department concerning the use of the Act, and we commend the Committee for now holding this series of oversight hearings.

However, we do not believe that the Congress yet has enough information to make permanent certain key provisions of the Patriot Act, particularly section 218 and those relating to information-sharing. (My testimony today does not address the spe-

cific provisions of the Patriot Act relating to information-sharing, sections 203 and 905, as that is the subject of another hearing. However, we do not believe that the Congress yet has adequate information about how the law enforcement community, including the FBI, determines what information about Americans should be shared with the CIA and other intelligence agencies, what specific safeguards exist against abuse, or how the agencies insure that they recognize and act appropriately on important information. For further information, please see the article on section 203 of the Act at *www.patriotdebates.com.*)

The subject of today's hearing is section 218 of the Patriot Act which amended the purpose requirement of the Foreign Intelligence Surveillance Act (FISA) and is sometimes described as having dismantled the "wall" between law enforcement and intelligence. While it is clear that more and better coordination is needed between law enforcement and intelligence on counterterrorism, it is not clear that amending the purpose requirement of the FISA was necessary to achieve that. More importantly, it is not clear whether the government is now using the extraordinary secret search and seizure powers under the FISA in ways that are both effective and consistent with constitutional requirements. The recent case of Brandon Mayfield, the innocent lawyer in Oregon jailed for two weeks, apparently because of his religion, raises serious and unanswered questions. The Committee should demand more information concerning the use of the FISA search and seizure authorities before extending section 218. If section 218 is extended, Congress should amend FISA to protect due process and Fourth Amendment rights.

My testimony today will also discuss the separate but related issue of the relationship between law enforcement and intelligence in investigating Americans and others inside the United States, and the so-called "wall." The Center has long advocated the necessity of tying domestic intelligence authorities to law enforcement to insure that government surveillance is targeted against actual wrong-doers and not against political or religious minorities. As FBI Director Mueller said, "there are no clear dividing lines that distinguish criminal, terrorist and foreign intelligence activity. Criminal, terrorist and foreign intelligence organizations and their activities are often inter-related or interdependent."[1] However, the most recent proposal for further intelligence reorganization recommends consideration of establishing a new MI5-like domestic intelligence agency presumably divorced from law enforcement. The recommendation made by the Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction to move the FBI's counterterrorism and counterintelligence operations under the new Director of National Intelligence raises serious questions about moving control of domestic intelligence away from the Attorney General to the DNI. We believe that doing so would be a mistake from the standpoint of both civil liberties and effective counterterrorism.

THE "WALL" BETWEEN LAW ENFORCEMENT AND INTELLIGENCE

The existence of a legal "wall" preventing law enforcement and intelligence agencies from sharing vital information about suspected terrorists is often cited by government officials as the main reason the CIA and FBI didn't discover and stop the September 11 hijackers.[2] The Justice Department made this argument when it sought to amend the purpose requirement of the Foreign Intelligence Surveillance Act in the Patriot Act and Attorney General Ashcroft repeated it when defending the pre-9/11 intelligence failures before the 9/11 Commission. But the existence of legal barriers to sharing information before 9/11 was highly exaggerated, and even the Justice Department has come to recognize that the real problems were bureaucratic failures of coordination and communication between and within the FBI and CIA.

The term "wall" was used as shorthand for the understanding that the fundamental principles limiting government surveillance of Americans apply differently in the case of law enforcement or intelligence. Such principles include the recognition that there are important consequences for individuals depending on the government's purpose in initiating surveillance; in particular whether it intends to use the fruits of its surveillance against an individual to prosecute and jail him. They include the teaching of the Fourth Amendment that the best protection against abuse of surveillance powers is to require the government to have some evidence of criminal activity before investigating an individual. Requiring some criminal predicate for

---

[1] *Oversight of the USA Patriot Act, Hearings* Before the Senate Comm. On the Judiciary, 109 Cong. (Apr. 5, 2005).

[2] Parts of this testimony were adopted from my article on *"Domestic Intelligence and Civil Liberties,"* SAIS Review of International Affairs Winter-Spring 2004, Volume 24, No. 1, available at http://www.saisreview.org/PDF/24.1martin.pdf.

government investigations in turn helps protect citizens from being targeted based on dissent, religion, or ethnicity, and helps to insure that surveillance and intelligence powers are not used for political purposes.

The classic understanding of foreign intelligence gathering—the collection of information that policymakers need concerning the capabilities and intentions of foreign governments and groups—is not, however, linked to a criminal predicate. The distinction between the two—investigating possible wrong-doing by individuals and spying on foreign powers—was the fundamental rationale for separating the functions of law enforcement and intelligence agencies. It was also understood that Fourth Amendment rules governing searches and seizures in the United States should be most protective when criminal sanctions against an individual are possible.

Thus, there were separate authorities written to govern law enforcement and foreign intelligence investigations inside the United States. In particular, since 1978, wiretapping to investigate crimes has been governed by one federal statute, while the Foreign Intelligence Surveillance Act (FISA) governs wiretapping "agents of a foreign power" inside the United States for the purpose of gathering foreign intelligence. Similarly, the Attorney General's Guidelines governing FBI activities, written by Attorney General Levi in 1976 and since amended, provided one set of rules for criminal investigations and another for gathering foreign intelligence relating to espionage or international terrorism inside the United States. These authorities allowed the government much wider latitude in gathering information about Americans and keeping it secret for foreign intelligence purposes than that which is allowed for law enforcement purposes. They also provided much less judicial oversight of the gathering of information for foreign intelligence purposes than for criminal investigations.

While the pre-September 11 framework assumed differences between law enforcement and intelligence, everyone, including the civil liberties community, always recognized the necessity of effective coordination between the intelligence community and law enforcement to fight terrorism.[3] Indeed, for all the talk of a "wall," the pre-September 11 legal regime acknowledged that terrorism-like espionage, and to a lesser extent international narcotics trafficking—is both a law enforcement and intelligence matter. Indeed, no statutory "wall" prohibited sharing information between the law enforcement and intelligence communities; to the contrary, the law expressly provided for such sharing. While the Foreign Intelligence Surveillance Act was interpreted to mean that prosecutors could not direct foreign intelligence wiretaps, as opposed to criminal wiretaps, the text of FISA expressly contemplated that FISA surveillance may uncover evidence of a crime. Before September 11, FISA information had been used in many criminal cases.

Moreover, none of the 9/11 failures were caused by the inability of prosecutors to direct FISA surveillance. The reports of the Congressional Joint Inquiry and 9/11 Commission describe many missed opportunities in detail. Although there were widespread bureaucratic misunderstandings about legal restrictions on information sharing, nowhere do the reports identify any *statutory prohibition* on information sharing as at fault. Instead, the failures resulted from the FBI and CIA failing to know what they knew. For example, while lower level FBI agents had important information about Al Qaeda associates in the United States that they shared with Headquarters, the higher-ups failed to understand the significance of the information, much less act on it. Similarly, the CIA knew for almost two years about the U.S. visa issued to an Al Qaeda suspect who would hijack a plane on September 11, but failed to inform the FBI or appreciate the importance of the information. This was a failure of analysis and coordination; it was not caused by legal restrictions on access to information.

THE PATRIOT ACT AND SECTION 218.

Before September 11, it was understood that if the government started out with the primary purpose of making a criminal case against an individual, it must use the criminal surveillance authorities, not FISA.[4] In the Patriot Act, the Justice Department asked Congress to repeal the fundamental requirement in FISA that its secret and extraordinary procedures be used only when the government's primary purpose is to collect foreign intelligence. Through section 218 of the Patriot Act, the

[3] See, for example, Kate Martin's September 24, 2001 testimony before the Senate Select Committee on Intelligence on the Legislative Proposals in the Wake of September 11, 2001 Attacks, including the Intelligence to Prevent Terrorism Act of 2001, available at www.cnss.org/kmtestimony0924.pdf.

[4] But see *In re: Sealed Case No. 02–001,* Foreign Intelligence Surveillance Court of Review, 18 November 2002.

Justice Department sought to allow the use of FISA's extraordinary powers when the government targets an individual for criminal prosecution or otherwise as long as foreign intelligence gathering was a significant purpose of the surveillance. Of course, since FISA only applies when there is probable cause that the target is an "agent of a foreign power" or foreign power, the significant purpose requirement will always be met when the other statutory requirements are met. (FISA authorizes surveillance of all individuals in the United States, both U.S. persons and non U.S. persons who meet the definition of "agent of a foreign power.")

In seeking section 218, the Department complained that FISA barred the sharing of information with prosecutors and law enforcement investigators. However, even if legal rather than bureaucratic obstacles existed to sharing information, Congress could have adequately addressed the problem simply by providing that FISA information could be shared with law enforcement personnel, as it did explicitly in section 504 of the Patriot Act. This provision alone—proposed by Senator Leahy, not the Justice Department—would have addressed whatever confusion existed about the FISA requirements at the FBI and elsewhere.

But the Patriot Act goes much further. Section 218 repeals the requirement that foreign intelligence gathering be the primary purpose when initiating FISA surveillance. Thus, the government is now free to use the broad powers in FISA to conduct secret surveillance on Americans with the intention of bringing criminal charges against them, or simply to collect information about them as long as there is probable cause that the individual is an agent of a foreign power.

In evaluating the effect of section 218, it is important to begin with a description of FISA authorities. The FISA statute authorizes secret surveillance on less probable cause of criminal activity than is authorized by the Fourth Amendment in criminal investigations. Moreover, FISA contains many fewer safeguards against abuse because there is no *post* surveillance check on either the legality of the initial warrant or on how the surveillance was conducted. While the Justice Department claims that there are judicial oversight and probable cause requirements built into FISA, there is no dispute that in most instances the government will never have to inform an American that his conversations were overheard, his house searched or his DNA seized pursuant to FISA. The statute only requires the government to inform Americans targeted by FISA wiretaps or searches of those searches if they are subsequently criminally indicted and the government tries to use the fruits of the searches against them. The statute also *permits,* but does not *require* the Attorney General to determine that there is no national security interest in continuing secrecy about the search of a U.S. person's home and then to inform that individual that his house was searched. 50 U.S.C. sec. 1825(b).

Even in those few cases where an individual is informed that he or she has been the target of FISA searches and seizures, the Attorney General always blocks access to the original application for the FISA warrant. See 50 U.S.C. secs. 1806(f) and 1825(g). Thus, there is no opportunity for a target to challenge the search and obtain adversarial, rather than *ex parte,* judicial review of the adequacy and legality of the search, because the original application for a FISA warrant, unlike a criminal warrant application, is always withheld from the target.

Unanswered questions concerning the use of FISA.

While the Justice Department continues to claim that the change in FISA's purpose requirement in section 218 is necessary to allow it to use FISA information in criminal prosecutions, its claims raise more questions than they answer. For example, the Department cites prosecutions of individuals based on FISA information obtained from surveillance conducted before the Patriot Act as evidence of the usefulness of section 218.[5] The Department, however, has provided no explanation about why section 504 is not sufficient to provide full authority for sharing all FISA information with prosecutors. Section 218's change to the purpose requirement would seem irrelevant to such sharing. This would seem especially true, of course as to the sharing of FISA surveillance conducted before section 218 changed the purpose requirement.

The second unanswered question concerns the effect of section 218 to allow the government to use the secret authorities in FISA in criminal cases instead of the usual Fourth Amendment warrants which contain greater protections. The Justice Department has offered no public explanation for why and when it decides to use the secret authorities of FISA, rather than the usual criminal authorities. This question is especially important as the extraordinary procedures of FISA are available not just for matters involving international terrorism. The statute also allows

[5] See Justice Department, USA Patriot Act: Sunsets Report, April 2005, in particular concerning the case of Sami Al-Arian.

the use of secret searches and seizures against Americans in investigations of "clandestine intelligence gathering" on behalf of a foreign government, which might well include legal activities such as preparing non-public reports for foreign governments or groups.

Similarly, the Department's description of its use of FISA surveillance pursuant to section 218 in the case of the "Portland Seven" again raises more questions than it answers. While the Department claims that section 218 allowed it to postpone arresting one individual in order to continue the investigation and arrest six more people, it provides no explanation about how the law worked to effect that result. To the contrary, missing from this explanation is any acknowledgement that the Department has the authority to postpone notice of *criminal* wiretap surveillance and physical searches and seizures until it is able to identify and arrest other conspirators. Indeed section 213 of the Patriot Act—the so-called sneak and peak authority—explicitly codifies that authority to delay notification of criminal searches and seizures. The Justice Department has said nothing about why they could not have used the delayed notice authority in section 213 and Title III of the wiretap statute to accomplish the same result in the Portland Seven case.

Moreover, in order to fully evaluate section 218, it is important to consider the broader context of the secret wiretap and surveillance authority in the FISA. The recent revelations concerning the secret search of Brandon Mayfield's home raise serious unanswered questions about possible abuse of the FISA authorities. Mayfield, a Muslim lawyer in Portland, Oregon was jailed for two weeks, without charges, on what turned out to be the false claim that he had material information concerning the March 11, 2004 terrorist bombing in Madrid. After he was released the FBI apologized for jailing an innocent person. In the course of investigating Mr. Mayfield, the FBI apparently obtained a warrant under the FISA to secretly search his home and seize copies of his documents, computer files and his DNA. Apparently, the FBI also secretly wiretapped his phone and e-mail. There is ample evidence that the FBI carried out the searches and seizures with the intention of jailing and prosecuting Mr. Mayfield. While the Inspector General is now investigating the case, including presumably how the FBI came up with a suspect who was Muslim based on a misread fingerprint, the Congress needs to undertake its own investigation, in particular on the use or abuse of the FISA authorities. There is no way to know how many other innocent Americans have had their houses searched or their phones tapped based on allegations resting on their religion. The search of Mr. Mayfield's home is an example of the dangers of FISA. Those dangers are increased by section 218 (regardless whether that section played a role in that particular search) because by making FISA surveillance more easily obtainable, section 218 makes it likely that a lot more people will be secretly searched. And the attendant secrecy raises the specter that the government will as it did in the Mayfield case—go after an innocent American. Under current law, there is no way to know how many Americans have been subject to such surveillance, or how many more will be.

At a minimum, Congress should obtain the answers to all these questions before extending section 218. The Committee should make arrangements to review the FISA applications—at least for U.S. persons—under secure circumstances. The Committee should investigate the use of FISA searches and seizures when the purpose of the investigation is to target individuals for criminal prosecution or deportation. The Committee should also investigate what protections exist against using protected First Amendment activities, including religious beliefs and political activities, as the basis for FISA surveillance. While the details of particular FISA applications are of course classified and cannot be publicly disclosed, there is much information concerning the law and its application which can be disclosed and needs to be publicly discussed before Congress extends section 218.

Needed Amendments.

Should the Congress determine to extend section 218 for an additional period of time, it should consider adopting two amendments to provide some minimal safeguards. The amendments are needed to protect the Fourth Amendment rights of individuals whose homes are secretly searched, and whose papers and DNA are secretly seized, but who turn out not be spies and terrorists and to protect the due process right of those the government seeks to prosecute and imprison based on the results of such secret searches and seizures.

Under current law, the government is required to notify an individual that he has been targeted under FISA only when it seeks to use the information against him. Mr. Mayfield is apparently the only individual ever notified by the government that he had been the target of a FISA search, who the government was not seeking to prosecute or deport. While it is not clear why he was informed, it is likely that the

government did so only because it had wrongly imprisoned him and is now being sued for that act. While the FISA refers to the Attorney General determining that there is no national security interest in continuing secrecy about the search of a U.S. person's home, the Justice Department claims that no court may compel it to inform an individual of a search in those circumstances. *See* Mar. 24, 2005 letter from Justice Department to Mr. Elden Rosenthal, referring to 50 U.S.C. § 1825(b).

Even when an individual is notified because he has been indicted, the government is not required to disclose anything more than the existence of the FISA surveillance unless it either seeks to introduce FISA information into evidence or the information is required to be disclosed to the defendant under the Brady exculpatory evidence rule. And then, all the government provides to the defendant is a record of his own telephone conversations or a copy of his own papers. See FISA, 50 U.S.C. §§ 1806(c), 1825(d). (Even these minimal protections are only available to individuals *not* alleged to be "alien terrorists." See 8 U.S.C. § 1534(e).)

The government is not required to disclose and, it appears, has never disclosed the application for a FISA warrant to anyone. Indeed, information obtained under FISA is accorded much greater secrecy than any other kind of classified information is accorded under the Classified Information Procedures Act or, in our view, than is consistent with constitutional due process requirements.

If Congress extends section 218, allowing secret surveillance when the government's primary purpose is not foreign intelligence gathering, but rather making a criminal case against an individual, Congress should consider how to bring the use of FISA information in line with basic due process requirements. One way to do this would be to treat FISA information like all other kinds of classified information by making it subject to the provisions of the Classified Information Procedures Act. Such a provision is included in the Civil Liberties Restoration Act, H.R.1502, sec. 401. Under current law, it is nearly impossible for a defendant to contest the introduction of FISA evidence against him because the government's application for the FISA search and related materials are automatically kept secret. That should be changed so that when FISA evidence is used in criminal cases, the court may disclose the application and related materials to the defendant or his counsel, with any necessary redactions, in accordance with the Classified Information Procedures Act. (Sources and methods information for example, might be withheld.) Such an amendment would offer a balanced and effective way to protect both sensitive national security information and the due process rights of individuals.

Congress should also consider amending the FISA to protect the Fourth Amendment rights of those whose homes are searched and conversations are overheard, but who turn out not to be terrorists or spies. There is no requirement under current law that the government inform innocent persons whose conversations are overheard, houses are searched and belongings are seized that the FBI was in their home and listening to their conversations. There is no after-the-fact check on the propriety of the search. An innocent individual never gets a chance to challenge the search, only one who is subsequently indicted. And with the repeal of the purpose requirement in section 218, the number of FISA searches has been steadily increasing.

A fundamental requirement of the Fourth Amendment is that an individual be notified of the government's search and seizure and Congress should take one small step to restore this constitutional protection to those who are targeted for secret searches and turn out to be innocent. Congress should consider amending the FISA so that, if it turns out that the person whose house was searched (and whose conversations or e-mail were intercepted) was not a terrorist or a spy, the individual would be told after some reasonable period of time that the government had searched his belongings and be given an inventory of what was taken. This could be done by amending 50 U.S.C. § 1825(b) to require the Attorney General when certain criteria are met to notify all those who were subject to FISA searches or seizures. Those criteria should include the passage of a definite time period and the determination that there is no current probable cause that the target is in fact an "agent of a foreign power." Doing so would restore Fourth Amendment protections and provide some measure of accountability for secret searches of Americans' homes.

DOMESTIC INTELLIGENCE REORGANIZATION PROPOSALS

In enacting the recommendations of the 9/11 Commission regarding the reorganization of U.S. intelligence agencies, the Congress accepted its conclusion that a new domestic MI5 or CIA should not be created. There has been a broad consensus among both civil libertarians and intelligence officials that the responsibility for intelligence activities inside the United States should ultimately remain with the Attorney General as the chief law enforcement officer rather than with an intelligence

official. As former intelligence and national security officials, including former DCI Robert Gates, John Hamre and Sam Nunn urged, "[e]ven as we merge the domestic and foreign intelligence we collect, we should not merge responsibility for collecting it . . . exclusive responsibility for authorizing and overseeing the act of domestic intelligence collection should remain with the Attorney General. This is the only way to protect the rights of the American people upon whose support a strong intelligence community depends."[6]

In the Intelligence Reform and Terrorism Prevention Act of 2004, the Congress set up a National Counterterrorism Center to insure sharing of information and coordination of plans, but agreed that ultimate responsibility for domestic operations should remain with the Attorney General. However, the most recent review done by the Silberman-Robb Commission has recommended that the counterterrorism and counterintelligence operations of the FBI be moved under the direct supervision of the new Director National Intelligence. Such a recommendation, if adopted, would make use of counterterrorism's most effective domestic tool—the ability to prosecute and jail terrorists more difficult. By separating domestic terrorism and counterintelligence from law enforcement, it could create new and more difficult coordination problems. Indeed the Commission also recommends the reorganization of national security responsibilities at the Justice Department, but does not explain how those prosecutorial efforts under the supervision of the Attorney General would be coordinated with a reorganized FBI carrying out the intelligence and investigations necessary to bring prosecutions under the supervision of the new NDI rather than the Attorney General. In making its recommendation, the Commission also overlooks the fundamental differences in intelligence at home and abroad and risks resurrecting all the bureaucratic difficulties attributed to the "wall" that law enforcement and intelligence agencies have been working to dismantle since September 11. Such a change is likely to threaten civil liberties.

Differences between intelligence at home and abroad. The Attorney General, unlike an intelligence director, has an institutional responsibility to protect constitutional rights and is subject to closer and more transparent congressional scrutiny. As William Webster, former director of both the FBI and CIA, testified last August concerning proposals to transfer the FBI's domestic intelligence authorities from the Attorney General to an intelligence official, "the FBI should take its guidance from the Attorney General on its dealings with U.S. persons and the manner in which it collects information in the United States. This has been an important safeguard for the American people, should not be destructive of effective operations, and avoids the risks of receiving vigilante-type instructions, whether from the intelligence community or the White House."[7]

Historically, overseas intelligence was largely carried out by the CIA (and Defense Department agencies) while the FBI was largely responsible for domestic intelligence because there are important differences between the missions and methods that are necessary and appropriate abroad and at home. These differences should not be disregarded by the simplistic device of labeling these different activities in the U.S. and abroad as "intelligence." Generally, the CIA has been confined largely to gathering foreign intelligence abroad for policymakers regarding the intentions and capabilities of foreign powers or groups. The FBI has had both law enforcement and intelligence responsibilities inside the United States, for both counter-espionage and international terrorism matters. While both involve intelligence, the difference in functions is important from the standpoint of civil liberties.

The CIA acts overseas, in secret, and its mission includes violating the laws of the country in which it is operating when necessary. It is charged with collecting information overseas without regard to individual privacy, rights against self-incrimination, or requirements for admissibility of evidence. It is also tasked with carrying out covert actions to influence events by whatever means the President authorizes. The agency gives the highest priority to protection of its sources and methods.

In contrast, the FBI, as an agency with both intelligence and law enforcement responsibilities, must *always* operate within the law of the jurisdiction in which it is operating, even when outside the U.S. It must respect the constitutional limits set by the First Amendment, the Fourth Amendment and due process on government activities inside U.S. borders, which limits have not (yet) been extended to aliens

---

[6] Center for Strategic and International Studies, *Guiding Principles for Intelligence Reform,* at 2 (Sept. 21, 2004), at http://www.csis.org/0409—intelreformprinciples.pdf.

[7] Testimony of William H. Webster before the Senate Committee on Governmental Affairs, *Reorganizing America's Intelligence Community: A View From the Inside* (Aug. 16, 2004), at 8, available at http://hsgac.senate.gov/—files/081604webster9934.pdf.

overseas.[8] While the task of foreign intelligence is to learn as much as possible to provide analyses to policymakers, deepseated notions of privacy rooted in the Constitution limit the information the government may collect and keep about Americans. There is much greater transparency of the FBI's operations, in part because they affect Americans and in part because they are likely to lead to prosecutions, with the result that information which is collected must generally be admissible as evidence at trial and the methods and informants used are quite likely to be publicly identified.

Examining how intelligence information is actually used in counterterrorism demonstrates the necessity of tying intelligence activities inside the U.S. to a law enforcement agency. The first use of "intelligence" information is to identify and locate individuals involved in planning terrorist acts. This information must then be used to prevent the attack, in ways that are legally permissible. Potential terrorists found in the United States may be placed under intensive surveillance. They may be apprehended if there is probable cause that they are engaged in criminal activity or are in the United States in violation of the immigration laws. They may be arrested not only for plotting terrorism, including attempt or conspiracy, but for any crime or visa violation. The government may also attempt to turn them into informants on their associates (with or without arresting them), but may not blackmail them to do so. Ultimately, in order to disable individuals from future terrorist activity, they have to be arrested and prosecuted. (They may also be deported.) Such "prevention" through prosecution has remained one of the government's major anti-terrorism tools even since September 11. Such an approach focuses on individuals involved in planning criminal activities and ultimately relies on law enforcement authorities.[9]

Whereas the FBI must arrest and charge individuals in the U.S. consistent with due process, the CIA and DoD intelligence agencies operating overseas are free to employ methods such as disinformation campaigns, secret kidnappings, and interrogations. The methods used by the CIA and foreign intelligence agencies to "disable" terrorists—predator drones shooting missiles at a car crossing the desert; turning individuals over without any legal proceedings to intelligence services infamous for coercive interrogations; or indefinitely detaining individuals incommunicado without any legal process—have never been deemed constitutional or appropriate to use against individuals in the United States. Even absent military hostilities, overseas intelligence methods include disruption of groups and harassment of individuals using agent provocateurs, blackmail or other means, which have not been allowed in the United States.

Moreover, counterterrorism intelligence inside the United States poses special risks to civil liberties. It is always difficult to investigate planned terrorist activity without targeting those who may share the religious or political beliefs or the ethnic backgrounds of the terrorists, but do not engage in criminal activity. It is easier for an agency to identify those who share the political goals or religious fanaticism of terrorists than to identify and locate those actually plotting harm. It is therefore crucial to structure bureaucratic rules and incentives to discourage investigations based on political and religious activities and to require focusing on finding actual terrorists. An important means for doing this is to require agencies to focus on criminal activity, which encompasses all terrorist plotting and financing, rather than authorizing an intelligence approach that absorbs all available information about thousands of individuals in the hope of finding something useful. A second important safeguard is the transparency inherent in a law enforcement agency ultimately answerable to the courts—transparency to which the CIA, as an intelligence agency, has never been subjected.

While questions have been raised concerning the effectiveness of various FBI efforts, those issues do not undercut the importance of tying domestic intelligence efforts to a law enforcement agency. Similarly, the fact that it is important to assure effective coordination between intelligence activities overseas and those in the U.S. does not argue for any separation of domestic intelligence activities from related law enforcement activities. Indeed, even as the 9/11 Commission recommended new

---

[8] While international human rights law provides many of the protections recognized in the Bill of Rights and is not limited by national borders, its applicability to intelligence activities in times of emergency or war is less developed.

[9] As the 9/11 Commission recognized: "Counterterrorism investigations in the United States very quickly become matters that involve violations of criminal law and possible law enforcement action. Because the FBI can have agents working criminal matters and agents working intelligence investigations concerning the same international terrorism target, the full range of investigative tools against a suspected terrorist can be considered within one agency." NATIONAL COMMISSION ON TERRORIST ATTACKS UPON THE UNITED STATES, THE 9/11 COMMISSION REPORT 424 (2004).

structures to insure coordination, it agreed that the FBI, not the CIA, should retain domestic intelligence responsibilities. "The FBI's job in the streets of the United States would thus be a domestic equivalent, operating under the U.S. Constitution and quite different laws and rules, to the job of the CIA's operations officers abroad." [10]

Given the importance of maintaining different laws and rules for the collection of intelligence on Americans than for the collection of intelligence overseas, the Attorney General should remain ultimately responsible for the FBI's operations. Putting an Intelligence Director or Office in charge of domestic intelligence will exacerbate the difficulties in reconciling the different approaches that are required in the U.S. and overseas. We note that the Silberman-Robb Commission did recommend that the rules for domestic intelligence should still be written by the Attorney General, but we suggest that such a division of responsibility—between an Attorney General who writes rules for intelligence and counterterrorism operations, but has no responsibility for how those rules are carried out and a Director of National Intelligence who has responsibility for how operations are carried out, but no responsibility for writing the rules—makes no sense. We respectfully suggest that the DNI should have responsibility for insuring coordination between domestic and foreign collection and for setting overall strategic priorities for domestic intelligence collection, while domestic intelligence operations should remain operationally tied to law enforcement.

In conclusion, let me reiterate our appreciation for the Committee's hard work on these difficult problems that are important for both our liberty and our security. We look forward to working with you in the future and stand ready to provide whatever assistance we can.

Mr. CHABOT. Thank you very much.

And Mr. Swire, you're recognized for 5 minutes.

TESTIMONY OF PETER SWIRE, PROFESSOR OF LAW, OHIO STATE UNIVERSITY

Mr. SWIRE. Thank you, Mr. Chairman, and thank you for the kind words from Ohio. Thank you, Mr. Ranking Member, for being here today and for you inviting me back to testify this week. Your Committee is doing an exemplary job, I believe, of developing a record for what to do next on the PATRIOT Act.

The topic of today's hearing, FISA and "The Wall," has been the focus of my biggest single research project since I left the Government 5 years ago. My testimony today is drawn from a Law Review article [1] that has been placed in the hearing record and is available online. Research for that article included many interviews, often on background, with Government officials who have worked with FISA over the decades.

I have one over-arching point today, as well as four specific points. The over-arching point is this: "The Wall" has been our chief protection against a slippery slope, against permitting secret FISA surveillance from expanding deep into normal law enforcement activities. If "The Wall" stays down, then it is the job of this Committee and the Congress to create a new set of checks and balances against abuse.

These hearings are the single biggest reexamination of FISA since it was passed in 1978. I therefore attached to the testimony a set of oversight questions, to try to clarify law and practice. I've also attached a list of concrete possible reforms that can, taken together, I hope, create the checks and balances needed to replace "The Wall." In 2001, a wall was taken out of the structure of FISA. It's up to Congress to build a sound structure for the future.

---

[10] 9/11 COMMISSION REPORT, at 423.

[1] The information referred to is located in the Appendix.

My four specific points: First, supporting Kate Martin's proposals in her written testimony; second, talking about "agent of a foreign power" definition; third, talking about the words in section 218, itself; and fourth, a brief comment on one other provision.

Turning to the next point, the definition of "agent of a foreign power," this is absolutely crucial to defining the scope of FISA. For law enforcement investigations, a wiretap means probable cause of a crime. For FISA, it's just probable cause the person is an agent of a foreign power.

Think about an individual who works in the United States for the Cali drug cartel. Is that person an agent of a foreign power? The Cali cartel is very organized. It physically controls a lot of land in Colombia. It may well be more of a foreign power than Al-Qaeda is, that doesn't own a big territory. So if one accepts that the Cali cartel is a foreign power, and a major smuggler is an agent of a foreign power, what about a street-level cocaine dealer? Is that an agent of a foreign power? Is that a FISA wiretap because that person is part of narco-terrorism?

To take another example, what about the activities of the so-called "Russian mafia"? Many organized crime groups have links to overseas operations. How small can the links back home be to still qualify that group's actions as part of a foreign power's operations?

My second specific point concerns a proposal for partially mending "The Wall." The Law Review article explores in detail the reasons for and against having "The Wall." Based on my research, the greatest problem with the old "primary purpose" test is that investigators genuinely don't know in the early stages of an investigation whether the case will primarily end up being for intelligence or law enforcement. The early wiretap order is a dual-use technology. It's for both intelligence and law enforcement, depending how things turn out.

My article argues that the missing legislative piece is a requirement within FISA that the surveillance, one, be important enough and, two, be justifiable on foreign intelligence grounds alone. It has to really be a foreign intelligence wiretap.

One way to go could be to say that a principal purpose, "a principal purpose," is foreign intelligence. Another way would be to amend FISA to include a new certification in the FISA application. The certification would say that, "The information sought is expected to be sufficiently important for foreign intelligence purposes to justify the order." It really has to be for foreign intelligence; maybe also it turns out to be for criminal.

In concluding, I note that the article goes piece by piece through FISA, suggesting ways to update many of its provisions in light of our experience since 1978 and since 2001. A special focus of the article is the so-called "gag rule" that applies to section 215 orders and national security letters. The Senate version of the SAFE Act has included one of my recommendations, which is to put a 6-month limit on the gag. You can't talk about the search; but 6 months later, ordinary people can. That limit would be extendable by order of the FISA court. I hope very much this Committee will follow along with the Senate, and include the same limit in the bill this year.

To return to my over-arching point, "The Wall" probably deserves to be lowered somewhat in our globalized world, where information sharing is vital to fast-moving interrogations—investigations. "The Wall," however, was our chief bulwark against the creep of the FISA system into ordinary law enforcement. If "The Wall" comes down, this Committee should erect new safeguards against the abuses that do come from secret surveillance. Thank you.

[The prepared statement of Mr. Swire follows:]

PREPARED STATEMENT OF PETER P. SWIRE

Testimony of Professor Peter P. Swire
Professor of Law
Moritz College of Law
The Ohio State University

before the

Subcommittee on Crime, Terrorism, and Homeland Security

of the

Judiciary Committee of the U.S. House of Representatives

on

Oversight Hearing on the Implementation of the USA PATRIOT Act:
Sections of the Act that Address -
Crime, Terrorism, and the Age of Technology

To Examine *Section 218* of the Patriot Act and the Foreign Intelligence Surveillance Act

April 28, 2005

Mr. Chairman, Mr. Ranking Member, I appreciate that the Committee has asked me back to testify this week. Your Committee is doing an exemplary job of developing a record from which everyone can become more informed about the Patriot Act. These extensive hearings will help the Committee, the Congress, and the general public have a far better basis for addressing the numerous legal issues implicated by the sunset of the Patriot Act.

The topic of today's hearing, the Foreign Intelligence Surveillance Act and the "wall," has been the focus of my single biggest research project since leaving the Government. My testimony is drawn today from my article on "The System of Foreign Intelligence Surveillance Law, 72 Geo. Wash. L. Rev. 1306, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=586616. That article has been submitted into the record. In addition to the usual law review research, the article was based on my experience chairing a White House Working Group in 2000 on how to update surveillance law for the Internet age. It was also based on extensive interviews with people who have worked on FISA issues over the past several decades, in the Justice Department, the intelligence agencies, the FBI, and from outside of government. I think I can accurately describe the article as the most complete history of FISA. The article attempts to explain both the compelling national security interests at stake in FISA as well as the need to maintain civil liberties and the rule of law for surveillance conducted within the United States. The article contains a detailed list of issues for legislative oversight and for potential statutory reform.

I have one over-arching point today, as well as three specific points. The over-arching point is this. The wall has been our chief protection against a slippery slope, against permitting secret FISA surveillance from expanding deep into normal law enforcement activities. If the wall stays down, then it is the job of this Committee and the Congress to create a new set of checks and balances against abuse.

I will say it a different way to underscore the point. Since 1978 we had a way to prevent FISA from spreading into domestic law enforcement. The wall kept FISA within limits. What will prevent the secret FISA system from growing and growing in the years to come? The only reasonable answer, in my view, is to establish a set of checks and balances to make up for the absence of the wall. These hearings are the single biggest re-examination of FISA since it was enacted in 1978. I have therefore attached to this testimony a list of concrete possible reforms that can, taken together, create the checks and balances needed to replace the wall.

My three specific points concern, first, the broad definition of "agent of a foreign power," second, a legislative proposal to mend the wall somewhat, and third, a brief comment on a part of FISA that is not the focus of today's hearing, Section 215.

Turning to the first point, the definition of "agent of a foreign power" is crucial to defining the scope of FISA. For law enforcement investigations, a wiretap can be issued where there is probable cause that a crime has been, is, or is about to committed. For

FISA, the probable cause test is entirely different – there must only be probable cause that the person is an "agent of a foreign power."

Consider an individual who works in the United States for the Cali drug cartel. Is that person an "agent of a foreign power"? The Cali cartel is a highly organized group that physically controls a substantial amount of territory in Colombia. Given these facts, one might well argue that the Cali cartel is more of a "foreign power" than the amorphous Al Qaeda network. If one accepts the Cali cartel as a "foreign power," and a major smuggler as an "agent of a foreign power," would a street-level cocaine dealer also qualify as an agent of narcoterrorism? To take another example, what about the activities of the so-called "Russian mafia?" Many organized crime groups have links to overseas operations. How small can the links back home be to still qualify that group's actions as on behalf of a foreign power? These might be good oversight questions to direct to the Department of Justice.

Narcotics and organized crime cases have historically accounted for over 80 % of law enforcement wiretaps. If many of those cases shift to FISA, then law enforcement tools, including Title III wiretaps, may become the exception rather than the norm. Already in 2003, FISA orders for the first time outnumbered all state and federal law enforcement wiretap orders. As I believe other testimony will develop, there are serious constitutional issues if ordinary law enforcement cases are handled in the FISA system. Fourth Amendment protections do not get repealed for searches in the United States, for criminal investigations, just because a suspect may have a tenuous link back to someone overseas.

My second specific point concerns a proposal for partially mending the wall. My law review article explains in detail the compelling arguments on both sides of the argument. Based on my interviews with many people in DOJ and the intelligence agencies, the greatest problem with the "primary purpose" test is that investigators genuinely don't know in the early stages of an investigation whether the case will be primarily for intelligence or instead for law enforcement. The early wiretap order is a "dual use" technology – it is for *both* intelligence and law enforcement, depending on how the investigation develops.

My article argues that the missing legislative piece is a requirement within FISA that the surveillance be: (1) important enough and (2) justifiable on foreign intelligence grounds alone. The proposal is to amend FISA to include a new certification in a FISA application. The certification would be that "the information sought is expected to be sufficiently important for foreign intelligence purposes to justify" the initial (and any subsequent) FISA order.

This certification would underscore the idea that FISA should be used where foreign intelligence goals justify use of the special system. True foreign intelligence investigations would deserve a FISA order. If orders are sought with little link to foreign intelligence, then the Justice Department should not make the certification. If such cases

go forward, FISA judges should ask the tough questions to ensure that there is an important foreign intelligence justification for the order.

In concluding, I note that my article goes piece by piece through FISA, suggesting ways to update a number of its provisions in the light of our experience since 1978 and 2001. A special focus of the article is the so-called "gag rule" that applies to Section 215 orders and National Security Letters. The Senate version of the SAFE Act has adopted one of my recommendations, to put a six-month limit on the gag. The limit would be extendable by order of the FISA court. I hope very much this Committee will include the same limit in its bill this year.

To return to my over-arching point, the wall probably deserves to be lowered somewhat in our globalized world, where information sharing is vital to fast-moving investigations. The wall, however, was our chief bulwark against the creep of the FISA system into ordinary law enforcement. If the wall comes down, this Committee should erect new safeguards against the abuses that come from secret surveillance.

Issues List for Possible Reform of the Foreign Intelligence Surveillance Act

The issues list here comes directly from Peter Swire, "The System of Foreign Intelligence Surveillance Law, 72 Geo. Wash. L. Rev. 1306, *available at* http://papers.ssrn.com/sol3/papers.cfm?abstract_id=586616. The reform proposals are discussed in greater detail in that paper.

A. The Practical Expansion of FISA since 1978

1. Expand reporting on FISA surveillance
   Ex., look at Title III and pen/trap reporting

2. Redefine "agent of a foreign power"
   Ex., define activities that come within domestic law enforcement.

B. Section 215 and National Security Letters to Get Records

1. Limit the use of NSLs because there is no judicial oversight

2. Limit the use of Section 215 orders

   a. For both, consider return to pre-2001 standard for "specific and articulable facts"

   b. For both, consider minimization or other ways to prevent search of entire, large databases

   c. For both, clarify that the record producer can consult an attorney and also seek to narrow the order as unduly burdensome or overbroad; the challenge might be either in district court or the FISC

3. Modify the "gag rule"

   a. Adopt the 6-month limit for the gag rule, subject to 6-month extensions by the FISC

C. What to Do About the Wall

1. Require certification that the "the information sought is expected to be sufficiently important for foreign intelligence purposes to justify" the initial (and any subsequent) FISA order.

D. Improved Procedures for the Foreign Intelligence Surveillance Court System

1. Create more of an adversarial system with the FISC
   Ex., create a "devil's advocate" within the system, or at least permit the FISC to ask for counsel in appropriate cases

2. Adversary council on FISC appeals

3. Certification of issues to the FISC in criminal cases, at discretion of district judges

4. Create a statutory basis for minimization and other procedures by the FISC

E. Additional Oversight Mechanisms

1. Greater reporting to the public and Congress on the use of FISA for criminal prosecution

2. Disclosure of legal theories used in the FISC

3. Greater House and Senate Judiciary Committee oversight

4. Consider greater use of Inspector General oversight after the fact

5. Consider providing notice of FISA surveillance considerably after the fact

Potential Oversight Questions

The following potential questions for oversight accompany the April 28 testimony of Peter Swire on Section 218 and the Foreign Intelligence Surveillance Act. They were compiled with the assistance of other persons who are expert in FISA, especially Kevin Bankston of the Electronic Frontier Foundation and Beryl Howell of Stroz Friedberg, LLC.

1. What steps has the Department of Justice taken to ensure that the more than 70 errors and misrepresentations regarding information sharing and unauthorized dissemination of information, which are described in the Foreign Intelligence Surveillance Court's 2002 Opinion and Order, have not been repeated?

2. Does the Department have knowledge of any misrepresentations made to the Foreign Intelligence Surveillance Court since the passage of Section 218?

3. Are criminal prosecutors directing and controlling the initiation and operation, continuation and expansion of FISA searches and surveillances of US persons?

4. In what types of criminal cases have prosecutors directed and controlled FISA investigations? For example, have they directed and controlled the initiation of FISA searches and surveillances of US persons in narcotics cases? RICO cases? Domestic terrorism cases?

5. Which attorneys in the Criminal Division and the U.S. Attorneys' Offices are receiving training in the use of FISA? Only those in the terrorism and espionage sections or in all sections?

6. Is the Department of Justice's Office of Intelligence Policy and Review (OIPR) attending all meetings and discussions between the FBI's intelligence agents and the Criminal Division regarding FISA cases? If not, does OIPR receive briefings or written information on all such meetings and discussions?

7. Does OIPR inform the Foreign Intelligence Surveillance Court when a FISA target is also the subject of a criminal investigation?

8. A small number of applications have been rejected by the FISC since the FISCR's decision, according to public reporting. How many, if any, of these denials resulted from a lack of a significant foreign intelligence purpose? Were any orders submitted to the FISC and then modified and eventually approved in response to FISC concerns about the lack of a significant foreign intelligence purpose?

9. Please share with this committee any written opinion or order issued by the FISC after the FISCR decision construing the significant purpose requirement, redacted as necessary to prevent disclosure of sources and methods.

10. Since the FISCR held that agents and lawyers of the Criminal Division may direct and control FISA surveillance, approximately what percentage of FISA applications or surveillances would the DOJ characterize as being so directed or controlled?

11. In light of the expanded use of FISA authorities for law enforcement investigations and prosecutions, in what ways, if any, should the House and Senate Judiciary Committees receive less oversight information on FISA issues than the House and Senate Intelligence Committees?

12. The Fourth Circuit in United States v. Truong Dinh Hung, 629 F.2d 908, 916 (4th Cir. 1980), found that the constitutional exception to the Fourth Amendment warrant requirement applies only to "foreign powers, their agents, and collaborators." The Court stated that "even these actors receive the protection of the warrant requirement if the government is primarily attempting to put together a criminal prosecution." Id. Does the Department consider this statement to be an accurate description of the law in the Fourth Circuit? Has the Department conducted surveillance under a FISA order in the Fourth Circuit where the government was "primarily attempting to put together a criminal prosecution"? Since the adoption of Section 218, has the Department conducted such surveillance in any circuit?

13. Does selling illegal narcotics, in and of itself, constitute "international terrorism" as defined in 50 U.S.C. § 1801? Is your answer different if the individual selling the narcotics knows that they come from an international organization that systematically brings illegal narcotics into the United States? Is your answer different if the individual knows that that activities of the international organization appear to "intimidate or coerce" a civilian population? Is it relevant to your answer if the international organization bribes or otherwise coerces public officials? Does such bribery or influence over public officials constitute activities that appear to be intended "to influence the policy of government by intimidation or coercion"? For these questions, in what ways do your answers differ if the person selling the narcotics is a U.S. person or not?

14. Does participation in organized crime activity, in and of itself, constitute "international terrorism" as defined in 50 U.S.C. § 1801? Is your answer different if the individual engaged in RICO or other organized crime activity knows that the organization systematically operates both inside and outside of the United States? Is it relevant to your answer if the international organization bribes or otherwise coerces public officials? Does such bribery or influence over public officials constitute activities that appear to be intended "to influence the policy of government by intimidation or coercion"? For these questions, in what ways do your answers differ if the person engaged in organized crime activity is a U.S. person or not?

15. One possible legal change would be to permit criminal defendants – or their cleared counsel – an opportunity to review the initial application for the FISA wiretap or search when contesting the admissibility of evidence obtained through a FISA search. What are the chief advantages and disadvantages of this possible change?

16. One possible legal change would be to require the Department to certify in applications for a FISA order that the "the information sought is expected to be sufficiently important for foreign intelligence purposes to justify" the initial (and any subsequent) FISA order. What are the chief advantages and disadvantages of this possible change?

17. One possible legal change would be to authorize expressly the FISCR and Supreme Court to permit parties from outside of the government to write briefs and participate in oral argument on appeals from the FISC. What are the chief advantages and disadvantages of this possible change?

18. One possible legal change is to authorize expressly the FISC to establish minimization or other procedural rules that would apply to applications for FISA orders. In light of the usual authority of Article III courts to establish procedural rules for their proceedings, what are the chief advantages and disadvantages of this possible change?

Mr. CHABOT. Thank you very much. And the Members now will have 5 minutes to ask questions of the witnesses, and I'll recognize myself for that purpose at this time.

Mr. Fitzgerald, let me refer to you first. Mr. Swire referred to the Mayfield case. And is the Mayfield case evidence of abuse of FISA, or is it evidence of abuse due to the PATRIOT Act? Or wasn't the Mayfield case a result of erroneously read fingerprints by the FBI and Mr. Mayfield—or Mr. Mayfield's own expert?

Mr. FITZGERALD. I'm not handling the Mayfield case, but from my understanding of the public record, that was a situation—a terrible situation that arose out of mis-identification of fingerprints, both by the FBI mis-identifying Mr. Mayfield's fingerprint as matching the exemplar they had, and by an expert selected by the defense and paid for by the court—made that same mistake. And I think the lesson of the Mayfield case is we have concerns about the fingerprint science.

With or without the amendments to the PATRIOT Act, the actions taken under FISA could have been done, and should be done if you thought that the person's fingerprint actually matched the materials involved in a bombing. So the problem we have is not with the PATRIOT Act, which didn't facilitate what happened. The law provided for it anyway. It was bad information on the fingerprints. And I don't see how the Brandon Mayfield situation casts section 218 in doubt. The Brandon Mayfield situation casts fingerprint science as something we ought to examine, but not the PATRIOT Act.

Mr. CHABOT. Thank you. Mr. Kris, let me follow up with you here. In Mrs.—in Ms. Martin's written testimony, she suggests that we amend FISA so that, if it turns out that the person who was under surveillance was not a terrorist or spy, the individual would be notified of the surveillance after some reasonable period of time.

I'm concerned, however, that such a requirement could jeopardize sensitive investigations. For example, were the associate of a terrorist notified that he'd been under investigation, that associate would almost certainly tip off the terrorist that the Government was probably onto him as well. Do you share that concern? Or what comment might you like to make on that?

Mr. KRIS. Well, I share your concern about the case you just described. If they mistakenly go up on someone who is connected with, but not himself, a terrorist, and then he tips off the other target, I think that would be very dangerous.

I guess my basic sense of this is that notification is acceptable, except when it's not. And right now, FISA has a provision under which—I think it's 1825(b), under which, if there's a search of a U.S. person home, and the Attorney General determines that there is no national security basis for maintaining the secrecy, then he shall inform the target. And I believe that provision——

[Sound of buzzer.]

Mr. KRIS. Every time I talk. And I believe that provision is involved in the Mayfield case; although I'm not absolutely sure. To expand it to reach all forms of searches or surveillance, not just U.S. person house searches, I think conceptually would be okay, if you could figure out what the right standard was. Maybe it would

be when probable cause is found to be lacking under *Franks v. Delaware*.

But administratively, it would impose a pretty significant burden. I think there were some 15, 17 hundred FISAs last year. And it would, I guess, mean that the Government would need to review each and every one of those to determine whether it met the standard. So I have some concerns about that, on that theory, as well.

Mr. CHABOT. Thank you. Professor Swire, do you agree with those you interviewed at the Department of Justice, that the greatest problem with the "primary purpose" test is that investigators generally don't know in the early stages of an investigation whether the case will be primarily for intelligence or instead for law enforcement? And do you agree that "The Wall" did prevent sharing of vital information?

Mr. SWIRE. Yes.

Mr. CHABOT. Okay.

Mr. SWIRE. I mean, I think that one of the questions comes up later on. So you've done your first wiretap. You didn't know which way it was going to go; but now it's up for renewal, and you really know it's turning into a law enforcement investigation. And I think it makes sense for the law to push things toward law enforcement at that point, if that's what's really happened. Among other things, that means that it will get notice to people after the fact of the wiretap.

Mr. CHABOT. Okay. And finally, Mr. Kris, in your written testimony, you suggest that keeping "The Wall" down will enhance the protection of civil liberties. And you stated this and described it to some degree in your opening statement.

Could you say again why you believe that coordination between law enforcement and intelligence officials helps to safeguard constitutional rights? And I know you went into that, but I'd like to hear about it again.

Mr. KRIS. Sure. I mean, I think there are two reasons to believe that it will be helpful in protecting civil liberties. The first is that it opens up these cases, these investigations, to a large number of energetic lawyers inside the Department of Justice, who previously really were limited in their access. And lawyers, I mean, for all their faults, you know, do have an awareness of and a respect for rules and laws. And it is for that reason, I think, that this country uses lawyer oversight to safeguard civil liberties in the area of national security.

And so, if it's done right, I think the opening up of these cases to many, many more lawyers will be a good thing, because they will be able to spot potential abuses early on and maybe put a stop to them.

The other reason that I articulated—and I say it with some hesitation, because I'm afraid it will be misconstrued and misused—but there are cases, and I think there always will be, where somebody needs to get locked up, if you're going to keep the country safe from terrorism. And today, if you can't do it using traditional law enforcement because of "The Wall," then I think you have to go to the alternatives. And one of those alternatives is military detention; which I believe, after Hamdi, civil libertarians do not smile upon.

And so, for that reason as well, I think, if compared to the alternatives, prosecution in an open court, with a jury of 12, court-appointed lawyer, public access, and so forth, is not something that we need to be afraid of.

Mr. CHABOT. Thank you. My time's expired. The gentleman from Virginia is recognized.

Mr. SCOTT. I think Ms. Martin and Mr. Swire pointed out that when you run these investigations where the primary purpose is something other than—when you get a FISA wiretap with the diminished—with no probable cause of a crime even required, you're running a criminal investigation without probable cause. And when we changed "primary purpose" to "significant purpose," it invited the question: What is the purpose of the wiretap, if the primary purpose wasn't foreign intelligence? What was the purpose of the wiretap?

And the Attorney General answered the question for us. He said it's a criminal investigation, and then you kind of put in parentheses, "without having to fool with the probable cause." Now, I suppose—is "probable cause" the problem, Mr. Fitzgerald? I mean, is the requirement that we get probable cause the problem? I mean, if we didn't have to fool with probable cause—if we could start listening in and searching without probable cause, we could probably do a better job for law enforcement.

Mr. FITZGERALD. I'd love to answer that question. It's not the problem. There's two misconceptions, I think, that are going on in the public debate. The first is that there's no probable cause requirement in FISA. Let me speak from the perspective of a terrorism investigation.

To get a probable—to get a FISA for a terrorism investigation, you have to have probable cause that the person is the agent of a foreign power; which means that they knowingly engage in activity—in sabotage or international terrorism, or activities that are in preparation thereof, on behalf of a foreign power——

Mr. SCOTT. Wait a minute. Keep reading.

Mr. FITZGERALD. Okay. Or they knowingly aid or abet any person in the conduct of activities, or they knowingly conspire.

Mr. SCOTT. Keep reading.

Mr. FITZGERALD. That's the end—Or as described in Subparagraph (a), (b), and (c). I'm talking about terrorism.

Mr. SCOTT. Oh, oh. Oh, you're talking about terrorism——

Mr. FITZGERALD. That's what I said.

Mr. SCOTT. —as far as the FISA.

Mr. FITZGERALD. I said "terrorism."

Mr. SCOTT. Well, what about the foreign—foreign intelligence? You have probable cause you can get some foreign intelligence. What about foreign affairs?

Mr. FITZGERALD. Okay, it's not probable cause you can get foreign intelligence. It's probable cause that the person is an agent of a foreign power.

Mr. SCOTT. Right.

Mr. FITZGERALD. You have to certify, in addition, that you're going to gain foreign intelligence, my point being——

Mr. SCOTT. Wait, wait, wait. Whoa, whoa. What is foreign intelligence?

Mr. FITZGERALD. Foreign intelligence, that's one of the things you have to get. But before you can even certify that you're getting foreign intelligence, you have to establish that the person is an agent of a foreign power. Under the terrorism statute, there is no——

Mr. SCOTT. Well, wait, wait a minute. Wait a minute——

Mr. FITZGERALD. Let me just——

Mr. SCOTT. Well, no, no, because people keep coming here, time and time again—this isn't the first hearing we've had.

Mr. FITZGERALD. I know.

Mr. SCOTT. They come and say you need a FISA to protect from terrorism.

Mr. FITZGERALD. Yes.

Mr. SCOTT. And then you point out that you can get a FISA warrant for things—have nothing to do with crimes, have nothing to do with terrorism, if you can get foreign affairs. The example I've used is——

Mr. FITZGERALD. And I disagree with that. And if you could let me explain, because you do need——

Mr. SCOTT. Okay, okay, well, let me make my point——

Mr. FITZGERALD. Okay.

Mr. SCOTT. —so you know what you're disagreeing with.

Mr. FITZGERALD. Okay.

Mr. SCOTT. If I've got probable cause that somebody's an agent of a foreign government, and we're about to negotiate a trade deal, and I can get their bottom price on steel, can I get a FISA wiretap?

Mr. FITZGERALD. That answer? I'll be blunt. I don't know.

Mr. SCOTT. Okay.

Mr. FITZGERALD. Because I—what I'm saying is I don't——

Mr. SCOTT. The answer everybody else has given is "Yes." And that's how easy it is, and how unrelated to crime and terrorism these FISA wiretaps are. And if you can—if that's all you've got to get, to get into somebody's home, to get a wiretap and all this, then it's a lot easier to run a criminal investigation without having to fool around with whether a crime is actually being committed.

Mr. FITZGERALD. Except that, if that's what you are doing, you'd be lying and making a false statement when you certified that the purpose of the investigation was to gather foreign intelligence. And when you try to bring that person into court for some drug crime and say, "We had a FISA wiretap," and show it to the judge, for something else, it would be out of it. Let me make this point——

Mr. SCOTT. A significant purpose was getting the bottom price on steel, and you tripped over a drug deal. Or you knew the drug deal was happening, and you knew he was negotiating a trade deal.

Mr. FITZGERALD. Sir, all I can tell you is this. In Chicago, we spend—I spend a lot of my time prosecuting drug cases and gang cases. We have never contemplated, much less done, anyone going near a FISA court to get a drug wire. We've got plenty of other——

Mr. SCOTT. Then what was the Attorney General talking about when he said, if the primary purpose of the FISA wiretap wasn't foreign intelligence, what was it? Why did he say "criminal investigation"?

Mr. FITZGERALD. And if I could get to the second part of what I wanted to say, it's most of those predicates require probable cause of activities which themselves are crimes when people commit ter-

rorist acts. The point being, I think that the primary purpose itself is a fiction. And I'd like to explain that, because I think it's important.

It may be that people say early on you don't know what the primary purpose is. Let me give you an example. If a CIA officer came into my office tomorrow and said, "We have sensitive information coming from overseas that someone's going to put a bomb in the middle of Chicago next week, and take lives," we would have the CIA in the room sharing their information. We would put the FBI in charge. We'd have several—lots of agents in Chicago. We'd have the Chicago Police Department. And we'd say, "Let's stop this bombing. Let's get the information, and let's go prevent it."

If you ask the CIA officer under truth serum what is the primary purpose in what he's doing, I have no doubt that he or she would say, "This is an intelligence operation to stop a bombing." If you ask the Chicago Police Department, "What is the primary purpose of this operation?" he no doubt, or she no doubt, would say, "We are trying to prevent the crime of a bombing that—"

Mr. SCOTT. You can't get a criminal warrant on something like that?

Mr. FITZGERALD. If it's coming from overseas, it might be a FISA. It may not be a criminal warrant, if it was classified information that we could not use. If it was an Al-Qaeda operation doing this bombing on behalf of a terrorist group, that is appropriate for a FISA.

My point being, different people involved in the same operation may have—one may have an intelligence purpose; one may have a criminal purpose. And if I, as the prosecutor, have to sit there and figure out, "How will a court review this later?" if there's a bombing prevented and people are arrested, and have to decide, "I can't use FISA, I can't use title III, I'm paralyzed"—we need to know that there's a legitimate intelligence purpose in trying to prevent a terrorist group from bombing a major metropolitan city, and we go forward.

We can't sit around having a philosophical discussion, saying, "Who thinks it's intelligence? Who thinks it's law enforcement? Where does the balance go?" We can't do that. And that's what we used to do.

The fellow in the back who testified this morning, Rob Khuzami, and I worked a case together in New York in 1994, where people were plotting to blow up the bridges and tunnels in New York. And no one wanted to bring the prosecutors in until the end because they were afraid that, by talking to prosecutors, it would look like a law enforcement matter, and the FISA may later be thrown out.

We can't go through a world where we don't bring in the cops and the prosecutors to decide what to do because we're afraid the consultation will color how a court looks at it later. So I think it's a fiction that a primary purpose exists. There are purposes. And if you have a legitimate intelligence purpose, I think we need to be able to proceed.

Mr. CHABOT. The gentleman's time has expired.

The gentleman from Indiana, Mr. Pence, is recognized for 5 minutes.

Mr. PENCE. Thank you, Mr. Chairman. And thank you for holding this hearing. I had—and I want to thank the panel. This is an extraordinary panel of experts and public servants. And I'm most especially pleased to have the opportunity to hear from and to meet Mr. Fitzgerald, whose reputation in law enforcement is highly regarded in this nation. And I'm grateful for your insights.

Two questions specifically for the panel. I'm very intrigued in reading your statement, Mr. Fitzgerald. I was literally added to the Judiciary Committee a week before we wrote the PATRIOT Act. I haven't crammed like that since law school. But I've been a defender of this act, believing that it has balanced our civil liberties in this country with positive advances in our ability to confront the enemies in our midst.

And I'm struck in your testimony by a variety of examples that you use; even one, I believe, that had to do with the '93 bombing of the World Trade Center and one Sheikh Omar Abdel Rahman who there were—according to your testimony, that there were criminal and intelligence investigations, but that prosecutors—because of "The Wall" that we're talking about in this hearing, prosecutors didn't have that information.

And it is—is it accurate to say in that case that prosecutors were in the dark about the details of a plot that our intelligence officials knew about by Sheikh Rahman to bomb the Holland and Lincoln Tunnels, the FBI Building, the UN, the George Washington Bridge, until very late in—very late in that investigation; and that that's materially changed by the section of the PATRIOT Act we're here to debate?

Mr. FITZGERALD. Yes. My understanding is that the first time a prosecutor was told about it, they were told very little, other than that it was an operation going on. And because FISAs were up, they were very concerned about contacts with prosecutors making it look like it was a primarily criminal purpose. And so they were brought in very late in the day, and decided when things had to be taken down, so to speak.

And a similar experience happened around the millennium, when there were threats to our country. And myself and my partner, another lawyer, sat by the phone for many days going up to the millennium eve, waiting for a phone call, if there was anything we could be told; while people on the intelligence side dealt with the case.

After the PATRIOT Act, if there were a threat like that, we'd be sitting down at meetings with the FBI, CIA, and exchanging information and deciding what we ought to be doing appropriately that is lawful and that will best protect our country.

Mr. PENCE. Thank you. It's just amazing to me. I think any Americans looking in on television at this hearing would be astounded at what used to be the practice—the left hand not knowing what the right hand is doing—between intelligence and domestic law enforcement.

Mr. Kris, you testified that you thought that if section 218 sunsets, that law enforcement would have greater authority.

Mr. KRIS. Yes.

Mr. PENCE. Which flies in the face of many of the critics of "The Wall." Now, I know you discussed this in your written testimony.

I'm looking at page 12 of your written testimony and—but I'd love for you to elaborate on that, because I think it's an intriguing point. Because as a limited-Government conservative, I'm always interested in how do we advance national security——

Mr. KRIS. Right.

Mr. PENCE. —and do that in a way that's consistent with limiting Government intrusion.

Mr. KRIS. Right. Well, I think the answer to your question really depends on an understanding of the decision of the Foreign Intelligence Surveillance Court of Review.

Mr. PENCE. Uh-huh.

Mr. KRIS. What that court held was that, as enacted in 1978, FISA did not discriminate between law enforcement methods of dealing with or protecting against terrorism and espionage and other foreign threats to national security, and any other method—a traditional intelligence method, diplomatic method, and so forth—of dealing with those threats.

So, the court basically held that, as enacted in 1978, FISA would have allowed surveillance even where the sole purpose was to prosecute a terrorist or a spy. The distinction, the court said, was not the nature of the method used to address the threat—law enforcement methods or some other method—but rather, the nature of the threat that was being addressed—a terrorist threat, as opposed to, say, a routine domestic crime, bank robbery or what have you.

But the court recognized that for 23 years everybody misread the statute in all three branches of Government. And until the Department figured it out and advanced the argument in the appeal, and the court agreed, nobody knew. Which meant that at the time the PATRIOT Act and section 218 in particular was enacted, the misunderstanding prevailed. And so the court held, section 218, in effect, codified that misunderstanding and created this false distinction between law enforcement methods of dealing with these threats and all other methods.

Now, if 218 were to sunset, I think the misunderstanding would sunset, too. Or at least there's a substantial argument to that effect.

Mr. PENCE. Well, you would lose that element of the statute that would clarify what the significant non-law enforcement purpose standard.

Mr. KRIS. And so I think you would probably—and again, I haven't done the really heavy lifting that would be necessary to determine this authoritatively. But I think you can see the logic of the argument that if 218 sunsets, you revert to the original—albeit newly discovered—meaning of the statute.

Mr. PENCE. Uh-huh.

Mr. KRIS. And that is why I believe if 218 sunsets without more, the Government may have more power than it does today.

Mr. PENCE. So——

Mr. CHABOT. The gentleman's time——

Mr. PENCE. —Americans' privacy rights were strengthened by the PATRIOT Act, in that regard.

Mr. KRIS. The PATRIOT Act cut back on Government power. That is what the court of review said.

Mr. CHABOT. The gentleman's time has expired.

The gentleman from Ohio seems to be chomping at the bit there, so go ahead, if you have a quick point.

Mr. SWIRE. Well, I think another way to look at it is there's a circuit split between the five or six circuits that went one way, and the FISA Court of Review that went the other way. Because there were numerous circuit court judges that had what the Justice Department found was a misunderstanding.

Mr. CHABOT. Thank you. We were just getting ready to go to a second round. Two Members have just gotten here. Did you want to get in on the second, or you still want to get in on the first?

Ms. JACKSON LEE. First.

Mr. CHABOT. You want to get in on the first. Okay. The gentlelady from Texas is recognized for 5 minutes.

Ms. JACKSON LEE. Thank you, Mr. Chairman. We have seemingly been patriotic now for a couple of days, and we've lived with the PATRIOT Act for a longer period than that. I want to thank the witnesses for their testimony, and the Ranking and Chairman for this hearing.

I was just meeting with some constituents, and one of their chief issues was the question of civil liberties. Isn't it interesting, in 2005, that that doubt of having civil liberties is being raised by Americans really across the land.

I think the important point to be made possibly—or for those of us who sit on this side of the panel is that there is not a divide in wanting to make sure that the homeland is secure; or, frankly, that there are not the basic and enhanced resources for law enforcement. But we have to be, in essence, the wall, the divide, the protector of excessiveness, and the representation that the present state of the law is not adequate.

So I simply—I appreciate the U.S. Attorney in his deciphering "primary" and "significant" and I will—Mr. Fitzgerald, I want to raise some questions with you. But Mr. Swire, if you could let me know, I know that there have been mistakes that the Department of Justice has made—some 70 of them, as I understand it—about information sharing, unauthorized dissemination of information. In fact, I think Attorney General Janet Reno first interjected into trying to give guidelines of where the FBI could begin to share information with the U.S. attorneys.

My question to you is to pick up where my colleague, Congressman Scott, was as I was listening to his inquiry about this "significant" and "primary" question. But also, have we even fixed some of the problems that are generated from the misrepresentations of information sharing, unauthorized dissemination of information? And how do we know that the Department has any knowledge of these misrepresentations and has any ability to account for them?

And let me make this other point. We learned in an earlier hearing today that we have the right to get certain information, the Congress does, under FISA. And I'm wondering whether we are even getting that information. Not only do we have the right to get information, but the public has a right to have pronouncements being made.

In your profession, or as you have traveled the highways and byways, are we fulfilling our responsibility? Are you getting pronouncements from the DOJ, or local DOJ, about anything dealing

with FISA? I yield to the gentleman. And I may interrupt you because my green light may go and I may want to deal with Ms. Martin or Mr. Kris and Mr. Fitzgerald.

Mr. SWIRE. Thank you, Congresswoman——

Ms. JACKSON LEE. Yes, sir.

Mr. CHABOT. The green light just went so——

Ms. JACKSON LEE. I'm on a beige light now, but that's all right.

Mr. SWIRE. A couple of points. One is attached to my testimony are possible oversight questions, to try to ask some questions that maybe the Committee would find useful to ask the Department of Justice. I think that having a greater oversight by the Judiciary Committees going forward—if this turns out to be really a criminal statute so often, maybe the Judiciary Committee should get the same oversight information that the Intelligence Committee——

Ms. JACKSON LEE. But do you know if they've answered any of the problems dealing with the question of 70 misrepresentations?

Mr. SWIRE. Well, it points out that there's no adversary process in the FISC court—in the FISA court. And the court there was able to discover that more or less on its own. And so we need to figure out how that oversight is going to happen in the future.

Ms. JACKSON LEE. Ms. Martin?

Ms. MARTIN. Well, I'd like to make the point that I think there are really two separate issues being talked about here. One is sharing and the failure to be able to share before September 11th, described by Mr. Fitzgerald. And I think we all recognize that that was a mistake and that it shouldn't happen again; that we don't want to write in a legal prohibition on that kind of sharing.

But the question I think that the Committee faces in connection with 218 is not a sharing question, but is the question of when are the FISA authorities going to be allowed to be used? The FISA authorities allow the Government to secretly search Americans' homes and secretly wiretap their telephones.

And those are extraordinary powers, going to the core of the fourth amendment. One of the core fourth amendment protections has been that when a person's home is searched and their telephone conversations are tapped, after the fact they're told about it. FISA is—the whole point of FISA is that you don't have to tell the person that that happened.

Section 218 broadens the circumstances under which the Government can use those extraordinary powers. And I think that the question the Committee needs to focus on is, given that we are going to have those extraordinary powers, given that we of course want the information collected by FISA to be freely available to law enforcement and prosecutors, what kinds of protections are we going to have against abuse of those secret powers? And the Mayfield case is an example, I think, of that problem; which I'd be glad to talk about.

Mr. CHABOT. The gentlelady's time has expired. I think the gentleman on his time is going to ask for a follow-up, because we're already on 7 minutes on yours.

Ms. JACKSON LEE. If Mr. Kris and Mr. Fitzgerald can answer, I'd appreciate it.

Mr. CHABOT. Well, they will, but I don't want to drag this out too long. The gentleman from California is recognized at this time.

Mr. LUNGREN. Thank you, Mr. Chairman. And I would ask Mr. Fitzgerald and Mr. Kris to please respond to the last comments made by Ms. Martin with respect to the fact that the—that 218 expanded in these areas these kinds of searches, and does not give adequate notice; and seemed to suggest that therefore it is inappropriate.

Mr. KRIS. I'll speak to the 218 question, because I'm actually prepared to say that it is essentially the case that 218 and the provisions that tear down "The Wall" don't affect the "who," the "what," the "where," the "when," or the "how" of FISA surveillance. What they really do is permit the two hands of the Government—law enforcement and intelligence—to talk and communicate in a normal way, one to the other.

When "The Wall" is up, the Government is free to do any surveillance that it can do when "The Wall" is down, with one condition; and that is, the prosecutors have to be kicked out. And there is no change connected to "The Wall" in the probable cause standards or the definitions of "agent of foreign power" or "foreign power." And so the same people can be targeted to the same extent on the same facilities.

The difference is that law enforcement officials can be involved and coordinate with the intelligence officials. The Government is essentially no longer put to that very difficult choice between either, A, coordinating or, B, conducting the surveillance. They can now do both. So I guess that's my basic response on that.

Mr. LUNGREN. Mr. Fitzgerald?

Mr. FITZGERALD. He said it better than I would have, so I agree.

Mr. LUNGREN. All right, you're not going to get off that early. Mr. Fitzgerald, in Ms. Martin's testimony, her written testimony, she suggests that Congress should take the opportunity to bring the FISA information in criminal proceedings "in line with basic due process requirements." It's my understanding that the current procedures governing FISA in criminal cases have been upheld as constitutional in Federal courts across the country. Are you aware of any Federal court that has held that the current procedures are unconstitutional?

Mr. FITZGERALD. No, and in the several times it's been litigated in cases I've participated in, it's always been held to be constitutional and to comport with due process.

Mr. LUNGREN. Even in the event that no courts have found it unconstitutional, do you see any reason for reforms? And if so, what reforms would you suggest?

Mr. FITZGERALD. I, personally, don't. I think that when judges review these materials they do review them to make sure that they're in order. And I think that—I think it's appropriate, given the sensitive nature of the material that goes into applications, often which can come from very sensitive sources or foreign governments who do not wish what they contribute to be exposed and the sources and methods.

Mr. LUNGREN. You talked in your testimony about the investigation of Osama Bin Laden in the 1990's. Based on that experience, how damaging do you think "The Wall" was to our nation's counterterrorism efforts during that time?

Mr. FITZGERALD. I think it was extremely damaging and——

Mr. LUNGREN. Why?

Mr. FITZGERALD. I would describe it this way. National security and civil liberties are both extremely important, so I'm going to make an analogy to a game; not because I don't think life and liberty and privacy aren't serious. But if you played football and you were on defense, and your job was to make sure no one attacked you, and where the risk were lives, you would not tell the defense that they have to separate into two huddles and can't talk to each other; which is what "The Wall" did.

And if you went and played a game like that, where two separate huddles couldn't collaborate, and one day they finally said, "You know what, you could actually talk before the other team tries to score a touchdown," where the price of a touchdown is lives, you would recognize that there's no way we should go through a dysfunctional system where we're not talking to each other, trying to defend against a lethal threat.

Mr. LUNGREN. Do you understand the concerns that some people have, that tearing down "The Wall" would in some way jeopardize our protections of individuals' privacy rights?

Mr. FITZGERALD. I do. I absolutely understand that, for two reasons. I understand privacy rights are very important. I want my privacy rights protected, so I don't at all cast any doubt on why people would be concerned about their privacy rights. And I understand the history from the '60's and '70's, why people would be concerned about that.

From a pragmatic point of view, I agree with David Kris. I think we do our best job, not just of protecting national security, but protecting privacy rights and civil liberties, if we have the law clear, and we put lawyers and others in the room and say, "These are the rules of the road," and we work together and make sure people don't make mistakes.

So I think that "The Wall," while it protects national security, doesn't jeopardize civil liberties—we want a system where we're all operating on the same set of laws and rules, and follow them, and make sure that people who are responsible, and have law degrees that they want to keep and jobs they want to keep, follow the rules and make sure that everyone around them follows the rules.

Mr. CHABOT. The gentleman's time has expired. We are going to go to a second round at this time, so I recognize myself for 5 minutes.

Mr. Kris or Mr. Fitzgerald, let me ask you this question. Do terrorist organizations work with other criminal elements, such as drug dealers and street gangs and other violent criminals of that nature? And if so, can you give some specific examples of that? And how common is this cooperation or association between terrorists or terrorist organizations and other criminal elements?

And prior to enactment of 218, how would the law enforcement agency in charge of the criminal investigation coordinate with the foreign intelligence agency in charge of the terrorist investigation? And how cumbersome was that process? And again, some of these things we've already touched on time and time again.

Mr. FITZGERALD. I will give you my limited perspective. I do know there have been occasions in the past where gangs and terrorists have linked up. I think going back to the late '80's, there

was a Chicago gang that tried to get shoulder-fired missiles for a foreign country—I think Libya—and that was exposed and later prosecuted. So that has happened.

In my personal experience, I've more seen more incidental involvement of gang members or street criminals. For example, the plot where they were trying to blow up the bridges and tunnels in New York City: they had to get stolen cars; they had to get guns; they had to get things like that; where in the course of an investigation they were dealing with street-level criminals, just because they needed fake passports; they needed cars; they wanted to get detonators. So they got into this with the criminal underworld because they needed to get logistics. But it was more of a—the plan was being done by the terror ring, and they were reaching out to other people just to get logistics.

I don't see us using FISA to go after a gang problem, at all. What I do see is if FISA's going after a terrorist problem, we may incidentally pick up someone if they turn to a gang member or street criminal as part of their effort to get a, you know, weapon or a detonator, that sort of thing. But I haven't seen yet a situation where we haven't been able to just deal with it as a terrorism issue where you might incidentally come across street-level criminals. And I hope it stays that way.

Mr. CHABOT. Thank you. Mr. Kris, anything you want to add to that?

Mr. KRIS. I'm not going to say anything about any particular cases, I don't think, in an open hearing; and as a former Government lawyer, not a current one.

I will say that there are cases that I know of that are public, in which terrorist organizations or other national security threats have used what would otherwise be sort of more traditional kinds of crime, to finance or facilitate their terrorist acts. We had cigarette smugglers, for example, who were raising money to buy weapons. And that can happen.

I think, legally, those kinds of crimes are treated like foreign intelligence crimes, under the new law tearing down "The Wall." And FISA could be used to gather evidence of those kinds of crimes. It can't be used to gather evidence—or primarily to gather evidence of ordinary crimes that are not being committed to facilitate those kinds of national security threats.

Mr. CHABOT. Thank you. Ms. Martin, you stated in your written testimony, and I think today orally as well, that the FISA statute authorizes secret surveillance on less probable cause of criminal activity than is authorized by the fourth amendment in criminal investigations. Some have claimed that FISA has no probable cause requirement. Is it your opinion that FISA has a probable cause requirement, or not? Would you comment on that, please?

Ms. MARTIN. Yes. It's clear that it does have a probable cause requirement, and the probable cause requirement is, as Mr. Fitzgerald stated, that someone be an agent of a foreign power. There are then paragraphs defining what an agent of a foreign power is.

In the terrorist context, it's pretty clear that that would be the equivalent of probable cause of criminal activity. But in the clandestine intelligence gathering context, which also applies to FISA, it's also clear that—if you read the FBI's own memo on the use of

FISA, that the probable cause required is less than the probable cause required for a purely criminal warrant in that context. Which is not to say there's no probable cause and that there is a criminal nexus, but the—And I see Mr. Kris agreeing with me, so I'll just end——

Mr. CHABOT. Okay.

Ms. MARTIN. —before I say anything else.

Mr. CHABOT. Okay. My time is about ready to expire. Let me ask one more question, if I could. Either Mr. Kris or Mr. Fitzgerald, would you explain why the FISA Court of Review concluded back in 2002 that section 218 of the USA PATRIOT Act is constitutional? And as the Chairman of the Constitution Subcommittee, I'm particularly interested in that.

Mr. KRIS. I'll try to—I'll try to tackle that. The court basically held that FISA is constitutional because it is reasonable, and reasonableness is the touchstone of analysis under the fourth amendment.

The court specifically relied, I think, on two prior Supreme Court decisions. First, the *Keith* case, United States against the United States District Court, from the 1970's; and the more recent decision of *City of Indianapolis v. Edmond*.

Keith held that in the case of surveillance involving domestic terrorists, standards different than and lower than those in title III would be permissible, because of the special nature of the threat that those kinds of domestic terrorist cases present. And I think that reasoning applies, a fortiori, to FISA, which involves foreign threats to national security, which are even more dangerous and more difficult to investigate.

In *Edmond,* the Supreme Court drew a distinction between ordinary and special kinds of law enforcement in its analysis and discussion of a checkpoint. And so I think the basic reason that the Court upheld FISA is that, like the statute which distinguishes between kinds of threats, rather than kinds of responses to threats, so, too, the fourth amendment ultimately draws that distinction. And surveillance is lawful under FISA if it is addressing the kind of threat that the statute deals with, regardless of the kind of method being used to deal with the threat.

Mr. CHABOT. Thank you very much. My time has expired.

The gentleman from Virginia is recognized for 5 minutes.

Mr. SCOTT. Thank you, Mr. Chairman. Mr. Kris, did I understand you to say that domestic—investigation of domestic terrorism did not require the same level of probable cause as other criminal warrants would require?

Mr. KRIS. Under current statutory law, that is not correct. Those would proceed under title III, the conventional criminal statute. But under the Constitution, the Supreme Court held in *Keith*, standards lower than title 3 maybe—or maybe not, in the probable cause area—would be tolerable.

Congress has never taken up the Court on that invitation in *Keith*, and has not enacted a special statute governing domestic terrorism. But *Keith* indicates that it could do so.

Mr. SCOTT. But the present state of the law is that domestic terrorism cannot be investigated with a lower probable cause standard than other crimes? That's the state of the law today?

Mr. KRIS. Yes.

Mr. SCOTT. Ms. Martin, you indicated about a criminal nexus to title—to FISA once. Did you say you needed a criminal nexus, or could have a criminal nexus?

Ms. MARTIN. Well, when you're investigating "clandestine intelligence gathering," as opposed to terrorism, it's not defined to equal criminal activity. It's defined to include activity that might be criminal. So you could say——

Mr. SCOTT. And it could——

Ms. MARTIN. —that it's connected to, but it's not a criminal probable cause standard.

Mr. SCOTT. It could be connected to the conduct of foreign affairs of the United States.

Let me ask Mr. Fitzgerald. Your reading—What code section were you reading off of when you were responding to the other question?

Mr. FITZGERALD. Fifty—Title 50, United States Code, Section 1801. When I talked about the agent of a foreign power, I was reading from section "b," and when I read from international terrorism, I think I read "b," and the terrorism parts were subsection "c" and "e." They also have in there the sections about clandestine intelligence activity.

Mr. SCOTT. Okay. Because I'm reading Title 1, section 101. When you talk about getting a FISA warrant, you can get it if you're getting foreign intelligence. And foreign intelligence information includes the conduct of foreign affairs of the United States; which may or may not have anything to do with a criminal activity.

Mr. FITZGERALD. And you're reading from subsection "e." And my point being, you have to satisfy the standard earlier that the person is an agent of a foreign power. If you satisfy that—and to be an agent of a foreign power, to engage in clandestine intelligence activity, that is a crime. To be an unregistered agent of a foreign power is a crime in itself.

Mr. SCOTT. Well, if you are a registered agent of a foreign power.

Mr. FITZGERALD. If you are a registered agent? Okay.

Mr. SCOTT. Yes.

Mr. FITZGERALD. Okay. Then if you're a registered agent of a foreign power, then that may not be a crime, because you're obviously not—you've registered. But if you're engaged in clandestine intelligence activities, you're a spy.

Mr. SCOTT. Well, if you are a registered agent of a foreign power——

Mr. FITZGERALD. Engaging in clandestine intelligence activity.

Mr. SCOTT. No. No, we're going to get some information from you. And the idea—your bottom price on a steel deal we're going to negotiate tomorrow afternoon. If I know you're going to be talking to people back home, I can wiretap your phone and listen in to get that information. And that's a FISA wiretap. No crime; just getting information. Right?

Mr. FITZGERALD. And as I told you before——

Mr. SCOTT. You don't know.

Mr. FITZGERALD. That part of it, I'm less familiar with. I could just read the statute——

Mr. SCOTT. Okay, well, see, we've got to deal with the whole thing. You're dealing with terrorism, and we're dealing with the code and determining whether we're going to allow this to continue. And the idea is, since we changed that primary purpose to a significant purpose, the Attorney General told us that you can run criminal investigations out of FISA on these lower standards.

Mr. FITZGERALD. And I could just add that the PATRIOT Act did not change that definition. The FISA statute, it didn't change the——

Mr. SCOTT. That it changed to say "primary purpose" to "significant purpose"; which invites the question, if it's not the primary purpose, what is?

Mr. FITZGERALD. And my only point being that if it's lawful to listen in on those trade negotiations, it was lawful before the PATRIOT Act, and afterwards.

Mr. SCOTT. Yes, but you can't run a criminal investigation. You can't use it as an excuse to running a criminal investigation if that wasn't your purpose.

Mr. FITZGERALD. And you can't do it here, if your primary purpose isn't to gain foreign intelligence. You have to certify that. That would be false if your——

Mr. SCOTT. Well, that's why we changed the law, so you could run a criminal investigation without probable cause. Let me ask a quick question, before all my time runs out. How do you challenge a FISA wiretap that was inappropriate? In criminal investigation, you challenge it using the exclusionary rule. How do you challenge—if they shouldn't have gotten the wiretap to begin with, if it was really a ruse, how do you challenge it?

Ms. MARTIN. It's impossible. Not only would you not be able to challenge it, you would never know about it. And that's the whole difficulty. And that's what Brandon Mayfield's case illustrates. There they got a secret FISA search of his home, and it turns out he's innocent. There's nothing in the statute that required the Attorney General or the Justice Department to inform him that the FBI had been inside his house. And the Justice Department made that clear when they did inform him, because they said, "We're going to tell you that, but we didn't have to tell you we were inside the house."

And the reason, apparently, they told him that they had been inside the house was only because he had been mistakenly jailed. So if he hadn't been jailed, he never would have been told that they had a wiretap or a physical search of his house, when it turned out it was a mistake.

And that's the problem that I think this Committee needs to look at. And that problem did pre-exist section 218 of the PATRIOT Act. There's no doubt about that. But it's been exacerbated.

Mr. CHABOT. The gentleman's time has expired, but if you want to follow up just for a minute——

Mr. SCOTT. I do want to follow up. I wanted Mr. Swire to comment.

Mr. SWIRE. The simple point I wanted to make is that in Kate Martin's testimony, she proposes legislative fix that's based on CIPA, classified procedures act, which came after 1978, and is a better way for handling those challenges than the '78 law had. Ba-

sically, we should update our 1978 version of FISA to the things we learned over time for how to handle the classified information and have those challenges done better.

Mr. SCOTT. Okay.

Mr. CHABOT. The gentleman's time has expired.

The gentleman from California, Mr. Lungren, is recognized for 5 minutes.

Mr. LUNGREN. Thank you, Mr. Chairman. Mr. Kris, I'd like to direct this to you, because listening to the comments and the questions of the gentleman from Virginia prompts this question; which is when we're talking about FISA and he's talking—and we're talking about a non-criminal act—we're talking about the position another country may have on trade—FISA can only come into effect if the individual involved is a foreign agent—an agent of a foreign government; is that not correct?

Mr. KRIS. Yeah. I mean, I think there's two separate legal requirements here that may be getting a little bit mixed.

Mr. LUNGREN. Yes.

Mr. KRIS. And maybe I can try to differentiate. To be a FISA target, you have to be an agent of a foreign power, or a foreign power, and the Government has to establish probable cause, the court has to find probable cause. And that's a requirement that, just as Ms. Martin says, in some cases, particularly where it's a terrorism case involving a U.S. person, it's essentially the same probable cause standard as in a criminal case, plus some additional requirements.

But in the espionage context, it's a slightly different standard. It is activities that involve, or may involve, or are about to involve a crime; which is—and the legislative history is very clear on this—somewhat lower than the traditional criminal probable cause standard. That is what the statute says.

The other requirement in a FISA application is a certification from some high-ranking Executive Branch official, like the FBI Director, that now a significant purpose is to obtain foreign intelligence information. There are two kinds of foreign intelligence information. There's the kind that is normally at issue in these kinds of "Wall"-related cases, what I will call counter-intelligence, or protective intelligence, information that is relevant or necessary to protect against a series of specified threats—terrorism, attack, so forth.

There is also a second definition in foreign intelligence information, and I'll call that affirmative, or positive foreign intelligence. And that is information with respect to a foreign power or foreign territory that relates to or, if concerning a U.S. person, is necessary to the defense or security of the United States or the conduct of foreign affairs.

And it is absolutely correct that information that is relevant to a trade negotiation would be, I think, or could be foreign intelligence information, under this second definition. However, I will also say that information is foreign intelligence information under that second definition only if it is with respect to a foreign power or a foreign territory.

And if you read the legislative history there, they contrast that "with respect to" language. On the one hand, with respect to a foreign territory or power; on the other hand, not about a U.S. person.

And so it really is, I think, if you read the legislative history, the kind of information that you would get from monitoring visiting foreign trade delegations, if that's what you were going to do. And I'm not saying we do it or not.

Mr. LUNGREN. As opposed to an American citizen.

Mr. KRIS. Right. And the two requirements are, in any event, independent. Because even if—it would be a very strange case, I must say, in which the Government would assert, on the one hand, there is probable cause that this U.S. person is a terrorist, or is knowingly engaged in international terrorism or activities in preparation therefor; and yet, our primary purpose is to gather information about a trade negotiation. That would be a very odd disjunction.

And I think—I don't say you should rely on the good faith of the Government officials involved. Having been one, I know better than that. But it would certainly be a difficult articulation for the FBI Director to make.

Mr. LUNGREN. Well, see, what I'm trying to do is figure out if we've been hearing about a straw man for quite a bit of time in various questions, or whether this is a serious problem. I mean, I'm aware of no abuse in this area. But is it a serious problem, where an American citizen has to worry about somehow FISA being used to invade their privacy under some tortured version of these terms? I'm just asking——

Mr. KRIS. Yes.

Mr. LUNGREN. —for your help on this, looking at this statute.

Mr. KRIS. I think my basic answer to that question is "No," because the probable cause requirements in 1801 of Title 50 remain the same, both before and after the PATRIOT Act, and still require the Government to make a substantial showing of criminality in clandestine intelligence cases, and what amounts to a full-blown traditional criminal showing of probable cause in a terrorism case, regardless of what prong of the foreign intelligence definition they are proceeding under.

Mr. LUNGREN. Thank you.

Mr. CHABOT. Does the gentleman yield back? The gentleman's time has expired.

The gentlelady from Texas is recognized for 5 minutes.

Ms. JACKSON LEE. I'd like to go back to Ms. Martin. But before I briefly turn to you, I just want to state for the record, to make it very clear, you were delineating two very horns of the dilemma that Members of this Committee and Congress have. And that is, of course, to recognize the vitality of information sharing, i.e., the—for lack of a better word, the sort of "Three Stooges" approach pre-9/11. And I don't say it unkindly. But I think many of us were sort of aghast about the lack of sharing that we thought might have been helpful. And of course, that was a combination of domestic and international only because the individuals came into the country. But there were some that were there in the country doing activities that did not seem to funnel in one place. So I don't disagree with you. And I think I don't even glean that we would not be concerned that we can't do a better job at information sharing.

I think there's some question of whether or not—we have this national intelligence director, which we now have, and, you know,

whether that bridges any necessary intelligence necessities because of the CIA, because of the FBI and other elements, that need to cooperate.

But the other part of it is—and these are my words—the broadness, the depth, of the power of the Government in utilizing FISA, and when to use this broad-based power; which is what my concern is. I've seen some looking maybe aghast or shocking from Mr. Kris when I mentioned the "Three Stooges," but this is—we're all big boys and girls up here and we can face conversation that may be somewhat pointed.

Again, it's not a personal commentary. It is just a commentary of what we've found ourselves. And when I say that, let me put everybody in the same boat together. Everybody was equally shocked that maybe there were not procedures in place.

As I look at your testimonies—so my interest is really to do as you've noted. In fact, I've noted in your testimony that the national security study deals with the question of protecting us and civil liberties. And I assume you're consistent in your work. And I think that's a fair balance. Maybe we're not—we probably won't agree on many issues. I happen to be on Homeland Security. I say that—I've said that before. But I think that you wouldn't ask a Member of Congress that they are not interested in that part of security—of securing the homeland. But it's the use of this power that concerns me.

And I circled something here: "The center has long advocated the necessity of tying domestic intelligence authorities to law enforcement to ensure that Government surveillance is targeted against actual wrongdoers, and not against political or religious minorities." However, if, for example—and I'm on the domestic side—a religious minority had as its philosophy and also its action the bombing of abortion clinics; its faith or its views were that they are absolutely abhorrent—abhor them, but then the next step was that they planned bombing—bombings. You don't include that in protections of civil liberties; is that correct?

Ms. MARTIN. No. That's actually an issue that we worked on to a great deal before September 11. Because we were concerned about two things: that the Government adequately investigate and stop abortion clinic violence; but that it not target groups who opposed abortion, or conduct surveillance of groups who opposed abortion, simply on the excuse that it was trying to stop abortion clinic violence.

And that line—between investigating and targeting politically motivated violence, while being careful to respect the first amendment rights of those who might share the political views of the violent actors—is an extremely important and difficult problem.

Ms. JACKSON LEE. Right. Let me take you up on that. Lights go out quickly here. Let's take that on the international basis, or at least the basis of groups that have gotten profiled: Muslims who gather in a mosque here in the United States; Pakistanis; people from Iran who live in the United States. Then how would the center expand on where you're going with the protection of the civil liberties and to avoid this expansive use of this procedure and still—where would we begin, or where would we take this hearing to really respond to that?

Because that, I think, as much as this is such a wonderful panel that talks about the necessity of security, and the U.S. Attorney, but we have in here the makings of the broad use of this procedure. How would you answer, a good way of providing that protection?

Mr. CHABOT. And the gentlelady's time has expired, but you can answer the question.

Ms. JACKSON LEE. You can answer the question, thank you. Thank you, Mr Chairman.

Ms. MARTIN. Well, I think it's an extremely important and extremely difficult question to answer, that has to be answered in many different specifics. But I think that, given where we are, that we are going to continue to have the use of what are basically completely secret surveillance authorities; and which we tried to write in all of these detailed protections so that people wouldn't be spied on because they were Muslim. But as you can tell from all of the lawyers sitting here, it's a complicated statute. And whether or not those details in the statute in the end are going to be sufficient to protect people is not—no longer clear to me.

I think that we have to come up with some new ways to look at what the Government is actually doing. And it's a hard problem because, of course, they have to operate in secret here. But I think I've made a couple of suggestions.

I think another suggestion we haven't talked about is that this Committee go look at the actual FISA applications, the warrants, and the returns, especially of U.S. persons, and see who's being surveilled and what they found when they've done the surveillance, and actually look at that. And that's another way to look at this problem.

Ms. JACKSON LEE. I thank the gentlelady. We'll take you up on that. At least, I will. Thank you.

Mr. CHABOT. Thank you. The gentlelady's time has expired. That concludes the second round of questioning.

And at this time, I'd like to ask unanimous consent to include in the record the Department of Justice's response to a letter from Senator Feinstein alleging abuses under the PATRIOT Act. And I understand that this indicates the absence of those abuses.

I'd also like to thank the witnesses for their testimony here this afternoon, which I really thought was excellent. The Subcommittee very much appreciates your contribution to this important effort. And in order to ensure a full record and adequate consideration of this important issue, the record will remain open for additional submissions for 7 days. Also, any written questions that a Member wants to submit should be submitted within the same 7-day period.

That concludes the Oversight Hearing on the "Implementation of the USA PATRIOT Act: Section 218—Foreign Intelligence Information. ('The Wall')" I want to thank all the Members for their attendance and their participation this afternoon. We want to especially thank the witness panel for being here and answering our questions. And if there's no further business to come before the Subcommittee, we're adjourned. Thank you.

[Whereupon, at 4 p.m., the Subcommittee was adjourned.]

APPENDIX

MATERIAL SUBMITTED FOR THE HEARING RECORD

PREPARED STATEMENT OF THE HONORABLE ROBERT C. SCOTT, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF VIRGINIA, AND RANKING MEMBER, SUBCOMMITTEE ON CRIME, TERRORISM, AND HOMELAND SECURITY

Thank you, Mr. Chairman, for holding this hearing on the issue that has been foreshadowing much of our discussion about the PATRIOT Act—the extent to which it dismantled "the wall." Given that where we have broken down the traditional wall between foreign intelligence gathering, particularly foreign intelligence, and criminal proceedings, to give the government broad authority to collect and share information, mostly secretly, I am concerned that we have also blurred the traditional line of protection for our privacy and freedoms.

While I agree that some lifting of the traditional restrictions in this area were justified for the government to better use the authorities it already had in many instances, I am also mindful that those restrictions were placed there for a very good reason. We have seen with "COINTELPRO," Watergate, the FBI spying on Dr. Martin Luther King, Jr., and with other incidents, what abuses can occur when we do not keep a tight enough reign on the government's use of extraordinary powers. We shouldn't have to experience those problems again to ensure that such abuses do not occur.

When we operate in the foreign intelligence arena, we have traditionally given fairly broad latitude for use of extraordinary investigative tools abroad, particularly involving non-U.S. persons. But when we turn those tools inward, we run a greater risk of including U.S. persons in some of the investigative sweeps that occur, unless we have sufficient barriers to prevent unwarranted extensions. Since much of the foreign intelligence side is secretive and ex parte for the government with no public oversight and review, we don't have the traditional notice, challenge and public scrutiny on the criminal side. We used to have the "wall" as a protection. With the wall gone, I believe w should focus on establishing sufficient notice, challenge and public reporting requirements to assure that foreign intelligence operations do not unduly creep into domestic activities of U.S. persons.

Some of our law enforcement officials seem to feel that the mere inclusion of information regarding uninvolved, innocent persons amounts to "no harm, no foul" if they are not arrested or subjected to having to challenge the incursion or other process—a sort of "what they don't know won't hurt them" philosophy. Yet, if overly broad information is collected, it can be spread all over town, greatly increasing the likelihood that your law enforcement, military or intelligence agency neighbor will know private things about you that you thought were private and known only by those to whom you knowingly gave the information. So, the problem with the "wall" being broken down isn't just improper acquisition and use of private information, but one of preventing people from having it the first place, other than those you gave it to with an expectation of privacy.

So Mr, Mr. Chairman, I look forward to the testimony of our witnesses on the extent to which our privacies and freedoms are being protected despite the dismantling of the "wall" through USA PATRIOT and other measures, and what safeguards are needed to prevent the creep of overly intrusive foreign intelligence operations and powers into the privacy of U.S. persons.

LETTER FROM WILLIAM E. MOSCHELLA, ASSISTANT ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE TO THE HONORABLE DIANNE FEINSTEIN

U.S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 26, 2005

The Honorable Dianne Feinstein
United States Senate
Washington, D.C. 20510

Dear Senator Feinstein:

In a letter dated April 4, 2005, the American Civil Liberties Union ("ACLU") responded to your March 25 request for information regarding alleged "abuses" of the USA PATRIOT Act. At your request, the Department of Justice has reviewed the ACLU's allegations. It appears that each matter cited by the ACLU either did not, in fact, involve the USA PATRIOT Act or was an entirely appropriate use of the Act. Thus, the ACLU is mistaken in its assertion in the letter that "the government has abused and misused the Patriot Act repeatedly" and in its press release, entitled "Patriot Act Abuses and Misuses Abound," that accompanied the letter and was released the night before the Attorney General was to appear before the Senate Judiciary Committee.

Our responses to the specific allegations are set forth below.

- **ALLEGATION #1: "Patriot Act [was used] to secretly search the home of Brandon Mayfield, a Muslim attorney whom the government wrongly suspected, accused and detained as a perpetrator of the Madrid train bombings."**

Mr. Mayfield's home was searched with the approval of a federal judge because the available information, including an erroneous finger-print match, gave investigators probable cause to believe that he was involved in the terrorist bombings in Madrid and not on account of any new authority created by the USA PATRIOT Act or any abuse of the Act.

The ACLU's allegation regarding Mr. Mayfield seems to be based in part on the mistaken idea that the search of Mr. Mayfield's home was conducted pursuant to Section 213 of the USA PATRIOT Act. That is not correct. The search was conducted pursuant to the Foreign Intelligence Surveillance Act ("FISA") under an authority that has existed in the FISA statute since 1995.

Because the search was conducted under a FISA court order, some of the USA PATRIOT Act provisions that amended FISA or relate to intelligence investigations may have been implicated or "used" in some sense of that word. For example, information-sharing provisions of the Act may have been used. And the time periods for the duration of FISA orders (Section 207) and the "significant purpose" test (Section 218) were implicated in the sense that those provisions apply to all FISA search applications. That does not in any way mean that these USA PATRIOT Act provisions were misused.

In addition, it would be wrong to suggest that Section 218 of the Act – and the change that provision made in the law – somehow made the search possible. The search could have been conducted just as readily under the standard in FISA in place prior to the USA PATRIOT Act. Under the previous standard in FISA, the government had to certify that "the purpose" of a search was to obtain foreign intelligence information, which is defined to include information necessary "to protect against . . . international terrorism." That standard had been interpreted to require that the "primary" purpose of the search was to obtain such information. In circumstances such as those the FBI encountered in the Mayfield investigation as they were known at the time, we believe that the government could have sought and obtained a FISA search warrant even under the old standard – certifying that the primary purpose of the search was to protect against international terrorism. Therefore, the ACLU is mistaken when it suggests that Section 218 "made the search possible."

Let us be clear: although Section 218 and its "significant purpose" test were not critical to obtaining a FISA search warrant with respect to Mayfield, Section 218 has been essential to the success of many national security investigations and the government's ability to fight terrorism effectively. See, e.g., U.S. Department of Justice, "The Use of Section 218 in Terrorism Investigations" (Apr. 11, 2005) (enclosed). Section 218 has been essential in facilitating information sharing between the intelligence community and the law-enforcement community, and we implore the Congress not to allow a wall to be reconstructed.

- **ALLEGATION #2: "Patriot Act [was used] to serve a National Security Letter (NSL) on an Internet Service Provider (ISP) so coercive under the terms prescribed by the statute that a federal court struck down the entire statute – as vastly expanded by the Patriot Act – used to obtain information about e-mail activity and web surfing for intelligence investigations."**

In Doe v. Ashcroft, 334 F. Supp. 2d 471 (S.D.N.Y. 2004), a federal district judge in New York struck down as unconstitutional Section 2709 of Title 18, a statute that authorizes the FBI to request "subscriber information and toll billing records information, or electronic communication transactional records" from a wire or communications service provider, including an Internet service provider (ISP), upon the written certification of a high-level FBI official that such information is

"relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities." 18 U.S.C. § 2709. Such a request is one of several varieties of so-called "national security letters" or "NSLs" authorized by law.

The USA PATRIOT Act did not create the authority contained in Section 2709, nor did the Act create NSLs generally. Rather, Section 2709 was enacted as part of the Electronic Communications Privacy Act of 1986. Although the USA PATRIOT Act amended Section 2709, the amendment was not central to the court's decision striking down the law. The ACLU's suggestion to the contrary is belied by its own attorney, Jameel Jaffer, who has stated in connection with this case: "The provisions that we challenged and that the court objected to were in the statute before the Patriot Act was passed . . . . We could have raised the same objections before the power was expanded." Shaun Waterman, Ashcroft: U.S. will appeal terror-law ruling, UPI, Sept. 30, 2004.

Nor is the ACLU accurate to the extent it implies – in stating that the "statute [is] . . . used to obtain information about e-mail activity and web surfing" – that Section 2709 can be used to obtain the content of electronic communications. It cannot. Section 2709 authorizes the FBI to request only "the name, address, length of service, and local and long distance toll billing records of a person or entity" for telephone service and the "name, address, and length of service" for electronic communications. 18 U.S.C. § 2709(b).

Finally, the ACLU promotes the mistaken impression that Section 2709 and the amendment made to it by the PATRIOT Act were designed, as the ACLU states in its letter, to investigate individuals who "posted a blog critical of the government" or "to obtain a list of people who have e-mail accounts with a given political organization." To the contrary: the USA PATRIOT Act amendments to Section 2709 included specific safeguards to protect the First Amendment rights of United States persons. Section 2709 authorizes the FBI to request the listed information if "relevant to an authorized investigation to protect against international terrorism or clandestine intelligence activities, provided that such an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States." (Emphasis added.)

The Department of Justice disagrees with key aspects of the district court's decision in Doe and has filed a notice of appeal with the U.S. Court of Appeals for the Second Circuit.

- **ALLEGATION #3: "Patriot Act [was used] to gag that ISP from disclosing this abuse to the public, and gag the ACLU itself, which represents the ISP, from disclosing this abuse to the public when the ACLU became aware of it, and from disclosing important circumstances relating to this abuse and other possible abuses of the gag, even to this very day."**

The ACLU is referring apparently here to the nondisclosure requirement contained in 18 U.S.C. § 2709 – the subject of the court's decision in Doe v. Ashcroft, discussed above. Again, the statute and its nondisclosure provision have existed since 1986 – long before the USA PATRIOT Act.

Such nondisclosure requirements are entirely appropriate under the circumstances. If information identifying the targets of international terrorism and espionage investigations were revealed, such disclosures would, as the U.S. Court of Appeals for the D.C. Circuit has recognized, "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." Center for National Security Studies v. U.S. Department of Justice, 331 F.3d 918, 928-29 (D.C. Cir. 2003). Indeed, the district court in Doe itself observed:

> [T]he Government's interest in protecting the integrity and efficacy of international terrorism and counterintelligence investigations is a compelling one. The Supreme Court has so acknowledged: "This Court has recognized the Government's 'compelling interest' in withholding national security information from unauthorized persons in the course of executive business." A suspected terrorist or foreign intelligence operative who is alerted that the Government is conducting an investigation may destroy evidence, create false leads, alert others, or otherwise take steps to avoid detection. More generally, such disclosures can reveal the Government's intelligence-gathering methods, from which foreign intelligence operatives or terrorists could learn better how to avoid detection.

Doe, 334 F. Supp. 2d at 513-14 (quoting Department of the Navy v. Egan, 484 U.S. 518, 527 (1988)).

- **ALLEGATION #4: "Patriot Act [was used] to charge, detain, and prosecute a Muslim student in Idaho, Sami al-Hussayen, for providing 'material support' to terrorists because he posted to an Internet website links to objectionable materials, even though such links were available on the websites of the government's own expert witness in the case and on the website of a major news outlet."**

Sami Al-Hussayen was charged in a fourteen-count indictment with three counts of providing or conspiring to provide material support to terrorists and eleven counts of making false statements to immigration authorities and visa fraud. Al-Hussayen consented to a detention order in his criminal case in the period leading up to trial because he was already subject to a detention hold by immigration authorities, who had requested his deportation for immigration fraud.

The ACLU is incorrect in claiming that the Department prosecuted Al-Hussayen "for engaging in First Amendment activities." The material-support-to-terrorism charges against Al-Hussayen were not based on an exercise of his right to free speech. On the contrary, the indictment charged that, among other things, Al-Hussayen had participated in illegal fundraising for HAMAS, a designated foreign-terrorist organization, as well as terrorist groups operating in Chechnya. Al-Hussayen did so by giving money and by using his computer skills to create and maintain websites, one of which included a fundraising appeal with a direct link to the official website for HAMAS. In addition, Al-Hussayen used his expertise in computer science to design web pages for the publication of several fatwas endorsing suicide attacks, and he himself published these fatwas on the Internet. One of these fatwas – published in May 2001 – actually suggested that an effective method for suicide attackers would be to fly an airplane into a building. Other evidence in the case included Al-Hussayen's own statements endorsing such violent jihad.

Prior to trial, Al-Hussayen moved to dismiss the material support charges on the grounds that his conduct was protected by the First Amendment. The trial judge denied that motion. Although Al-Hussayen was acquitted of the material support charges and some of the immigration charges, the jury was deadlocked on other immigration charges. Under these circumstances, the Government could have asked for a second trial on the remaining immigration charges. Instead, Al Hussayen was deported based on his immigration fraud, and the remaining charges were dropped.

- **ALLEGATION #5: "Patriot Act [was used] to deny, on account of his political beliefs, admission to the United States of a Swiss national, Tariq Ramadan, a prominent Muslim scholar who was to assume a teaching position at Notre Dame University."**

It is our understanding that the USA PATRIOT Act was not used to deny a visa to Tariq Ramadan. Indeed, a final determination regarding Ramadan's reapplication for a visa never occurred. The Ramadan case was handled by the Department of Homeland Security and the Department of State, and further questions regarding that case should be directed to those departments.

- **ALLEGATION #6: "Patriot Act [was used] to investigate and prosecute crimes that are not terrorism offenses, even though it cited terrorism prevention as the reason Congress should enact the law, and cites terrorism prevention as the reason why it cannot be changed."**

The ACLU highlights five matters that involved uses – not abuses – of the USA PATRIOT Act that did not involve terrorism investigations. Such uses were entirely proper and were not, as the ACLU contends, "misuses" of the Act. Many provisions in the Act simply updated the law to reflect recent technological developments and have been used, as Congress intended, not only in terrorism

cases, but also to combat other serious criminal conduct. Other provisions of the Act made general improvements to the law that apply to all types of criminal investigations. With respect to these provisions, the Department has used its authority appropriately to investigate and prosecute criminal offenses.

- **ALLEGATION A – "The FBI used the Patriot Act against Michael Galardi, the owner of two Las Vegas strip clubs, and several local officials that it believes accepted bribes from Galardi. Investigators reportedly delivered subpoenas under Section 314 of the Patriot Act – portrayed to Congress as necessary to undercut terrorist financing – to two Las Vegas stockbrokers ordering the release of detailed business records that prosecutors hope will reveal hidden proceeds that may be evidence of bribery."**

In the Las Vegas investigation, investigators requested financial information from various financial institutions pursuant to regulations promulgated under Section 314(a)[1] of the USA PATRIOT Act. Section 314 is entitled "Cooperative Efforts to Deter Money Laundering." Subpart (a) of Section 314 directs the Secretary of the Treasury to adopt regulations for the purpose of encouraging the sharing of information among financial institutions and federal law enforcement and regulatory agencies that pertain to individuals reasonably suspected of engaging in "terrorist acts or money laundering activities." (Emphasis added.) The plain text of the provision therefore makes it clear that the statute can and should be used in cases that do not involve terrorism.

The regulations promulgated pursuant to Section 314(a) were issued in September 2002, and are set forth in 31 C.F.R. §103.100. They establish a process by which federal law enforcement agencies may request account information from financial institutions through the Treasury Department's Financial Crimes Enforcement Network (FinCEN) if the requested information pertains to either terrorist activity or money laundering. In addition, by agreement between FinCEN and federal law enforcement agencies, this process may only be used to obtain information that is essential to a significant investigation.

It should be noted that a FinCEN request identifies only the existence of financial accounts. Account records are not available under Section 314(a) or the regulations promulgated under it. To obtain records, a law enforcement agency must comply with traditional legal process, such as a federal grand jury subpoena. Therefore, to the extent the ACLU suggests that the government used "subpoenas under 314 of the Patriot Act," it is incorrect.

---

[1]Section 314(a) originated in legislation to combat international money laundering, which was proposed by then Senate Banking Committee Chairman Sarbanes. *See* Section 104 of S. 1511, 1st Sess., 107th Cong.

In the Las Vegas case, the FBI followed the prescribed procedure to the letter. Michael Galardi ultimately pleaded guilty to a RICO violation in connection with his scheme to bribe local government officials.

- **ALLEGATION B – "The Justice Department used the Patriot Act against a lovesick 20-year-old woman from Orange County, CA, who planted threatening notes aboard a Hawaii-bound cruise ship on which she was traveling with her family. The woman, who said she made the threats to try to return home to her boyfriend, was sentenced to two years in federal prison because of a provision in the Patriot Act targeting threats of terrorism against mass transportation systems."**

The Department of Justice properly used Section 801 of the USA PATRIOT Act to prosecute Kelley Marie Ferguson, who pleaded guilty to one count of conveying false information about an attempt to cause death to the passengers and crew of a mass transportation system. Section 801, introduced by Senator Leahy, prohibits an individual from, among other things, conveying false information concerning attacks on mass transportation vehicles. In this case, Ms. Ferguson left two notes in cruise-ship restrooms stating that all American passengers and crew on the ship would be killed if the ship ported in the United States. Because of these notes, the ship was temporarily diverted off the shore of Honolulu with more than 1600 passengers and 700 crew members aboard. Approximately 120 federal, state, and local law enforcement officers of the Hawaii Joint Terrorism Task Force investigated the threat and searched the ship. After all of this took place, Ms. Ferguson left a third threatening note.

While it turned out that the terrorist threat in this case was a hoax, law enforcement authorities responded appropriately by taking seriously the threat to the lives of United States citizens. Ms. Ferguson was charged with and pleaded guilty to a violation of Section 801 – a violation that did involve a threat of terrorism in this case. Thus, this is not an example of a provision of the USA PATRIOT Act being used "outside the terrorism context," as the ACLU suggests.

In any event, even if Ms. Ferguson's threats had not been perceived to be and treated as threats of terrorism, it would have been entirely appropriate to prosecute her under Section 801. Nothing in the language or legislative history of that provision suggests that it is, or should be, confined to cases of terrorism. See 18 U.S.C. § 1993 (codifying Section 801). Indeed, when Senator Leahy described the provision on the floor of the Senate, he stated that the provision, as its title indicates, "targets acts of terrorism and other violence against mass transportation systems." Cong. Rec. S10997 (daily ed. Oct. 25, 2001) (emphasis added). Senator Leahy went on to provide an example of the "gap" in the law that Section 801 was intended to address; the example he provided – a deranged

passenger slitting the throat of a Greyhound bus driver, resulting in the death of six individuals – did not involve terrorism. Id.

- **ALLEGATION C – "In July 2002 Czech-born University of Connecticut graduate student, Tomas Foral, 26, became the first person to be charged under the USA Patriot Act for possession of a biological agent with no 'reasonably justified' purpose, a crime carrying a sentence of up to a decade in prison. His crime: discovering 35-year-old tissue samples from an anthrax-infected cow in a broken university cold-storage unit and moving them to a working freezer. Unfortunately for Foral, that freezer broke at the height of the anthrax scare and a tipster who found the samples phoned in Foral's name to the authorities. Foral finally agreed to community service and some restrictions on his activities."**

Section 817 of the USA PATRIOT Act prohibits individuals from possessing a biological agent, such as anthrax, "of a type or in a quantity that, under the circumstances, is not reasonably justified by a prophylactic, protective, bona fide research, or other peaceful purpose." 18 U.S.C. § 175. The use of this provision was entirely appropriate in the case of Tomas Foral. Foral was instructed by his professors to kill and then dispose of five anthrax samples. Instead, he knowingly kept two of the five samples of this extremely dangerous biological agent in his personal freezer in the school's laboratory even though he was not engaged in research involving anthrax.

Again, nothing in the language of Section 817 limits its use to cases of terrorism, and nothing in the legislative history suggests that Congress intended such a limitation. The provision was based on legislation that Senator Biden introduced in the 106th Congress – well before the events of September 11, 2001, and the anthrax attacks that followed shortly thereafter. Cong. Rec. S10997 (daily ed. Oct. 25, 2001) (statement of Sen. Leahy); Cong. Rec. S11049 (daily ed. Oct. 25, 2001)(statement of Sen. Biden). The provision was intended simply to make it illegal to possess anthrax or other dangerous biological agents absent a bona fide research or other peaceful purpose – a prohibition that is needed and appropriate even in circumstances not known to involve terrorism.

- **ALLEGATION D – "On March 23, 2005, the Department of Justice charged David Banach of Parsippany, New Jersey under the Patriot Act for shining a laser beam on an airplane using a hand held device. Banach, age 38, faces a statutory maximum of 20 years in prison and a $250,000 fine for the offense, even though the FBI admitted that the incident had no connection to terrorism. Banach claimed that he was using the device to look at stars with his seven year-old daughter from the deck of his home."**

David Banach was charged with two counts of making false statements, in violation of 18 U.S.C. § 1001, and one count of interfering with pilots of an aircraft with reckless disregard for the safety of human life, in violation of 18 U.S.C. § 1993(a)(5), a provision that was added to the criminal code in Section 801 of the USA PATRIOT Act. Again, the use of Section 801, which, among other things, prohibits individuals from interfering with someone operating a mass transportation vehicle, was entirely appropriate in this case. According to the indictment, Banach admitted shining a hand-held laser into the cockpit of a small passenger jet, temporarily blinding the pilots as they were approaching a New Jersey airport for landing. He also admitted lying to FBI agents repeatedly about this incident.

As noted above, nothing in the language or legislative history of Section 801 suggests that the provision is or should be limited to cases of terrorism.

- **ALLEGATION E – "Section 213, the 'sneak and peek' warrant provision of the Patriot Act, appears to have been used almost exclusively outside of terrorism investigations. Indeed, when the Department of Justice selectively reported some of the instances in which it has used sneak and peek warrants, its list consisted primarily of investigation of non-terrorism offenses, even though it cites counter-terrorism rationales as the reasons why reasonable limits should not be put on these searches."**

Delayed-notice search warrants have been used by law enforcement officers for decades in traditional criminal investigations, such as those involving drugs and child pornography. Such warrants were not created by the USA PATRIOT Act; the Act simply codified a common-law practice recognized by courts across the country and created a uniform nationwide standard for the issuance of those warrants. The Department has continued using delayed-notice search warrants in criminal investigations appropriately but sparingly since the passage of the Act. The Department estimates, for example, that fewer than one in 500 search warrants obtained nationwide are delayed-notice warrants. For further details regarding the Department's use of Section 213, we are enclosing a copy of a letter from Assistant Attorney General William Moschella to Chairman Specter dated April 4, 2005.

* * * *

As these facts show, the ACLU is simply incorrect in its claim that the "government has abused and misused the Patriot Act repeatedly." The Department of Justice takes seriously any accusation that the Department is "abusing or misusing" any provision of law – including the USA PATRIOT Act. It appears that in this case the accusations made by the ACLU are baseless. During the hearing, Attorney General Gonzales rightly stated:

"All of us have the same objective: ensuring the security of the American people while preserving our civil liberties. I therefore hope that we will consider reauthorization in a calm and thoughtful manner. Our dialogue should be based on facts, rather than exaggeration."

We appreciate this opportunity to present the facts and look forward to continuing to work with you to ensure the reauthorization of the USA PATRIOT Act. We sincerely believe that the tools it contains are essential to the government's ability to fight terrorism and serious criminal conduct.

Sincerely,

William E. Moschella

William E. Moschella
Assistant Attorney General

Enclosures

cc: Anthony Romero
Director, ACLU

The Honorable Arlen Specter
Chairman
Committee on the Judiciary

The Honorable Patrick J. Leahy
Ranking Minority Member
Committee on the Judiciary

LETTER FROM WILLIAM E. MOSCHELLA, ASSISTANT ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE TO THE HONORABLE ARLEN SPENCER

U. S. Department of Justice

Office of Legislative Affairs

Office of the Assistant Attorney General

Washington, D.C. 20530

April 4, 2005

The Honorable Arlen Specter
Chairman
Committee on the Judiciary
United States Senate
Washington, D.C. 20510

Dear Mr. Chairman:

We have indicated in some of our responses to questions for the record, including those recently submitted on April 1, 2005, that we would supplement our responses to some questions. This letter is intended to supplement previous information we have provided regarding the usage of section 213 of the USA PATRIOT Act ("the Act"), relating to delayed-notice search warrants. We believe the information contained herein completely answers all the Committee's questions submitted to date regarding section 213 and we look forward to working with you on this and other issues related to the reauthorization of the USA PATRIOT Act.

As you know, the Department of Justice believes very strongly that section 213 is an invaluable tool in the war on terror and our efforts to combat serious criminal conduct. In passing the USA PATRIOT Act, Congress recognized that delayed-notice search warrants are a vital aspect of the Department's strategy of prevention: detecting and incapacitating terrorists, drug dealers and other criminals before they can harm our nation. Codified at 18 U.S.C. § 3103a, section 213 of the Act created an explicit statutory authority for investigators and prosecutors to ask a court for permission to delay temporarily notice that a search warrant was executed. While not scheduled to sunset on December 31, 2005, section 213 has been the subject of criticism and various legislative proposals. For the following reasons, the Department does not believe any modifications to section 213 are required.

To begin with, delayed-notice search warrants have been used by law enforcement officers for decades. Such warrants were not created by the USA PATRIOT Act. Rather, the Act simply codified a common-law practice recognized by courts across the country.[1] Section 213 simply created a uniform nationwide standard for the issuance of those warrants, thus ensuring that delayed-notice search warrants are evaluated under the same criteria across the nation. Like any other search warrant, a delayed-notice search warrant is issued by a federal judge only upon a showing that there is probable cause to believe that the property to be searched for or seized constitutes evidence of a criminal offense. A delayed-notice warrant differs from an ordinary search warrant only in that the judge specifically authorizes the law enforcement officers executing the warrant to wait for a limited period of time before notifying the subject of the search that a search was executed.

[1] *See infra* note 4.

In addition, investigators and prosecutors seeking a judge's approval to delay notification must show that, if notification were made contemporaneous to the search, there is reasonable cause to believe one of the following might occur:[2]

1. notification would endanger the life or physical safety of an individual;
2. notification would cause flight from prosecution;
3. notification would result in destruction of, or tampering with, evidence;
4. notification would result in intimidation of potential witnesses; or
5. notification would cause serious jeopardy to an investigation or unduly delay a trial.

To be clear, it is only in these five tailored circumstances that the Department may request judicial approval to delay notification, and a federal judge must agree with the Department's evaluation before approving any delay.

Delayed-notice search warrants provide a crucial option to law enforcement. If immediate notification were required regardless of the circumstances, law enforcement officials would be too often forced into making a "Hobson's choice": delaying the urgent need to conduct a search and/or seizure *or* conducting the search and prematurely notifying the target of the existence of law enforcement interest in his or her illegal conduct and undermine the equally pressing need to keep the ongoing investigation confidential.

A prime example in which a delayed-notice search warrant was executed is Operation Candy Box. This operation was a complex multi-year, multi-country, multi-agency investigative effort by the Organized Crime Drug Enforcement Task Force, involving the illegal trafficking and distribution of both MDMA (also known as Ecstasy) and BC bud (a potent and expensive strain of marijuana). The delayed-notice search warrant used in the investigation was obtained on the grounds that notice would cause serious jeopardy to the investigation (*see* 18 U.S.C. § 2705(a)(2)(E)).

In 2004, investigators learned that an automobile loaded with a large quantity of Ecstasy would be crossing the U.S.-Canadian border en route to Florida. On March 5, 2004, after the suspect vehicle crossed into the United States near Buffalo, Drug Enforcement Administration (DEA) Special Agents followed the vehicle until the driver stopped at a restaurant. One agent then used a duplicate key to enter the vehicle and drive away while other agents spread broken glass in the parking space to create the impression that the vehicle had been stolen. The ruse worked, and the drug traffickers were not tipped off that the DEA had seized their drugs. A subsequent search of the vehicle revealed a hidden compartment containing 30,000 MDMA tablets and ten pounds of BC bud. Operation Candy Box was able to continue because agents were able to delay notification of the search for more than three weeks.

On March 31, 2004, in a two-nation crackdown the Department notified the owner of the car of the seizure and likewise arrested more than 130 individuals. Ultimately, Operation Candy Box resulted in approximately 212 arrests and the seizure of $8,995,811 in U.S. currency, 1,546 pounds of MDMA powder, 409,300 MDMA tablets, 1,976 pounds of marijuana, 6.5 pounds of

[2] *See* 18 U.S.C. § 2705(a)(2).

methamphetamine, jewelry valued at $174,000, 38 vehicles, and 62 weapons. By any measure, Operation Candy Box seriously disrupted the Ecstasy market in the United States and made MDMA pills less potent, more expensive and harder to find. There has been a sustained nationwide eight percent per pill price increase since the culmination of Operation Candy Box; a permanent decrease of average purity per pill to the lowest levels since 1996; and currency seizures have denied traffickers access to critical resources - preventing the distribution of between 17 and 34 million additional Ecstasy pills to our nation's children.

Had Operation Candy Box agents, however, been required to provide immediate notification of the search of the car and seizure of the drugs, they would have prematurely revealed the existence of and thus seriously jeopardized the ultimate success of this massive long-term investigation. The dilemma faced by investigators in the absence of delayed notification is even more acute in terrorism investigations where the slightest indication of governmental interest can lead a loosely connected cell to dissolve. Fortunately though, because delayed-notice search warrants are available, investigators do not have to choose between pursuing terrorists or criminals and protecting the public – we can do both.

It is important to stress that in *all* circumstances the subject of a criminal search warrant is informed of the search. It is simply false to suggest, as some have, that delayed-notice search warrants allow the government to search an individual's "houses, papers, and effects" without notifying them of the search. In every case where the government executes a criminal search warrant, including those issued pursuant to section 213, the subject of the search is told of the search. With respect to delayed-notice search warrants, such notice is simply delayed for a reasonable period of time – a time period defined by a federal judge.

Delayed-notice search warrants are constitutional and do not violate the Fourth Amendment. The U.S. Supreme Court expressly held in *Dalia v. United States* that the Fourth Amendment does not require law enforcement to give immediate notice of the execution of a search warrant.[3] Since *Dalia*, three federal courts of appeals have considered the constitutionality of delayed-notice search warrants, and all three have upheld their constitutionality.[4] To our knowledge, no court has ever held otherwise. In short, long before the enactment of the USA PATRIOT Act, it was clear that delayed notification was appropriate in certain circumstances; that remains true today. The USA PATRIOT Act simply resolved the mix of inconsistent rules, practices and court decisions varying from circuit to circuit. Therefore, section 213 had the beneficial impact of mandating uniform and equitable application of the authority across the nation.

The Committee has requested detailed information regarding how often section 213 has been used. Let us assure you that the use of a delayed-notice search warrant is the exception, not the rule. Law enforcement agents and investigators provide immediate notice of a search warrant's execution in the vast majority of cases. According to Administrative Office of the U.S. Courts (AOUSC), during a 12-month period ending September 30, 2003, U.S. District Courts handled 32,539 search warrants. By contrast, in one 14-month period – between April 2003 and July 2004 –

[3] *See Dalia v. United States*, 441 U.S. 238 (1979); *see also Katz v. United States*, 389 U.S. 347 (1967).

[4] *See United States v. Freitas*, 800 F.2d 1451 (9th Cir. 1986); *United States v. Villegas*, 899 F.2d 1324 (2d Cir. 1990); *United States v. Simons*, 206 F.3d 392 (4th Cir. 2000).

the Department used the section 213 authority only 61 times according to a Department survey. Even when compared to the AOUSC data for a shorter period of time, the 61 uses of section 213 still only accounts for less than 0.2% of the total search warrants handled by the courts. Indeed, since the USA PATRIOT Act was enacted on October 26, 2001, through January 31, 2005 – a period of more than three years – the Department has utilized a delayed-notice search warrant only 155 times.[5]

We have been working with United States Attorneys across the country to refine our data and develop a more complete picture of the usage of the section 213 authority. We have manually surveyed each of the 94 United States Attorneys' Offices for this information which, we understand, is not in a database. We are pleased to report our additional findings below.

In September 2003, the Department made public the fact that we had exercised the authority contained in section 213 to delay notification 47 times between October 2001, and April 1, 2003.[6] Our most recent survey, which covers the time frame between April 1, 2003, and January 31, 2005, indicates we have delayed notification of searches in an additional 108 instances. Since April 1, 2003, no request for a delayed-notice search warrant has been denied. It is possible to misconstrue this information as evidence that courts are merely functioning as a "rubber stamp" for the Department's requests. In reality, however, it is an indication that the Department takes the authority codified by the USA PATRIOT Act very seriously. We judiciously seek court approval only in those rare circumstances – those that fit the narrowly tailored statute – when it is absolutely necessary and justified. As explained above, the Department estimates that it seeks to delay notice of fewer than 1 in 500 search warrants issued nationwide. To further buttress this point, the 108 instances of section 213 usage between April 1, 2003, and January 31, 2005, occurred in 40 different offices. And of those 40 offices, 17 used section 213 only once. Looking at it from another perspective over a longer time frame, 48 U.S. Attorneys' Offices – or slightly more than-half – have never sought court permission to execute a delayed-notice search warrant in their districts since passage of the USA PATRIOT Act.

To provide further detail for your consideration, of the 108 times authority to delay notice was sought between April 1, 2003, and January 31, 2005, in 92 instances "seriously jeopardizing an investigation" (18 U.S.C. § 2705(a)(2)(E)) was relied upon as a justification for the application. And in at least 28 instances, jeopardizing the investigation was the sole ground for seeking court approval to delay notification, including Operation Candy Box described above. It is important to note that under S.1709, the "SAFE Act," which was introduced in the 108th Congress, this ground for delaying notice would be eliminated. Other grounds for seeking delayed-notice search warrants were relied on as follows: 18 U.S.C. § 2705(a)(2)(A) (danger to life or physical safety of an individual) was cited 23 times; 18 U.S.C. § 2705(a)(2)(B) (flight from prosecution) was cited 45 times; 18 U.S.C. § 2705(a)(2)(C) (destruction or tampering with evidence) was cited 61 times; and 18 U.S.C. § 2705(a)(2)(D) (intimidation of potential witnesses) was cited 20 times. As is probably

[5] The data reflected in this letter were gathered from paper surveys completed by each U.S. Attorney's Office. While we believe the survey method to be accurate, we cannot completely rule out the possibility of reporting errors.

[6] *See* Letter from Jamie E. Brown, Acting Assistant Attorney General, Office of Legislative Affairs, U.S. Department of Justice to F. James Sensenbrenner, Chairman, House of Representatives Committee on the Judiciary (May 13, 2003).

clear, in numerous applications, U.S. Attorneys' Offices cited more than one circumstance as justification for seeking court approval. The bulk of uses have occurred in drug cases; but section 213 has also been used in many cases including terrorism, identity fraud, alien smuggling, explosives and firearms violations, and the sale of protected wildlife.

Members of the Senate Judiciary Committee have also been concerned about delayed notification of seizures and have requested more detailed explanation of the number of times seizures have been made pursuant to delayed-notice warrants. The Department is pleased to provide the following information.

Seizures can be made only after receiving approval of a federal judge that the government has probable cause to believe the property or material to be seized constitutes evidence of a criminal offense and that there is reasonable necessity for the seizure. (*See* 18 U.S.C. § 3103a(b)(2)). According to the same survey of all U.S. Attorneys' Offices, the Department has asked a court to find reasonable necessity for a seizure in connection with delayed-notice searches 45 times between April 1, 2003, and January 31, 2005. In each instance in which we have sought authorization from a court during this same time frame, the court has granted the request. Therefore, from the time of the passage of the USA PATRIOT Act through January 31, 2005, the Department has exercised this authority 59 times. We previously, in May 2003, advised Congress that we had made 15 requests for seizures, one of which was denied.[7] In total, since the passage of the USA PATRIOT Act, the Department has therefore requested court approval to make a seizure and delay notification 60 times. Most commonly, these requests related to the seizure of illegal drugs. Such seizures were deemed necessary to prevent these drugs from being distributed because they are inherently dangerous to members of the community. Other seizures have been authorized pursuant to delayed-notice search warrants so that explosive material and the operability of gun components could be tested, other relevant evidence could be copied so that it would not be lost if destroyed, and a GPS tracking device could be placed on a vehicle. In short, the Department has sought seizure authority only when reasonably necessary.

The length of the delay in providing notice of the execution of a warrant has also received significant attention from Members of Congress. The range of delay must be decided on a case-by-case basis and is always dictated by the approving judge or magistrate. According to the survey of the 94 U.S. Attorneys' Offices, between April 1, 2003 and January 31, 2005, the shortest period of time for which the government has requested delayed-notice of a search warrant was 7 days. The longest such specific period was 180 days; the longest unspecified period was until "further order of the court" or until the end of the investigation. An unspecified period of time for delay was granted for six warrants (four of these were related to the same case). While no court has ever rejected the government's request for a delay, in a few cases courts have granted a shorter time frame than the period originally requested. For example, in one case, the U.S. Attorney for the District of Arizona sought a delay of 30 days, and the court authorized a shorter delay of 25 days.

Of the 40 U.S. Attorneys' Offices that exercised the authority to seek delayed-notice search warrants between April 1, 2003, and January 31, 2005, just over half (22) of the offices sought

[7] *See* Letter from Jamie E. Brown, Acting Assistant Attorney General, Office of Legislative Affairs, U.S. Department of Justice to F. James Sensenbrenner, Chairman, House of Representatives Committee on the Judiciary (May 13, 2003).

extensions of delays. Those 22 offices together made approximately 98 appearances to seek additional extensions. In certain cases, it was necessary for the Offices to return to court on multiple occasions with respect to the same warrant. One case bears note. The U.S. Attorney in the Southern District of Illinois sought and received approval to delay notification based on the fifth category of adverse result – that immediate notification would seriously jeopardize the investigation. The length of the delay granted by the court was 7 days. However, the notification could not be made within 7 days and the office was required to seek 31 extensions. So, each week for almost eight straight months, the case agent was made to swear out an affidavit, and the Assistant United States Attorney (AUSA) then had to reappear before the judge or magistrate to renew the delay of notice.

In the vast majority of instances reported by the U.S. Attorneys' Offices, original delays were sought for between 30 to 90 days. It is not surprising that our U.S. Attorneys' Offices are requesting up to 90-day delays. Ninety days is the statutory allowance under Title III for notification of interception of wire or electronic communications (*see* 18 U.S.C. 2518(8)(d)). In only one instance did a U.S. Attorney's Office seek a delay of a specified period of time longer than 90 days (180 days), and the court granted this request. In another instance, an office sought a 90-day delay period, and the court granted 180 days. In seven instances, the Department sought delays that would last until the end of the investigation. In only once instance was such a request modified. In that matter, the court originally granted a 30-day delay. However, when notification could not be made within 30 days, the U.S. Attorney's Office returned to the judge for an extension, and the judge granted an extension through the end of the investigation, for a total of 406 days. This is, according to our survey, the longest total delay a court authorized. However, most extensions were sought and granted for the same period as the original delay requested.

In one case, a court denied a U.S. Attorney's Office's request for an extension of the delay in providing notice. This matter involved three delayed-notice search warrants -- all-stemming from the same investigation. The original period of delay sought and granted was for 30 days on all three warrants. The Office then sought 30-day extensions on all three warrants out of concern that the multiple targets of the investigation might flee to a foreign country if notified. The court denied our request. The judge in the matter reasoned that the need to delay notification warranted only a 30-day stay of service, particularly in light of the fact that one of the targets of the investigation was, by this time, in federal custody in California on an unrelated matter. At some point after notification was made, however, the other targets fled to Mexico.

In sum, both before enactment of section 213 and after, immediate notice that a search warrant had been executed has been standard procedure. Delayed-notice search warrants have been used for decades by law enforcement and, as demonstrated by the numbers provided above, delayed-notice warrants are used infrequently and scrupulously – only in appropriate situations where immediate notice likely would harm individuals or compromise investigations, and even then only with a judge's express approval. The investigators and prosecutors on the front lines of fighting crime and terrorism should not be forced to choose between preventing immediate harm – such as a terrorist attack or an influx of illegal drugs – and completing a sensitive investigation that might shut down an entire terror cell or drug trafficking operation. Thanks to the long-standing availability of delayed-notice warrants in these circumstances, they do not have to make that

choice. Section 213 enables us to better protect the public from terrorists and criminals while preserving Americans constitutional rights.

As you may be aware, the Department published a detailed report last year that includes numerous additional examples of how delaying notification of search warrants in certain circumstances resulted in beneficial results. We have enclosed a copy for your convenience.

If we can be of further assistance regarding this or any other matter, please do not hesitate to contact this office.

Sincerely,

William E. Moschella

William E. Moschella
Assistant Attorney General

Enclosure

cc: The Honorable Patrick J. Leahy
Ranking Minority Member

The Use of Section 218 in Terrorism Investigations

Background: Before the passage of the USA PATRIOT Act, 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 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 such coordination, 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.

In recent testimony before the Senate Judiciary Committee, Patrick Fitzgerald, U.S. Attorney for the Northern District of Illinois, recounted from personal experience how this "wall" between law enforcement and intelligence personnel operated in practice:

> 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."

The USA PATRIOT Act brought down this "wall" separating intelligence officers from law enforcement agents. It not only erased the perceived statutory impediment to more robust information sharing between intelligence and law enforcement personnel, but 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 of the USA PATRIOT Act eliminated the "primary purpose" requirement. Under section 218, the government may 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, and thereby allowing for increased coordination and sharing of information between intelligence and law enforcement personnel. Section 504 buttressed section 218 by specifically amending FISA to allow intelligence officials conducting FISA surveillance or searches to "consult" with federal law enforcement officials to "coordinate" efforts to investigate or protect against international terrorism, espionage, and other foreign threats to national security, and to clarify that such coordination "shall not" preclude the certification of a "significant" foreign intelligence purpose or the issuance of an authorization order by the Foreign Intelligence Surveillance Court.

The Department has moved aggressively to implement sections 218 and 504 of the USA PATRIOT Act 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 officers, 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.

These efforts to increase coordination and information sharing between intelligence and law enforcement officers, which were made possible by the USA PATRIOT Act, have yielded extraordinary dividends by enabling the Department to open numerous criminal investigations, disrupt terrorist plots, bring numerous criminal charges, and convict numerous individuals in terrorism cases.

Examples:

1. **PORTLAND SEVEN:** 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 had been 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 suspected 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 domestic 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 sections 218 and 504 of the USA PATRIOT Act, 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. Charges against the seventh defendant were dismissed after he was killed in Pakistan by Pakistani troops on October 3, 2003. Without sections 218 and 504 of the USA PATRIOT Act, however, this case likely would have been referred to as the "Portland One" rather than the "Portland Seven."

2. **SAMI AL-ARIAN:** The Department shared information pursuant to sections 218 and 504 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 states 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, sections 218 and 504 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 in enabling prosecutors to build their case and pursue the proper charges. The trial in this case is scheduled to begin May 16, 2005.

3. **VIRGNIA JIHAD:** Prosecutors and investigators also used information shared pursuant to sections 218 and 504 of the USA PATRIOT Act in investigating the defendants in the socalled "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 nine 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 primarily operates in Pakistan and Kashmir and has ties to the al Qaeda terrorist network. As the result of an investigation that included the use of information obtained through FISA, prosecutors on June 25, 2003, indicted eleven individuals in a 41-count indictment. Subsequently, four of these defendants, Yong Ki Kwon, Mohammed Aatique, Donald Thomas Surratt, and Khwaja Mahmood Hasan, pled guilty and agreed to cooperate. On September 25, 2003, a superseding indictment was filed charging the remaining seven defendants with the conspiracy, conspiracy to levy war against the United States, conspiracy to provide material support to al Qaeda, conspiracy to contribute services to the Taliban, conspiracy to contribute material support to Lashkar-e-Taiba, supplying services to the Taliban, commencing an expedition against a friendly nation, conspiracy to possess and use a firearm in connection with a crime of violence, receipt of firearm or ammunition with cause to believe a felony will be committed therewith, false official statements, and using a firearm in connection with a crime of violence. The first phase of the case has been completed with all of the defendants convicted.

4. **YEMENI SHEIKH:** The information sharing between intelligence and law enforcement personnel made possible by sections 218 and 504 of the USA PATRIOT Act 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 had 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 be used to support HAMAS, al Qaeda, and any other mujahideen, and "swore to Allah" that they would keep their dealings secret. Al-Moayad and Zayed were extradited to the United States from Germany in November 2003 and were convicted on March 10, 2005. Al-Moayad and Zayed face up to 60 and 30 years in jail respectively.

5. **ARNAOUT CASE:** The Department used sections 218 and 504 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 obtain charitable donations fraudulently 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.

6. **DRUGS FOR STINGER MISSILES:** The broader information sharing and coordination made possible by sections 218 and 504 of the USA PATRIOT Act assisted the prosecution in San Diego of several persons involved in an al Qaeda drugs-for-weapons plot, which culminated in several guilty pleas. Two defendants 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. The lead defendant in the case is currently awaiting trial.

7. **IRAQI SPY:** Sections 218 and 504 were 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 officers conducting surveillance of Dumeisi pursuant to FISA coordinated and shared information with law enforcement agents and prosecutors investigating Dumeisi for possible violations of criminal law. Because of this coordination, law enforcement agents and prosecutors learned from intelligence officers 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 Dumeisi's trial.

SUBMISSION BY PETER SWIRE ENTITLED "THE SYSTEM OF FOREIGN INTELLIGENCE SURVEILLANCE LAW"

The System of Foreign Intelligence Surveillance Law

Peter P. Swire*

TABLE OF CONTENTS

 The article was published as 72 Geo. Wash. L. Rev. 1306 (2004), with the same content but different page numbers.

Professor, Moritz College of Law of the Ohio State University and John Glenn Scholar in Public Policy Research. I thank the people with experience in foreign intelligence law who helped me in this project, many of whom prefer not to be identified. Stewart Baker, Jerry Berman, Jim Dempsey, John Podesta, and Ruth Wedgwood are among those who have helped teach me this topic. I am grateful for comments on earlier drafts from Susan Freiwald, Beryl Howell, Kim Lane Scheppele, Peter Raven Hansen, Coleen Rowley, Stephen Saltzburg, Michael Vatis, and those who attended my presentations at the Association of American Law Schools annual conference, the George Washington University Law School, the Moritz College of Law, and the University of Toledo School of Law. My thanks to Najah Allen, Katy Delaney, Heather Hostetler, and Scott Zimmerman for research assistance, and to the Moritz College of Law and the John Glenn Institute for research support.

The Foreign Intelligence Surveillance Act ("FISA")[1] was enacted in 1978 to solve a long-simmering problem. Since Franklin Roosevelt, Presidents had asserted their "inherent authority" to authorize wiretaps and other surveillance for national security purposes.[2] Over time, the Supreme Court made clear that the Fourth Amendment required a neutral magistrate to issue a prior warrant for ordinary wiretaps, used for domestic law enforcement purposes.[3] Yet the Supreme Court reserved a realm of "foreign intelligence" wiretaps where the court had not yet stated what procedures were required by the Fourth Amendment.

In the face of this uncertainty, both supporters and critics of surveillance had an incentive to compromise. Supporters of surveillance could gain by a statutory system that expressly authorized foreign intelligence wiretaps, lending the weight of Congressional approval to surveillance that did not meet all the requirements of ordinary Fourth Amendment searches. Critics of surveillance could institutionalize a series of checks and balances on the previously unfettered discretion of the President and the Attorney General to conduct surveillance in the name of national security.

---

[1] The Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified at 50 U.S.C. §§ 1801-1811(2000).
[2] *See infra* text accompanying note 36.
[3] Katz v. United States, 389 U.S. 347 (1967); *see infra* text accompanying notes 21-24.

The basic structure of FISA remained unchanged from 1978 until the attacks of September 11, 2001. In the wake of those attacks, Congress quickly enacted the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the "USA-PATRIOT" or "Patriot" Act).[4] The Patriot Act made significant changes to FISA, notably by tearing down the "wall" that had largely separated foreign intelligence activities from the usual prosecution of domestic crimes.[5] The Patriot Act also greatly expanded the statutory authority to require libraries and other organizations to disclose records and tangible objects to federal investigators, while making it a criminal act to report that the disclosure had been made.[6] In related changes, Attorney General Ashcroft loosened internal Justice Department Guidelines that had constrained investigators' discretion on how to investigate, in the name of domestic security, activities protected by the First Amendment.[7] Because the Patriot Act was passed so quickly, with only minimal hearings and debate in Congress, the FISA changes and other provisions of the Act are scheduled to sunset on December 31, 2005.[8]

This period before the sunset will be the occasion for the most important debate on the system of foreign intelligence surveillance law since passage of the 1978 Act. In 2003, for the first time, the number of surveillance orders issued under FISA exceeded the number of law enforcement wiretaps issued nationwide.[9] This article, drawing on

---

[4] Uniting and Strengthening America by Providing Appropriate Tools required to Intercept and Obstruct Terrorms Act (USA PATRIOT Act) of 2001, P.L. No. 107-56, 115 Stat. 272 .
[5] *See infra* Part IV.A.
[6] *See infra* text accompanying notes 174-76, 310-322.
[7] *See infra* text accompanying notes 198-200.
[8] USA PATRIOT Act, § 224, 115 Stat. at 295..
[9] In 2003, 1724 surveillance orders were issued under FISA. Letter from William E. Moschella, U.S. Department of Justice, Office of Legislative Affairs to L. Ralph Mecham, Director, Administrative Office of the United States Courts, Apr. 30, 2004, *available at* http://www.epic.org/privacy/terrorism/fisa/2003_report.pdf. For 2003, 1,442 non-FISA wiretap orders

both my academic and government experiences,[10] seeks to create a more informed basis for assessing how to amend FISA and otherwise improve the ability of our foreign intelligence law to meet the twin goals of national security, on the one hand, and protection of the rule of law and civil liberties, on the other.

Part I of the article discusses national security surveillance before 1978, tracing both the development of the Fourth Amendment for law enforcement wiretaps and the distinct legal authorities that recognized broader authority for the President in the areas of national security and foreign affairs. Part I also includes an examination of the history of abuses of national security surveillance in the period before 1978. These abuses, many of which were revealed in the course of the Watergate crisis, were a crucial education to Congress and the American people about the ways in which domestic security surveillance was often executed contrary to existing laws and in ways that posed serious threats to the democratic process.

Part II explains the 1978 compromises embodied in FISA and contrasts its special rules with the stricter rules that apply to wiretaps used in the ordinary criminal context. Part III examines the history of foreign intelligence surveillance law from 1978 until the attacks of September 11, 2001. Although the legal structure changed only incrementally during this time, the period was marked by a large increase in the number of FISA

---

were issued under law enforcement authorities. 2003 Wiretap Report 3, *available at* http://www.uscourts.gov/wiretap03/contents.html.

[10] During my service as Chief Counselor for Privacy in the U.S. Office of Management and Budget, I was asked by Chief of Staff John Podesta to chair a fifteen-agency White House Working Group on how to update wiretap and other electronic surveillance law for the Internet age. That process resulted in proposed legislation that was introduced in 2000 as S. 3083, 106th Cong. (2000). *See* Press Release, The White House, Assuring Security and Trust in Cyberspace (July 17, 2000), http://www.privacy2000.org/presidential/POTUS_7-17-00_fact_sheet-on_assuring_security_and_trust_in_cyberspace.htm (announcing legislation proposed by Chief of Staff John D. Podesta in remarks at the National Press Club). For the text of Podesta's remarks, see Press Release, The White House, Remarks by the President's Chief of Staff John D. Podesta on Electronic

surveillance orders. This history suggests that FISA had met at least some of the goals of its drafters, regularizing and facilitating the surveillance power subject to institutional checks from all three branches of government.[11]

Part IV charts the recent history of FISA. The expansion of FISA authority in the Patriot Act was limited for a time by the first publicly-released decision of the Foreign Intelligence Surveillance Court, which was responding, in part, to over seventy-five instances of misleading applications for FISA surveillance.[12] That decision, in turn, was reversed in the first-ever decision of the Foreign Intelligence Surveillance Court of Review, which essentially upheld the expanded Patriot Act powers against statutory and constitutional challenge.[13]

Part V examines the system of foreign intelligence surveillance law. Because the usual Fourth Amendment and due process protections do not apply in individual cases, it becomes more important to have system-wide checks and balances against recurrence of the abuses of earlier periods. The article explores the claim that "everything has changed" in the wake of September 11.[14] That claim, if true, could justify expanded surveillance powers. There are significant counter-arguments, however, that suggest that the threats today are more similar than often recognized to the threats from earlier periods, undercutting the case for expanded powers.

Part VI then explores proposals for reform. Due to the classified nature of the foreign intelligence process there are limits to the ability of outside commentators to

---

Privacy to National Press Club (July 18, 2000), http://www.privacy2000.org/presidential/POTUS_7-17-00_remarks_by_podesta_on_electronic_privacy.htm.

[11] *See infra* text accompanying notes 103-24..

[12] In re All matters to Foreign Intelligence Surveillance, 218 F. Supp. 2d 611, 615 (Foreign Intel. Surv. 2002) [Hereinafter "FISC Decision"].

[13] *See In re* Sealed Case, 310 F.3d 717 (Foreign Int. Surv. Ct. Rev. 2002) [hereinafter *FISCR Decision*].

[14] *See infra* Part V.D.

assess details of the workings of the system of foreign intelligence surveillance law. Nonetheless, the changes since September 11 have been in the direction of eliminating a number of the important checks and balances that were created when Congress last had full discussions of foreign intelligence surveillance law.[15] The proposals for reform here can be considered as either concrete proposals or as a guide to the questions Congress should ask in its oversight of the system as the sunset approaches. In either event, more thorough vetting of institutional alternatives is necessary in wake of the very large changes to this area of law since the fall of 2001.

I. National Security Surveillance Before 1978

The legal standard for "national security" or "foreign intelligence" surveillance results from the interaction of two conflicting positions. The first position is that wiretaps taking place on American soil should be treated like wiretaps used for law enforcement purposes, with the same Fourth Amendment protections. The second position is that the President has special authority over national security issues, and therefore can authorize wiretaps with fewer or no Fourth Amendment limits. This Part of the article examines the legal basis for the two positions and then examines the sobering history of problems arising from domestic surveillance before 1978.

A. The Fourth Amendment and Law Enforcement Wiretaps

The law for domestic wiretaps, used for law enforcement purposes, has evolved considerably in the past century. In the 1928 case *Olmstead v. United States*[16] the Supreme Court found no Fourth Amendment limits on a wiretap unless it was

[15] *See id.*
[16] Olmstead v. United States, 277 U.S. 438, 464-66 (1928).

accompanied by physical trespass on a suspect's property.[17] Justice Brandeis famously dissented in *Olmstead,* saying that the Framers "conferred, as against the Government, the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."[18] Congress responded to the decision by passing the Communications Act of 1934.[19] Although that statute provided federal standards for wiretaps, state officials could wiretap subject only to the often-weak standards and enforcement of state laws.[20] Meanwhile, as discussed below, many federal wiretaps were placed by agents who failed to comply with the Communications Act.

The law for domestic wiretaps changed decisively in the 1960s. In 1967, in *Katz v. United States*,[21] the Supreme Court held that full Fourth Amendment protections would apply to electronic surveillance of private telephone conversations.[22] Later court decisions adopted the "reasonable expectation of privacy" test described in Justice Harlan's concurrence in *Katz* as the doctrinal test for when a probable cause warrant would be required under the Fourth Amendment.[23] The Supreme Court specifically

---

[17] *See id.* at 464-66.
[18] *Id.* at 478 (Brandeis, J., dissenting).
[19] For the history, see Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 630 (2003).
[20] For a detailed study of the historical weaknesses of protections at the state level, see SAMUEL DASH ET AL., THE EAVESDROPPERS (De Capo Press 1971) (1959); *see also* Charles H. Kennedy & Peter P. Swire, *State Wiretaps and Electronic Surveillance After September 11*, 54 HASTINGS L.J. 971, 977 (2003) (analyzing the history and current practice of state wiretap laws); *Id.* at app. A (fifty-state survey of state laws on wiretaps, stored records, and pen registers and trap and trace orders); *Id.* at app. B (survey of state wiretap law changes in the first nine months after the events of September 11).
[21] Katz v. United States, 389 U.S. 347 (1967).
[22] *Id.* at 353.
[23] The "reasonable expectation of privacy" test was announced by Justice Harlan in *Katz*, *Id.* at 361 ("My understanding of the rule that has emerged from prior decisions is that there is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"). This doctrinal test has been adopted, for instance, in California. v. Ciraolo, 476 U.S. 207, 211 (1986) and Kyllo v. United States, 533 U.S. 27, 33 (2001).

Professor Orin Kerr has recently argued that the federal courts have only rarely departed from traditional, property-based understandings of what is protected by the Fourth Amendment, and thus have used the "reasonable expectation of privacy test" much less than most observers have realized. *See The Fourth Amendment in New Technologies: Constitutional Myths and the Case for Restraint*, 102 MICH. L.

reserved the issue of whether similar warrants were required for wiretaps done for national security purposes.[24]

Also in 1967, the Supreme Court applied the Fourth Amendment to wiretaps performed by state officials in *Berger v. New York*.[25] In doing so, the Supreme Court gave detailed guidance to legislatures about what sort of protections were appropriate for wiretaps for law enforcement purposes.[26] For purposes of this article, it is important to note two required safeguards that have not necessarily applied to national security wiretaps: (1) judicial supervision of wiretaps; and (2) notice to the subject of the wiretap after the wiretap has expired.[27]

Congress responded the next year in Title III of that year's crime bill.[28] The basic rules for these "Title III" wiretaps were quite strict, with multiple requirements that do not apply to the usual probable cause warrant for a physical search. The Title III rules generally apply today to law enforcement wiretaps in the United States, as discussed further below.

The Electronic Communications Privacy Act of 1986 ("ECPA") was the next significant legal change to the regime for domestic electronic surveillance.[29] Whereas Title III applied to "wire" and "oral" communications, i.e., to phone wiretaps and bugs, ECPA extended many of the same protections to e-mail and other "electronic"

REV. 799 (2004). For my response to Professor Kerr, see Peter P. Swire, Katz *is Dead. Long Live* Katz, 102 MICH. L. REV.904 (2004).

[24] *Katz*, 389 U.S. at 358 n. 23.

[25] Berger v. New York, 388 U.S. 41, 54-64 (1967).

[26] *See id.*

[27] *See infra* text accompanying notes 108-12.

[28] Omnibus Crime Control and Safe Streets Act of 1969, Pub. L. No. 90-351, 82 Stat. 197 (1968) (codified at 18 U.S.C. § § 2510-2521 (2000)).

[29] Electronic Communications Privacy Act of 1986, Pub. L. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

communications.[30] The Title III and ECPA rules then remained largely unchanged until the Patriot Act in 2001, when the privacy protections for domestic wiretaps were loosened in a number of respects.[31] Notwithstanding these recent changes, the essential structure of Title III and ECPA remains in effect today, including the requirement of judicial supervision of wiretaps, the need to give notice to the object of surveillance once the wiretap is completed, and the obligation to minimize the amount of surveillance in order to prevent intrusions that are outside of the law enforcement investigation.

B. The Law and Logic of National Security Wiretaps

This history of applying the Fourth Amendment and the rule of law to wiretaps is accompanied by a second history, that of using wiretaps and other surveillance tools to protect the national security. Consider the Cold War example of an employee of the Soviet Embassy. What should the standards have been for wiretaps of that employee, who might also be an agent of the KGB? A Title III wiretap would often be impossible

[30] Electronic communications lack three of the protections that apply to wire and oral communications: the requirement of high-level Department of Justice approval before conducting the surveillance, 18 U.S.C. § 2516(1); restriction to a list of serious offenses, *Id.*; and, most significantly, no application of the relatively strict rules for suppressing evidence obtained in violation of the applicable rules. § 2515. In 2000, as part of the process in which I was involved, the Clinton Administration proposed applying these three protections to electronic communications. *See supra* note 10 This proposal has not been enacted.

[31] *See* Peter P. Swire, *Administration Wiretap Proposal Hits the Right Issues But Goes Too Far*, Brookings Terrorism Project Website, *available at* http://www.peterswire.net (Oct. 3, 2001). Professor Kerr has claimed that the Patriot Act actually increased privacy protections in the area of domestic electronic surveillance. Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 608 (2003). I have discussed these issues at length with Professor Kerr, and he moderated his claims substantially from the early working paper to final publication. In essence, Professor Kerr finds an increase in privacy protection where the USA Patriot Act codified the permissibility of surveillance in situations where arguably law enforcement was previously free to act without statutory or constitutional restraint. Id. at 608. My critique of that approach is fourfold. First, there quite possibly are or should be constitutional limits on some of the surveillance that the Patriot Act apparently authorizes. Second, the Act sets the statutory standards so low in Professor Kerr's examples that any privacy protections are minimal at best. Third, if the Department of Justice had publicly claimed the even broader surveillance powers that Professor Kerr asserts it might possess, then there quite possibly would have been a political reaction from Congress to limit those broader surveillance powers. Fourth, any modest privacy gains that Professor Kerr might identify are outweighed by other aspects of the Act that reduce privacy in

to get, because there would be no probable cause that a crime had been or would be committed. Yet this potential or known spy plausibly posed a serious threat to national security. A wiretap might create extremely useful intelligence about the Soviet agent's confederates and actions.

For many people, including those generally inclined to support civil liberties, the example of a known spy operating within the United States provides an especially compelling case for allowing wiretaps and other surveillance. Spies operating within the United States pose a direct threat to national security. For instance, spies can and have turned over nuclear and other vital military secrets to foreign powers.[32] At the same time, some of the usual safeguards on wiretaps seem inappropriate when applied to foreign agents. Notifying the target of a criminal wiretap after the fact is required by the notice component of the Fourth Amendment and can be a crucial safeguard because it alerts citizens and the press of any over-use or abuse of the wiretap power. By contrast, notifying a foreign agent about a national security power can compromise sources and methods and create a diplomatic scandal. Similarly, minimization in the domestic context helps preserve the privacy of individuals who are not the target of a criminal investigation. Minimization in the foreign intelligence context, by contrast, can mean discarding the only hints available about the nature of a shadowy and hard-to-detect threat to security.

---

the electronic surveillance area, especially in the area of foreign intelligence surveillance discussed in this article.

[32] *See, e.g.*, Joseph Finder, *The Spy Who Sold Out*, N.Y. TIMES, July 2, 1995, § 7, at 5(criticizing Aldrich Ames for selling double agent identities); Atossa M. Alavi, *The Government Against Two: Ethel and Julis Rosenburg's Trial*, 53 CASE W. RES. 1057, 1059 (2003) (identifying Klaus Fuchs as the supplier of nuclear technology to the Soviets).

During wartime especially, it is easy to see how the temptation to use "national security" wiretaps against spies and foreign enemies, even on U.S. soil, would be irresistible. The legal basis for such a national security power can be derived from the text of the Constitution. The President is named Commander in Chief of the armed forces, and domestic actions against foreign powers may be linked to military and intelligence efforts abroad. This explicit grant of power to the President is supplemented by vague and potentially very broad language in Article II of the Constitution, that the President shall exercise the "executive power" and "take Care that the Laws be faithfully executed."[33] Going beyond the text, the Supreme Court in 1936 in *United States v. Curtiss-Wright Export Corp.*[34] relied on the structure of the Constitution and the nature of sovereign nations to establish the "plenary and exclusive power of the President as the sole organ of the federal government in the field of international relations."[35]

President Franklin Roosevelt, responding to the Second World War, was the first President to authorize wiretaps on national security grounds.[36] The use of such wiretaps expanded during the Cold War. In 1967, in *Katz*, the Supreme Court declined to extend its holding to cases "involving the national security."[37] In 1971, Justice Stewart summarized the expansion of the executive power that "in the two related fields of national defense and international relations[,] . . . largely unchecked by the Legislative

[33] U.S. CONST., art. II, § 3.
[34] United States V. Curtiss-Wright Export Corp., 299 U.S. 304 (1936).
[35] *Id.* at 320.
[36] *See* Alison A. Bradley, *Comment: Extremism in the Defense of Liberty?: The Foreign Intelligence Surveillance Act and the Significance of the USA PATRIOT ACT*, 77 TUL. L. REV. 465, 468 (2002) (describing limited nature of national security wiretaps authorized by President Roosevelt).
[37] Katz v. United States, 389 U.S. 347, 358 n.23 (1967).

and Judicial branches, has been pressed to the very hilt since the advent of the nuclear missile age."[38]

The Supreme Court finally addressed the lawfulness of national security wiretaps in 1972 in *United States v. United States District Court*[39], generally known as the "Keith" case after the name of the district court judge in the case.[40] The defendant, Plamondon, was charged with the dynamite bombing of an office of the Central Intelligence Agency in Michigan.[41] During pretrial proceedings, the defendants moved to compel the United States to disclose electronic surveillance information that had been obtained without a warrant.[42] The Attorney General submitted an affidavit stating that he had expressly approved the wiretaps, which were used "to protect the nation from attempts of domestic organizations to attack and subvert the existing structure of the Government."[43] The United States objected to disclosure of the surveillance materials, claiming that the surveillance was a reasonable exercise of the President's power (exercised through the Attorney General) to protect the national security.[44] Both the district court and the circuit court held for the defendant.[45]

The Supreme Court unanimously affirmed.[46] Justice Powell's opinion found that Title III, by its terms, did not apply to the protection of "national security information" and that the statute did not limit "the constitutional power of the President to take such

---

[38] New York Times Co. v. United States, 403 U.S. 713, 727 (1971) (Stewart, J., concurring); *see* STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW ch. 4, 60-91 (3d ed. 2002) (analyzing growth of executive power in national security realm).
[39] United States v. United States Dist. Ct., 407 U.S. 297 (1972) [hereinafter *Keith*].
[40] *Id.*
[41] *Id.* at 299.
[42] *Id.* at 299-300.
[43] *Id.* at 300 n.2.
[44] *See id.* at 301.

measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means . . . ."[47] As it turned to the constitutional discussion of the scope of the Fourth Amendment, the Court expressly reserved the issues of foreign intelligence surveillance that are now covered by FISA: "[T]he instant case requires no judgment on the scope of the President's surveillance power with respect to the activities of foreign powers, within or without this country."[48]

The Court then turned to the question left open by *Katz*, "[w]hether safeguards other than prior authorization by a magistrate would satisfy the Fourth Amendment in a situation involving the national security."[49] The Government sought an exception to the Fourth Amendment warrant requirement, relying on the inherent Presidential power and duty to "'preserve, protect, and defend the Constitution of the United States.'"[50] The Court acknowledged the importance of that duty, yet held that a warrant issued by a neutral magistrate was required for domestic security wiretaps.[51] Noting the First Amendment implications of excessive surveillance, the Court concluded: "Security surveillances are especially sensitive because of the inherent vagueness of the domestic security concept, the necessarily broad and continuing nature of intelligence gathering, and the temptation to utilize such surveillances to oversee political dissent."[52]

---

[45] *Id.*
[46] *Id.* at 324 (noting that "Mr. Justice Rehnquist took no part in the consideration or decision of this case.").
[47] *Id.* at 302 (quoting 18 U.S.C. § 2511(3)).
[48] *Id.* at 308. Later, the Court reiterated the point: "We have not addressed, and express no opinion as to, the issues which may be involved with respect to activities of foreign powers or their agents." *Id.* at 321-22 (citation omitted).
[49] *Id.* at 309 (quoting *Katz v. United States*, 389 U.S. 347, 358 n.23).
[50] *Id.* at 310 (quoting U.S. CONST. art. II, § 1).
[51] *Id.* at 319-321.
[52] *Id.* at 320.

While recognizing the potential for abuse in domestic security wiretaps, the Court also recognized the "different policy and practical considerations from the surveillance of 'ordinary crime.'"[53] The list of possible differences is entirely familiar to those engaged in the debates since September 11: the gathering of security intelligence is often for a long term; it involves "the interrelation of various sources and types of information;" the "exact targets of such surveillance may be more difficult to identify;" and there is an emphasis on "the prevention of unlawful activity."[54] In light of these differences, the nature of "reasonableness" under the Fourth Amendment can shift somewhat. The Court invited legislation: "Congress may wish to consider protective standards for [domestic security] which differ from those already prescribed for specified crimes in Title III."[55] The Court specifically suggested creating a different standard for probable cause and designating a special court to hear the wiretap applications, two invitations taken up by Congress in FISA.[56]

C. National Security Wiretaps and "The Lawless State"

The Supreme Court's invitation was eventually accepted by Congress in 1978 in the Foreign Intelligence Surveillance Act.[57] FISA was enacted at a unique time, in the wake of Watergate and spectacular revelations about illegal actions by U.S. intelligence agencies. In my opinion, anyone who wishes to debate FISA and possible amendments to it has a responsibility to consider the history of this period. I am not a pessimist who believes that intelligence activities inevitably will return to the level of lawlessness at that

[53] *Id.* at 322.
[54] *Id.*
[55] *Id.*
[56] *Id.* at 323.

time. I do believe, however, that human nature has remained largely unchanged since then. Unless effective institutional safeguards exist, large and sustained expansions of domestic intelligence activity, in the name of national security, can quite possibly recreate the troublesome behaviors of the past.

One particularly detailed account of the earlier period is a 1977 book by Morton Halperin, Jerry Berman and others entitled THE LAWLESS STATE: THE CRIMES OF THE U.S. INTELLIGENCE AGENCIES.[58] That book devotes an annotated chapter to the illegal surveillance activities of each agency -- the FBI, the CIA, the Army, the IRS, and others. The most famous discussion of the deeds and misdeeds of the intelligence agencies are the reports by the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, known as the "Church Committee" after its chairman, Frank Church.[59] The 1976 final report summarized the number of people affected by domestic intelligence activity:

> FBI headquarters alone has developed over 500,000 domestic intelligence files, and these have been augmented by additional files at FBI Field Offices. The FBI opened 65,000 of these domestic intelligence files in 1972 alone. In fact, substantially more individuals and groups are subject to intelligence scrutiny than the number of files would appear to indicate, since typically, each domestic intelligence files contains information on more than one individual or group, and this information is readily retrievable through the FBI General Name Index.
>
> The number of Americans and domestic groups caught in the domestic intelligence net is further illustrated by the following statistics:

---

[57] The Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (1978) (codified at 50 U.S.C. §§ 1801-1811(2000)).
[58] MORTON H. HALPERIN ET AL., THE LAWLESS STATE: THE CRIMES OF THE U.S. INTELLIGENCE AGENCIES (1976).
[59] FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK II, § I, U.S. Senate, Apr. 26, 1976 (footnotes omitted), *available at* http://www.derechos.net/paulwolf/cointelpro/churchfinalreportIIa.htm [hereinafter CHURCH FINAL REP. I].

> -- Nearly a quarter of a million first class letters were opened and photographed in the United States by the CIA between 1953-1973, producing a CIA computerized index of nearly one and one-half million names.
>
> -- At least 130,000 first class letters were opened and photographed by the FBI between 1940-1966 in eight U.S. cities.
>
> -- Some 300,000 individuals were indexed in a CIA computer system and separate files were created on approximately 7,200 Americans and over 100 domestic groups during the course of CIA's Operation CHAOS (1967-1973).
>
> -- Millions of private telegrams sent from, to, or through the United States were obtained by the National Security Agency from 1947 to 1975 under a secret arrangement with three United States telegraph companies.
>
> --An estimated 100,000 Americans were the subjects of United States Army intelligence files created between the mid 1960's and 1971.
>
> -- Intelligence files on more than 11,000 individuals and groups were created by the Internal Revenue Service between 1969 and 1973 and tax investigations were started on the basis of political rather than tax criteria.
>
> -- At least 26,000 individuals were at one point catalogued on an FBI list of persons to be rounded up in the event of a "national emergency."[60]

These statistics give a flavor for the scale of domestic surveillance. Rather than repeat the history in detail here, it is helpful to identify themes that show the important concerns raised by improper surveillance:

1. *Routine violations of law.* In THE LAWLESS STATE[61] the authors identify and document literally hundreds of separate instances of criminal violations by intelligence

[60] *Id.*
[61] HALPERIN ET AL., *supra* note 57.

agencies.[62] The Church Committee reported "frequent testimony that the law, and the Constitution were simply ignored."[63] The Committee quoted testimony from the man who headed the FBI's Intelligence Division for ten years: "[N]ever once did I hear anybody, including myself, raise the question: 'Is this course of action which we have agreed upon lawful, is it legal, is it ethical or moral.' We never gave any thought to this line of reasoning, because we were just naturally pragmatic."[64] Instead of concern for the law, the intelligence focus was on managing the "flap Potential" – the likely problems if their activities became known.[65]

2. *Expansion of surveillance, for prevention and other purposes.* After World War II, "preventive intelligence about 'potential' espionage or sabotage involved investigations based on political affiliations and group membership and association. The relationship to law enforcement was often remote and speculative . . . ."[66] Until the Church Committee's hearings, the FBI continued to collect domestic intelligence under "sweeping authorizations" for investigations of "'subversives', potential civil disturbances, and 'potential crimes.'"[67] Based on its study of the history, the Church Committee concluded: "The tendency of intelligence activities to expand beyond their initial scope is a theme which runs through every aspect of our investigative findings. Intelligence collection programs naturally generate ever-increasing demands for new

---

[62] *E.g., id.* at 3 (estimating number of surveillance crimes committed); id. at 93 (describing surveillance violations by the FBI).
[63] CHURCH FINAL REP. I, *supra* note 59.
[64] *Id.*
[65] *Id.*
[66] FINAL REPORT OF THE SELECT COMMITTEE TO STUDY GOVERNMENTAL OPERATIONS WITH RESPECT TO INTELLIGENCE ACTIVITIES, INTELLIGENCE ACTIVITIES AND THE RIGHTS OF AMERICANS, BOOK II, § II, U.S. Senate, Apr. 26, 1976 (footnotes omitted), *available at* http://www.derechos.net/paulwolf/cointelpro/churchfinalreportIIb.htm [hereinafter CHURCH FINAL REP. II].

data. And once intelligence has been collected, there are strong pressures to use it against the target."[68]

3. *Secrecy.* An essential aspect of domestic intelligence was secrecy:

> Intelligence activity . . . is generally covert. It is concealed from its victims and is seldom described in statutes or explicit executive orders. The victim may never suspect that his misfortunes are the intended result of activities undertaken by his government, and accordingly may have no opportunity to challenge the actions taken against him.[69]

It was only in the wake of the extraordinary events of Watergate and the resignation of President Nixon that Congress and the public had any inkling of the scope of domestic intelligence activities. That realization of the scope led directly to thoroughgoing legal reforms (many of which are being rolled back or questioned in the wake of September 11).

4. *Use against political opponents.* The Church Committee documented that: "Each administration from Franklin D. Roosevelt's to Richard Nixon's permitted, and sometimes encouraged, government agencies to handle essentially political intelligence."[70] Wiretaps and other surveillance methods were used on members of Congress, Supreme Court Justices, and numerous mainstream and non-mainstream political figures. The level of political surveillance and intervention grew over time.[71] By

---

[67] *Id.*
[68] CHURCH FINAL REP. I, *supra* note 59.
[69] *Id.*
[70] *Id.*
[71] "The FBI practice of supplying political information to the White House . . . under the administrations of President Lyndon Johnson and Richard Nixon . . . grew to unprecedented dimensions." CHURCH FINAL REP. II, *supra* note 66.

1972, tax investigations at the IRS were targeted at protesters against the Vietnam War,[72] and "the political left and a large part of the Democratic party [were] under surveillance."[73]

5. *Targeting and disruption of unpopular groups, including the civil rights movement.* The FBI's COINTELPRO – counterintelligence program – "was designed to 'disrupt' groups and 'neutralize' individuals deemed to be threats to national security."[74] Targets for infiltration included the Klu Klux Klan and the Black Panthers. A special target was Martin Luther King, Jr., from late 1963 until his death in 1968. The Church Committee report explained:

> In the words of the man in charge of the FBI's 'war' against Dr. King, 'No holds were barred. . . . The program to destroy Dr. King as the leader of the civil rights movement included efforts to discredit him with Executive branch officials, Congressional leaders, foreign heads of state, American ambassadors, churches, universities, and the press.'[75]

In one especially ugly episode, Dr. King was preparing to go to Sweden to receive the Nobel Peace Prize when the FBI sent him an anonymous letter threatening to release an embarrassing tape recording unless he committed suicide.[76]

6. *Chilling of First Amendment rights.* The FBI's COINTELPRO program targeted "speakers, teachers, writers, and publications themselves."[77] One internal FBI

---

[72] *Id.* Examining evidence of use of intelligence information against political opponents, the Committee concluded: "A domestic intelligence program without clearly defined boundaries almost invited such action." *Id.*

[73] HALPERIN ET AL., *supra* note 58, at 124.

[74] CHURCH FINAL REP. I, *supra* note 59.

[75] *Id.*

[76] *See* HALPERIN ET AL., *supra* note 58, at 86. The Church Committee reported on breath of the FBI's infiltration of the black community: "In 1970, the FBI used its 'established informants' to determine the 'background, aims and purposes, leaders and Key Activists" in every black student group in the country, 'regardless of [the group's] past or present involvement in disorders.'" CHURCH FINAL REP. II, *supra* note 66.

memorandum "called for 'more interviews' with New Left subjects 'to enhance the paranoia endemic in these circles' and 'get the point across there is an FBI agent behind every mailbox.'"[78] Once a federal agency is trying to get the message out that there is an "agent behind every mailbox," then the chilling effect on First Amendment speech can be very great indeed.

7. *Harm to individuals.* The hearings in the 1970s produced documented cases of harm to individuals from intelligence actions. For instance, an anonymous letter to an activist's husband accused his wife of infidelity and contributed strongly to the breakup of the marriage.[79] Also, "a draft counsellor deliberately, and falsely, accused of being an FBI informant was 'ostracized' by his friends and associates."[80] In addition to "numerous examples of the impact of intelligence operations," the Church Committee concluded that "the most basic harm was to the values of privacy and freedom which our Constitution seeks to protect and which intelligence activity infringed on a broad scale."[81]

8. *Distortion of data to influence government policy and public perceptions.* Used properly, intelligence information can provide the President and other decisionmakers with the most accurate information possible about risks to national security. The Church Committee found that intelligence agencies sometimes warped intelligence to meet their political goals:

> The FBI significantly impaired the democratic decisionmaking process by its distorted intelligence reporting on Communist infiltration of and influence on domestic political activity. In private remarks to Presidents and in public

[77] CHURCH FINAL REP. I, *supra* note 59.
[78] *Id.*
[79] *Id.*
[80] *Id.*
[81] *Id.*

> statements, the Bureau seriously exaggerated the extent of Communist influence in both the civil rights and anti- Vietnam war movements.[82]

9. *Cost and ineffectiveness.* The Church Committee concluded: "Domestic intelligence is expensive . . . . Apart from the excesses described above, the usefulness of many domestic intelligence activities in serving the legitimate goal of protecting society has been questionable."[83] After reviewing the effectiveness of various aspects of domestic intelligence, the Committee's chief recommendation was "to limit the FBI to investigating conduct rather than ideas or associations."[84] The Committee also specifically recommended continued "intelligence investigations of hostile foreign intelligence activity."[85]

In summary, the history shows numerous concrete examples of law-breaking by the U.S. intelligence agencies. More generally, the history helps show how secret information gathering and disruption of political opponents over time can threaten democracy itself. The fear is that leaders using "dirty tricks" and secret surveillance can short-circuit the democratic process and entrench themselves in power. The legal question is how to construct checks and balances that facilitate needed acts by the government but which also create long-term checks against abuse.

II. The 1978 Compromise: The Foreign Intelligence Surveillance Act

[82] CHURCH FINAL REP. II, *supra* note 66. *See also* RICHARD G. POWERS, SECRECY AND POWER: THE LIFE OF J. EDGAR HOOVER 429 (1987).
[83] CHURCH FINAL REP. I, *supra* note 59.
[84] *Id.*
[85] *Id.*

At the level of legal doctrine, the Foreign Intelligence Surveillance Act of 1978 was born from the two legal traditions discussed in Part I: the evolving Supreme Court jurisprudence that wiretaps required judicial supervision, and the continuing national security imperative that at least some foreign intelligence wiretaps be authorized. At the level of practical politics, FISA arose from the debate between the intelligence agencies, who sought maximum flexibility to protect national security, and the civil libertarians, who argued that the abuses revealed by the Church Committee should be controlled by new laws and institutions.[86]

The clear focus of FISA, as shown by its title, was on foreign rather than domestic intelligence. The statute authorized wiretaps and other electronic surveillance against "foreign powers."[87] These "foreign powers" certainly included the Communist states arrayed against the United States in the Cold War. The definition was broader, however, including any "foreign government or any component thereof, whether or not recognized by the United States."[88] A "foreign power" included a "faction of a foreign nation," or a "foreign-based political organization, not substantially composed of United States persons."[89] Even in 1978, the definition also included "a group engaged in international terrorism or activities in preparation therefor."[90]

Surveillance could be done against an "agent of a foreign power," which classically would include the KGB agent or someone else working for a foreign intelligence service.[91] An "agent of a foreign power" could also include a person who

---

[86] Hearing on *Foreign Intelligence Surveillance Act*, 95th Cong. 147, 148 (1979) (statement of Jerry Berman).
[87] The current definition is codified at 50 U.S.C. § 1801(a).
[88] *Id.* § 1801(a)(1).
[89] *Id.* § 1801(a)(2), (5).
[90] *Id.* § 1801(a)(4).
[91] *See id.* § 1801(b).

"knowingly engages in sabotage or international terrorism, or activities that are in preparation therefor, for or on behalf of a foreign power."[92] The definition of "international terrorism" had three elements: violent actions in violation of criminal laws; an intent to influence a government by intimidation or coercion; and actions that transcend national boundaries in their method or aims.[93]

The Act drew distinctions between United States persons and non-United States persons.[94] The former consists essentially of U.S. citizens and permanent residents.[95] Non-U.S. persons could qualify as an "agent of a foreign power" simply by being an officer or employee of a foreign power, or a member of an international terrorist group.[96] The standards for surveillance against U.S. persons were stricter, in line with the Church Committee concerns about excessive surveillance against domestic persons. U.S. persons qualified as an "agent of a foreign power" only if they knowingly engaged in listed activities, such as clandestine intelligence activities for a foreign power, "which activities involve or may involve a violation of the criminal statutes of the United States."[97]

In FISA, Congress accepted in large measure the invitation in *Keith*[98] to create a new judicial mechanism for overseeing national security surveillance. The new statute

---

[92] *Id.* § 1801(b)(2)(C).
[93] *See id.* § 1801(c). The term "international terrorism" was defined in full as activities that—
> (1) involve violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or of any State, or that would be a criminal violation if committed within the jurisdiction of the United States or any State; (2) appear to be intended— (A) to intimidate or coerce a civilian population; (B) to influence the policy of a government by intimidation or coercion; or (C) to affect the conduct of a government by assassination or kidnapping; and (3) occur totally outside the United States or transcend national boundaries in terms of the means by which they are accomplished, the persons they appear intended to coerce or intimidate, or the locale in which their perpetrators operate or seek asylum."

Id.
[94] *Id.* § 1801(i).
[95] *Id.*
[96] *Id.* § 1801(b)(1)(A).
[97] *Id.* § 1801(b)(2)(A).
[98] *Keith*, 407 U.S. 297 (1972).

used the terms "foreign power" and "agent of a foreign power" employed by the Supreme Court in *Keith*, where the Court specifically said that its holding applied to domestic security wiretaps rather than surveillance of "foreign powers."[99] Instead of creating a special regime for domestic security, however, Congress decided to split surveillance into only two parts – the procedures of Title III, which would apply to ordinary crimes and domestic security wiretaps, and the special procedures of FISA, which would apply only to "agents of a foreign power."[100]

A curious hybrid emerged in FISA between the polar positions of full Title III protections, favored by civil libertarians, and unfettered discretion of the Executive to authorize national security surveillance, favored by the intelligence agencies. The statute required the Chief Justice to designate seven (now eleven) district court judges to the new Foreign Intelligence Surveillance Court ("FISC").[101] These judges had jurisdiction to issue orders approving electronic surveillance upon finding a number of factors, notably that "there is probable cause to believe that the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . ."[102] This probable cause standard looks to quite different facts than the Title III standard, which requires "probable cause for belief that an individual is committing, has committed, or is about to commit a particular offense" for which wiretaps are permitted.[103]

FISA orders contain some but not all of the other safeguards in Title III. Both regimes require high-level approval within the Department of Justice, with the Attorney

---

[99] *Id.* at 308, 321-22.
[100] The 1978 law created the split by providing, in terms still effective today, that Title III and FISA "shall be the exclusive means by which electronic surveillance . . . and the interception of domestic wire and oral communications may be conducted." 18 U.S.C. § 2511(2)(f).
[101] 50 U.S.C. § 1803.
[102] *Id.* § 1805(a)(3)(A).
[103] 18 U.S.C. § 2518(3)(a).

General having to give personal approval for FISA applications.[104] Both regimes require minimization procedures to reduce the effects on persons other than the targets of surveillance.[105] Both provide for electronic surveillance for a limited time, with the opportunity to extend the surveillance.[106] Both require details concerning the targets of the surveillance and the nature and location of the facilities placed under surveillance.[107] Both allow "emergency" orders, where the surveillance can begin without judicial approval subject to quick, subsequent approval by a judge.[108]

As for differences, Title III gives discretion to the judge to refuse to issue the order, even where the statutory requirements have been met.[109] Under FISA, however, the judge "shall" issue the order once the statutory findings are met.[110] FISA has looser standards about whether other, less intrusive surveillance techniques must first be exhausted.[111]

The most important difference is that the existence of a Title III wiretap is disclosed to the subject of surveillance after the fact, in line with the Fourth Amendment

---

[104] *Compare* 50 U.S.C. § 1805(a)(2) (approval by the Attorney General for FISA applications), *with* 18 U.S.C. § 2518(11)(b)(i) (approval also permitted for domestic surveillance by the Deputy Attorney General, the Associate Attorney General, or an acting or confirmed Assistant Attorney General). The officers other than the Attorney General were added in 1984. Pub. L. No. 98-473, § 1203(a) (1984).
[105] *Compare* 50 U.S.C. § 1805(a)(4) (FISA applications), *with* 18 U.S.C. § 2518(5) (Title III applications).
[106] *Compare* 50 U.S.C. § 1805(e) (FISA applications), *with* 18 U.S.C. § 2518(5) (Title III applications).
[107] *Compare* 50 U.S.C. § 1805(c)(1) (FISA applications), *with* 18 U.S.C. § 2518(4) (Title III applications).
[108] FISA originally required an emergency order to receive judicial approval in twenty-four hours, but this was extended to seventy-two hours in 2001. Pub. L. No. 107-108, § 314(a)(2)(B) (2001) (codified at 50 U.S.C. § 1805(f)). Title III emergency orders must be approved by a judge within forty-eight hours. 18 U.S.C. § 2518(7).
[109] "Upon such application the judge *may* enter an ex parte order, as requested or as modified, authorizing or approving interception . . . ." 18 U.S.C. § 2518(3) (emphasis added).
[110] 50 U.S.C. § 1805(a).
[111] Title III requires that a wiretap or other electronic surveillance be a last resort, available only when "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous." 18 U.S.C. § 2518(3)(C). Under FISA, the application must simply certify "that such information cannot reasonably be obtained by normal investigative techniques." 50 U.S.C. § 1804(7)(C).

requirement that there be notice of government searches.[112] By sharp contrast, the FISA process is cloaked in secrecy. Targets of FISA surveillance almost never learn that they have been subject to a wiretap or other observation. The only statutory exception is where evidence from FISA surveillance is used against an individual in a trial or other proceeding. In such instances, the criminal defendant or other person can move to suppress the evidence on the grounds that the information was unlawfully acquired or the surveillance did not comply with the applicable order. Even in this setting the individuals have no right to see the evidence against them. The judge, upon a motion by the Attorney General, reviews the evidence in camera (in the judge's chambers) and ex parte (without assistance of defense counsel).[113]

The secrecy and ex parte nature of FISA applications are a natural outgrowth of the statute's purpose, to conduct effective intelligence operations against agents of foreign powers.[114] In the shadowy world of espionage and counter-espionage, nations that are friends in some respects may be acting contrary to U.S. interests in other respects. Prudent foreign policy may suggest keeping tabs on foreign agents who are in the United States, but detailed disclosure of the nature of that surveillance could create embarrassing incidents or jeopardize international alliances.

---

[112] Title III requires notice "[w]ithin a reasonable time but not later than ninety days" after surveillance expires. Notice is given to the persons named in the order and others at the judge's discretion. An inventory is provided concerning the dates and scope of surveillance. In the judge's discretion, the person or counsel may inspect such intercepted communications, applications and orders as the judge determines to be in the interest of justice. The judge may also, on a showing of good cause, postpone notice. 18 U.S.C. § 2518(8)(d).

[113] These procedures are set forth in 50 U.S.C. § 1806. In ruling on a suppression motion, the judge "may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.* § 1806(f). If the court determines that the surveillance was conducted lawfully, "it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure." *Id.* § 1806(g).

[114] *See* 50 U.S.C. § 1802(a0(1)(A)(i).

Along with the limited nature of judicial supervision, Congress decided to create additional institutional checks on the issuance of the secret FISA wiretaps. To regularize Congressional oversight, the Attorney General must report to the House and Senate Intelligence Committees every six months about FISA electronic surveillance, including a description of each criminal case in which FISA information has been used for law enforcement purposes.[115] The Attorney General also must make an annual report to Congress and the public about the total number of applications made for orders and extensions of orders, as well as the total number that were granted, modified, or denied.[116] This report is similar to that required for Title III wiretaps, but the latter provides additional details such as the types of crimes for which a wiretap is used and the number of wiretaps that resulted in successful prosecutions.[117] Although the FISC ruled against an order for the first time in 2002, as described below,[118] the annual FISA reports provide a rough guide of the extent of FISA surveillance.[119]

Congress also relied on institutional structures within the executive branch to check over-use of domestic surveillance.[120] The requirement that the Attorney General authorize applications meant that the FBI on its own could no longer implement national security wiretaps. Applications by the FBI would need to be approved by the Justice

---

[115] *See id.* § 1808(a). In the initial years after passage of FISA, the Intelligence Committees were additionally required to report to the full House and Senate about the operation of the statute. *Id.* § 1808(b).
[116] *Id.* § 1807.
[117] *See* 18 U.S.C. § 2529 (reports on Title III wiretaps); *see also id.* § 3126 (reports on pen register and trap and trace orders).
[118] *See infra* note 199.
[119] *See* Electronic Privacy Information Center, *Foreign Intelligence Surveillance Act Orders 1979-2002*, *available at* http://www.epic.org/privacy/wiretap/stats/fisa_stats.html (collecting FISA report statistics). The 2003 FISA Report stated that three additional orders were denied in 2003. William E. Moschella, U.S. Department of Justice, Office of Legislative Affairs letter to L. Ralph Mecham, Director, Administrative Office of the United States Courts, Apr. 30, 2004, *available at* http://www.epic.org/privacy/terrorism/fisa/2003_report.pdf. At the time of this writing, no further information is publicly available about the three denials.

Department. In light of the historical evidence about the independence of long-time FBI Director J. Edgar Hoover from control by the Justice Department,[121] and the disagreements that have often continued between the FBI and the Department,[122] this supervision by the Justice Department was a potentially significant innovation in FISA.

Reacting to the historical evidence about surveillance of political speech and association, the 1978 statute 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."[123] This language reflects a Congressional concern about infringement on First Amendment activities, but provides only modest safeguards, because an individual could apparently be considered an agent of a foreign power based "largely" or "substantially" on protected activities.

Finally, the text of the 1978 statute showed that the purpose of the FISA wiretaps was foreign intelligence rather than preventing or prosecuting crimes. The Church Committee and other revelations of the 1970s had shown that the FBI had used the risk of "subversion" and other potential crimes as the justification for investigating a vast array of political and other domestic activity.[124] The 1978 statute therefore specified that the

---

[120] 50 U.S.C. § 1805(a)(2).
[121] *E.g.*, JIM MCGEE & BRIAN DUFFY, MAIN JUSTICE 309 (1996).
[122] *See, e.g.*, Jeff Nesmith et al., *Subtle forces swirl just beneath siege inquires: The tug of personality conflict in Washington alters flow of Waco controversy*, AUSTIN AMERICAN-STATESMAN, Sept. 19, 1999, at A1 (discussing "tension" between the Department of Justice and the FBI and between Attorney General Reno and FBI Director Freeh).
[123] 50 U.S.C. § 1805(a)(3)(A).
[124] *See* CHURCH FINAL REP., *supra* note 59 (noting that between 1960 and 1974, "subversion" alone was used to justify over 500,000 investigations, with apparently no prosecutions for the actual crime).

application for a FISA order certify that "the purpose of the surveillance is to obtain foreign intelligence information."[125]

In summary, the 1978 FISA revealed a grand compromise between the advocates for civil liberties and the intelligence community. From the civil liberties side, FISA had the advantage of creating a legal structure for foreign intelligence surveillance that involved Article III judges. It had the disadvantage of having standards that were less protective overall than were constitutionally and statutorily required for investigations of domestic crimes. In particular, the notice requirement of the Fourth Amendment did not apply, and targets of FISA surveillance usually never learned they were the objects of government searches. From the intelligence perspective, FISA had the disadvantage of imposing bureaucratic rules and procedures on searches that had previously been done subject to the inherent authority of the President or the Attorney General. An advantage, which became more evident over time, was that FISA provided legislative legitimation for secret wiretaps, and created standardized bureaucratic procedures for getting them. By establishing these clear procedures, it became easier over time for the number of FISA surveillance orders to grow. To describe the compromise in another way, FISA set limits on surveillance by the Lawless State, but gave the Lawful State clear rules that permitted surveillance.

III. FISA from 1978 to 2001

The Foreign Intelligence Surveillance Act of 1978 was part of a broad-based effort in the wake of Watergate to place limits on the Imperial Presidency and its

[125] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, § 104, 92 Stat. 1783 (codified at 50 U.S.C. § 1804(7)). This language was changed in 2001 to say that " a significant purpose of the investigation is to obtain foreign intelligence information." Id. *See infra* Part IV.A.1..

surveillance activities.[126] The Privacy Act of 1974 clamped down on secret files on Americans and created new legal rules for how personal information could be used by federal agencies.[127] The Freedom of Information Act was broadened substantially in 1974,[128] and greater openness in government was encouraged by the Government in the Sunshine Act,[129] new rules in legislatures to open up committee hearings to the public,[130] and more aggressive investigative journalism in the wake of the revelations by Woodward and Bernstein.[131]

The FBI in particular had to change its operations, including its domestic surveillance activities, in the wake of the revelations about the Lawless State. The best-known limits on the FBI's activities were the Guidelines on Domestic Surveillance issued by Attorney General Levi in 1976.[132] These Guidelines limited domestic security investigations to activities that both "involve or will involve the use of force or violence" and "involve or will involve the violation of federal law." The Guidelines defined procedures and time limits for preliminary, limited, and full investigations. The FBI was required to report in detail about investigations to the Department of Justice, and the Attorney General or his designees had the power to terminate investigations at any time. To address concerns about intrusion into First Amendment activity, the Guidelines stated that all domestic security investigations "shall be designed and conducted so as not to

[126] *See generally* ARTHUR M. SCHLESINGER, THE IMPERIAL PRESIDENCY (1973).
[127] Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, 1896 (codified at 5 U.S.C. § 552a).
[128] Freedom of Information Act, Pub. L. No. 93-502, § 4, 88 Stat. 1561, 1564 (1974) (amending 5 U.S.C. § 552).
[129] Government in the Sunshine Act, Pub. L. No. 94-409, 90 Stat. 1241 (1976) (codified as amended at 5 U.S.C. § 552 et seq.).
[130] *See generally* The Reporters' Committee for Freedom of the Press, Tapping Officials' Secrets, *available at* http://www.rcfp.org/tapping (collecting state open meeting laws).
[131] *See* CARL BERNSTEIN & ROBERT WOODWARD, ALL THE PRESIDENT'S MEN (1974) and THE FINAL DAYS (1977).

limit the full exercise of rights protected by the Constitution and laws of the United States."[133]

The Levi Guidelines represented a judgment that the best way to save the FBI as an effective agency was to demonstrate that it had come within the rule of law. Greater oversight of investigations by the Justice Department was central to the new approach: "If the FBI would play by the new rules, the Justice Department would defend it to the hilt."[134] The FBI likely shifted over time to a much higher compliance with legal rules than had been true before the revelations of the 1970s.[135]

The implementation of FISA after 1978 followed a similar pattern of Justice Department oversight of the FBI. Mary Lawton, the lead drafter of the Levi Guidelines, eventually became the chief of the Office of Intelligence Policy and Review ("OIPR") within the Justice Department.[136] Previously, the FBI had forum shopped in different parts of the Justice Department to get approval for domestic surveillance. Now the OIPR became the gatekeeper for all applications to the Foreign Intelligence Surveillance Court.

---

[132] Attorney General, U.S. Department of Justice, "Domestic Security Investigations," Apr. 5, 1976. For subsequent verisions of these guidelines see http://www.epic.org/privacy/fbi (including comprehensive links to subsequent domestic surveillance guidelines and related materials).

[133] Id.

[134] McGee & Duffy, *supra* note 121, at 311.

[135] For instance, shortly after I left the government I had a lengthy conversation with a senior FBI lawyer who had watched the changes over previous decades. He frankly admitted that the Bureau had not worried much about breaking the law before the mid-1970s. He said, though, that the painful revelations and the bad effects on the careers of those caught up in those revelations had led to a profound change in the organization's culture. The Bureau, by early 2001, had developed a culture of compliance.

These statements tracked the views of a very knowledgeable insider with whom I worked in government. He agreed that the FBI had generally learned to follow the rules since the 1970s. He also believed that they often had very aggressive interpretations of the rules, and then they stayed within the limits of their interpretation.

This shift to a culture of compliance has some important implications. First, these observations on the Bureau's behavior underscore the importance of rules such as the Attorney General Guidelines. If an agent complies with a set of defined rules, then the content of those rules matters. Second, the lessons from the 1970s deeply impressed a generation of FBI employees with the risks of excessive surveillance and intrusion into First Amendment activities. With the passage of time, fewer veterans of that experience will remain in the Bureau, and the impact of those lessons will be less, potentially raising the risk of renewed abuses.

Mary Lawton, who had once finished first in her class at the Georgetown Law Center, sat at the center of the process, applying "Mary's Law" to applications for FISA surveillance.[137]

The 1996 book MAIN JUSTICE, which provides the most detailed public writing about the period, summarizes the combined effect of having FISA applications signed by the intelligence agent, the lawyer who drafted it, the head of the intelligence agency, and the Attorney General:

> All those signatures served a purpose, to assure the federal judge sitting in the FISA court that a national security wiretap was being sought for 'intelligence purposes' and for no other reason—not to discredit political enemies of the White House, not to obtain evidence for a criminal case through the back door of a FISA counterintelligence inquiry.[138]

This is consistent with my view of perhaps the most controversial change in FISA in the Patriot Act – the breaking down of the "wall" between foreign intelligence and law enforcement activities. My own understanding is that the wall has existed since the creation of FISA in 1978, but there has always been a gate in it. The OIPR has been the gatekeeper. It has permitted foreign intelligence information to go to law enforcement in a limited number of cases, but it has historically remained mindful of the basic dictate of FISA, that the purpose of FISA surveillance was for foreign intelligence and that there should be safeguards on the domestic surveillance that had created such problems in the period of The Lawless State.

This understanding is consistent with the text of FISA and the actions of the Justice Department in 1995. As discussed above, the text of the original FISA stated that

---

[136] MCGEE & DUFFY, *supra* note 121, at 314.
[137] For an admiring portrait of Mary Lawton and her role in shaping foreign intelligence law until her death in 1993, see the chapter entitled "Mary's Law" in MAIN JUSTICE. *Id.* at 303-19.
[138] *Id.* at 318.

"the purpose" of the surveillance was to obtain foreign intelligence information.[139] The text also provided mechanisms for using information from FISA wiretaps in court, subject to special rules about in camera review by the judge of the FISA material.[140] Taken together, the text suggests a preponderance of use of the special wiretaps for foreign intelligence, with use for law enforcement only where the evidence was developed in the course of a bona fide foreign intelligence surveillance.[141] In 1995, two years after the death of Mary Lawton, Attorney General Janet Reno issued confidential guidelines to formalize procedures for contacts among the FBI, the Criminal Division, and OIPR for foreign intelligence and foreign counterintelligence investigations.[142] The guidelines gave OIPR a central role in the process. Both the FBI and the Criminal Division, for instance, were required to notify OIPR of contact with each other concerning such investigations, and contacts between the FBI and the Criminal Division were logged.[143] The FBI was generally prohibited from contacting any U.S. Attorney's Office concerning such investigations without prior permission of both OIPR and the Criminal Division.[144] OIPR was further directed to inform the FISC of the existence of, and basis for, any contacts among the FBI, the Criminal Division, and a U.S. Attorney's

---

[139] *See supra* note 125 and accompanying text.
[140] *Id.*
[141] The Senate Report on FISA stated, "'Contrary to the premises which underlie the provision of Title III of the Omnibus Crime Control Act of 1968 . . . it is contemplated that few electronic surveillances conducted pursuant to [FISA] will result in criminal prosecution.'" MCGEE & DUFFY, *supra* note 120 at 326-27 (quoting members of the Senate Select Committee on Intelligence, 1978 Report).
[142] Memorandum from Janet Reno, Attorney General, to Assistant Attorney General, Criminal Division, FBI Director, Counsel for Intelligence Policy, and United States Attorneys (July 19, 1985), at http://www.fas.org/irp/agency/doj/fisa/1995procs.html [hereinafter "Reno Guidelines"]. For a description of the genesis and contents of the 1995 Guidelines, see id. at 327-43.
[143] *Id.*
[144] *Id.* § A.2.

Office "in order to keep the FISC informed of the criminal justice aspects of the ongoing investigation."[145]

Alongside these developments in the Justice Department, FISA changed only modestly from 1978 until the events of September 11, 2001. Federal courts upheld FISA against constitutional challenges.[146] The courts also upheld some broadening of the purpose requirement, allowing surveillance where "the primary purpose," rather than "the purpose," was to gather foreign intelligence information.[147]

Although FISA originally applied only to electronic surveillance, Congress gradually widened its scope to other tools commonly used by law enforcement in criminal cases. After Attorney General Reno relied on her inherent powers to authorize physical surveillance of CIA spy Aldrich Ames' home, the Justice Department requested and received the authority in 1995 to apply to the FISC for physical searches.[148] In 1998, the Act was extended to include pen register and trap-and-trace orders (listing of the telephone numbers and similar information contacted by an individual).[149] The same year, the Act was extended to permit access to limited forms of business records, notably including vehicle rental records of the sort relevant to investigations of the Oklahoma City and first World Trade Center bombings.[150] These extensions were analogous to

---

[145] *Id.* § A.7.
[146] *E.g.*, United States v. Duggan, 743 F.2d 59, 71 (2d Cir. 1984) (no violation of Fourth Amendment or the separation of powers); United States v. Belfield, 692 F.2d 141, 149 (D.C. Cir. 1982) (no violation of Fifth or Sixth Amendment rights); United States v. Falvey, 540 F. Supp. 1306, 1313 (E.D.N.Y. 1982) (no violation of First Amendment rights).
[147] *Duggan*, 743 F.2d at 77-78; for a discussion of other cases that also used the "primary purpose" test, see note 217 and accompanying text.
[148] *See* Intelligence Authorization Act for Fiscal Year 1995, Pub. L. No. 103-359, § 807, 108 Stat. 3444, 3444-45 (1994) (codified as amended at 50 U.S.C. § 1821-29).
[149] *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, 112 Stat. 2396, 2405 (1998) (codified at 50 U.S.C. §§ 1841-1846).
[150] *Id.* at § 602 (codified at 50 U.S.C. §§ 1861-1862 (2000)) (permitting access held by common carriers, physical storage facilities, public accommodation facilities, and vehicle rental facilities).

FISA electronic surveillance, with the primary purpose to gather information on foreign powers or agents of foreign powers.

The most significant change was likely the increased number of FISA orders. Once the FISA system was up and running in 1981, there remained between 433 and 600 orders for each year through 1994, except for a one-year total of 635 in 1984.[151] In 1995, 697 orders were granted, growing in subsequent years to 839, 748, 796, 880, and 1012 during President Clinton's term.[152] FISA orders fell to 934 in 2001, and grew to record numbers of 1228 in 2002 and 1727 in 2003.[153] By comparison, the number of federal Title III wiretap orders in 1981 was 106, with a peak of 601 in 1999 and a total of 578 in 2003, the most recent year for which statistics are available.[154] State law enforcement also conducted Title III wiretaps, with a total of 861 reported for 2002.[155] Taken together, FISA wiretaps have grown substantially in the past decade, especially after September 11. Since the early 1980s they have constituted the majority of federal wiretaps.

In assessing the implementation of FISA from 1978 to early 2001, the basic structures from the 1970s remained fairly fixed. The bargain of FISA had been realized – the government could carry out secret surveillance in the United States, subject to limits to "foreign intelligence" activities and oversight by all three branches of government. The "wall" was in place, with the OIPR as the chief gatekeeper for exchange of

---

[151] Electronic Privacy Information Center, *Foreign Intelligence Surveillance Orders 1979-2002, available at* http://www.epic.org/privacy/wiretap/stats/fisa_stats.html.
[152] *Id.*
[153] *Id.*; William E. Moschella, U.S. Department of Justice, Office of Legislative Affairs letter to L. Ralph Mecham, Director, Administrative Office of the United States Courts, Apr. 30, 2004, *available at* http://www.epic.org/privacy/terrorism/fisa/2003_report.pdf.
[154] 2003 Wiretap Report 3, *available at* http://www.uscourts.gov/wiretap03/contents.html.

information between the foreign intelligence and law enforcement operations. Despite the Attorney General Guidelines, there were some instances where civil liberties critics produced evidence that "domestic surveillance" had interfered with First Amendment activities, but these instances seemed fairly few.[156] There was some expansion of legal authority, but the greatest practical change was likely the increased number of FISA applications over time, especially since efforts to fight terrorism climbed during the 1990s.[157]

IV. The Patriot Act, The New Guidelines, and New Court Decisions

The attacks of September 11 led to the greatest changes by far in FISA law and practice since its creation in 1978. This Part examines the statutory amendments in the Patriot Act, new Attorney General guidelines on foreign intelligence surveillance and domestic security investigations, and the first published decisions by the Foreign Intelligence Surveillance Court and the Foreign Intelligence Surveillance Court of Review.

A. The USA-PATRIOT Act

The Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 ("Patriot" Act)[158] was proposed by the Bush Administration a week after the attacks of September 11 and

---

[155] *Id.* For discussion of the relative lack of institutional safeguards on wiretaps conducted at the state level, see Kennedy & Swire, *supra* note 20, at 977-983.

[156] The greatest concerns were expressed about FBI surveillance of the Committee in Solidarity with the People of El Salvador (CISPES) in the 1980s. *See* Electronic Privacy Information Center, *The Attorney General's Guidelines*, *available at* http://www.epic.org/privacy/fbi/ (collecting sources).

[157] For instance, FISA wiretaps and search authorizations increased from 484 in 1992 to 839 in 1996 (after the Oklahoma City and first World Trade Center incidents), while federal Title III wiretaps increased more slowly, from 340 in 1992 to 581 in 1996. *See* Electronic Privacy Information Center, *Foreign Intelligence Surveillance Act Orders 1979-2002*, *available at* http://www.epic.org/privacy/wiretap/stats/fisa_stats.html (listing FISA statistics); Electronic Privacy Information Center, *Title III Electronic Surveillance 1968-2002*, *available at* http://www.epic.org/privacy/wiretap/stats/wiretap_stats.html (listing Title III statistics).

signed into law on October 26, 2001.[159] Among the numerous changes in the law, the focus here is on three topics: the permission for FISA orders to have only "a significant purpose" of foreign intelligence; the use of FISA orders to get any "tangible object;" and the expansion of national security letters.

1. From "primary purpose" to "a significant purpose." The 1978 law required the application for a FISA order to certify that "the purpose of the surveillance is to obtain foreign intelligence information."[160] As discussed above, a number of Circuit Courts interpreted this language to mean that the "primary purpose" of the order must be to obtain foreign intelligence information.[161] To ensure that the purpose of criminal law enforcement did not predominate, the "wall" was created between law enforcement and foreign intelligence investigations.

The Bush Administration proposed that the text should change so that "a purpose" would be for foreign intelligence information.[162] After debate in Congress, the Patriot Act finally provided that "a significant purpose" must exist in order to obtain foreign intelligence information.[163] A separate provision emphasized that Congress wished to promote information sharing between criminal investigations and foreign intelligence

---

[158] Uniting and Strengthening America by Providing Appropriate Tools Required to intercept and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, P.L. No. 107-56, 115 Stat. 272 [hereinafter Patriot Act].
[159] *Id.* For an illuminating and detailed account of the passage of the Act, see Beryl A. Howell, *Seven Weeks: The Making of the USA PATRIOT Act*, 72 GEO. WASH. L. REV. 1145 (2004).
[160] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783, 1788 (codified at 50 U.S.C. § 1804(7)).
[161] *See* cases cited *supra* notes 146-147and accompanying text.
[162] Section 153 of the Administration's original proposal would have changed "the purpose" to "a purpose." Center for Democracy & Technology, *Testimony of Jerry Berman before the Senate Select Comm. on Intelligence on Legislative Measures to Improve America's Counter-Terrorism Programs*, Sept. 24, 2001, *available at* http://www.cdt.org/testimony/010924berman.shtml.
[163] Patriot Act, P.L. No. 107-56, § 218, 115 Stat. 272, 291 (codified at 50 U.S.C. § 1804(7)).

investigations.[164] The implications of these legislative changes were the subject of first published opinions by the FISC and the FISCR, and are discussed further below.

2. FISA orders for any "tangible object." Section 215 of the Patriot Act expanded the sweep of FISA orders to compel production of business records and other tangible objects.[165] The original FISA had focused on electronic surveillance and had not created a FISA mechanism for the government to get business records. After the Oklahoma City and first World Trade Center bombings, Congress authorized the use of FISA orders for travel records only.[166]

Section 215 contained two statutory changes that drastically expanded this power. First, the type of records subject to the order went far beyond travel records. Now the search can extend to "any tangible things (including books, records, papers, documents, and other items) . . . ."[167] By its terms, the statute apparently would allow a FISA order to trump other laws that usually govern the release of records, including for medical records and other categories of records that are generally subject to privacy protections.

Second, the legal standard changed for obtaining the order. Previously, the application had to show "specific and articulable facts giving reason to believe that the person to whom the records pertain is a foreign power or an agent of a foreign power."[168]

---

[164] Section 203 of the Patriot Act made it significantly easier for grand jury information to be shared for foreign intelligence and counterintelligence purposes. *Id.* § 203(a), 115 Stat. at 278-281. It also provided:

> Notwithstanding any other provision of law, it shall be lawful for foreign intelligence or counterintelligence . . . 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.

Id. § 203 (d), 115 Stat. at 281.

[165] *Id.* § 215, 115 Stat. at 287-288.

[166] *See* Intelligence Authorization Act for Fiscal Year 1999, Pub. L. No. 105-272, 112 Stat. 2396, 2411-12 (1998) (codified at 50 U.S.C. §§ 1861-1862) (permitting access held by common carriers, physical storage facilities, public accommodation facilities, and vehicle rental facilities).

[167] *Supra* note 165, 115 Stat. at 287.

[168] 50 U.S.C. § 1861(b)(2)(B) (1999) (current version at 50 U.S.C.A. § 1861(b)(2) (2003)).

This standard, although less than probable cause, is relatively strict. The Patriot Act eliminated the need for any particularized showing. The application need merely "specify that the records concerned are sought for an authorized investigation . . . to protect against international terrorism or clandestine intelligence activities."[169] What counts as an authorized investigation is within the discretion of the executive branch.

Under this change in the text, FISA orders can now apply to anyone, not only the target of the investigation. Previously, the records or other objects sought had to concern either a foreign power or the agent of a foreign power. Now, the FISA order can require production of records about persons who have nothing to do with a foreign power.[170] The only weak restraints include the need for "an authorized investigation" and the requirement that surveillance of U.S. persons not be based solely upon First Amendment activities.[171] This is a significant change, permitting seizure of records of persons who are not the target of an investigation and not an agent of a foreign power.[172] Similarly, by permitting the order to cover records of all persons, the literal terms of Section 215 would permit an entire database to be the subject of a FISA order. So long as there is "an authorized investigation" the statute does not set any limits on the type or number of records subject to the FISA order.[173]

---

[169] 50 U.S.C. § 1861(b)(2) (2003).
[170] *See id.*
[171] *See id.*
[172] An analogous point was made by Justice Stevens concerning the expansion of searches in the law enforcement setting:

> Just as the witnesses who participate in an investigation or a trial far outnumber the defendants, the persons who possess evidence that may help to identify an offender, or explain an aspect of a criminal transaction, far outnumber those who have custody of weapons or plunder. Countless law-abiding citizens—doctors, lawyers, merchants, customers, bystanders—may have documents in their possession that relate to an ongoing criminal investigation.

Zurcher v. Stanford Daily, 436 U.S. 547, 579 (1978) (Stevens, J., dissenting).
[173] *See* 50 U.S.C. § 1861.

It is true that the range of records available to the government in criminal investigations has also expanded in recent decades.[174] One important safeguard in the criminal area, however, is that the records must be sought in connection with a crime that has been, is, or will be committed. In addition, as discussed further below,[175] Section 215 contains what is often called a "gag rule"—"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."[176] No similar rule applies to business records produced in the course of a criminal investigation.

3. Expansion of "National Security Letters." The Patriot Act significantly expanded the scope of the little-known tool of "National Security Letters" (NSLs). These are essentially the foreign intelligence corollary to administrative subpoenas for criminal investigations. Before the Patriot Act, NSLs allowed for access to certain records listed by statute, such as subscriber information for phone companies and Internet Service Providers and basic account information from banks and credit reporting agencies.[177]

The amendments to NSLs track the changes in Section 215. Previously, there was the same significant showing required for each record, that "there are specific and articulable facts giving reason to believe that the person or entity to whom the information sought pertains is a foreign power or an agent of a foreign power."[178] The Patriot Act requires only that the records be "relevant" to an authorized investigation, and

---

[174] For my discussion of the expanded power of the government to get records in the area of criminal investigations see Peter P. Swire, Katz *is Dead. Long Live* Katz., 102 Mich. L. Rev. 904 (2004).
[175] *See infra* notes 3255-26 and accompanying text (discussing gag rule in Section 215).
[176] 50 U.S.C. § 1861(d).
[177] NSLs are permitted under the Electronic Communications Privacy Act, 18 U.S.C. § 2709, for telephone and electronic communications records; the Right to Financial Privacy Act, 12 U.S.C. § 3414(a)(5)(A), for financial records; and the Fair Credit Reporting Act, 15 U.S.C. § 1681u for credit records.

no longer requires that the target of the request be a foreign power or agent of a foreign power.[179]

The Patriot Act broadened the sorts of investigations that qualify for NSLs for telephone and transactional records. Before, NSLs applied only to an "authorized foreign counter-intelligence operation."[180] Now they apply to "an authorized investigation to protect against international terrorism or clandestine intelligence activities."[181] The Patriot Act also lowered the level of official who could authorize an NSL. Previously, clearance had to come from a position of at least Deputy Assistant Director.[182] Now, a Special Agent in Charge in a Bureau field office may authorize an NSL, without any clearance by FBI headquarters.[183]

The expanded scope of NSLs likely deserves significant attention because they operate without the participation of a judge and individuals never receive notice that the records have been sought.[184] Federal officials have stated that NSLs have become more common and been used at least "scores" of times since September 11.[185] Moreover, the Bush Administration has sought approval for the CIA and the Pentagon to use NSLs inside of the United States, without the participation of the FBI or the Department of Justice.[186]

---

[178] 18 U.S.C. § 2709(b)(1)(B) (2000).
[179] 18 U.S.C. § 2709 (b)(1) (2003). As a modest safeguard, the Patriot Act included the requirement that "an investigation of a United States person is not conducted solely on the basis of activities protected by the first amendment to the Constitution of the United States." *Id.*
[180] 18 U.S.C. § 2709(b)(2)(A) (1999).
[181] 18 U.S.C. § 2709(b)(1) (2003).
[182] 18 U.S.C. § 2709(b) (1999).
[183] 18 U.S.C. § 2709(b) (2003).
[184] The individual may discover the use of the NSL if a criminal prosecution is later brought.
[185] Dan Eggen & Robert O'Harrow, Jr., *U.S. Steps Up Secret Surveillance*, WASH. POST, Mar. 23, 2003, at A1 (reporting on congressional testimony).
[186] Eric Lichtblau & James Risen, *Broad Domestic Role Asked for C.I.A. and the Pentagon*, N.Y. TIMES, May 2, 2003, at A21.

4. Other changes in the Patriot Act. There were other FISA amendments in the Patriot Act that will not be the subject of detailed analysis here. The standard for getting a FISA pen register or trap-and-trace order was simplified in the Patriot Act. Previously, these orders could only be issued if there was reason to believe that the telephone line subject to the order had been or was about to be used in communications involving international terrorism or an agent of a foreign power.[187] That requirement was dropped in the Patriot Act, with the standard becoming essentially the same as for domestic orders. The order can issue where the information is "relevant to an ongoing investigation."[188]

The Patriot Act also extended "roving" wiretaps to FISA. Wiretap orders historically were linked to an individual telephone. With changing technology, individuals more often used multiple phones and other communications facilities. Congress approved the use of law enforcement wiretaps linked to an individual—roving wiretaps—in 1998.[189] The Patriot Act permitted roving wiretaps under FISA for the first time, "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."[190]

---

[187] 50 U.S.C. § 1842(c)(3) (2000).
[188] 50 U.S.C. § 1842(c)(2) (2003). For discussion of the domestic standard for pen register and trap-and-trace orders, see Peter P. Swire, *Administration Wiretap Proposal Hits the Right Issues But Goes Too Far*, Brookings Terrorism Project Website, October 3, 2001, *available at* http://www.brookings.edu/dybdocroot/views/articles/fellows/2001_swire.htm.
[189] 18 U.S.C. § 2518(11)-(12).
[190] 50 U.S.C. § 1805(c)(2)(B) (2003). For a critique of post-Patriot Act proposals by the Department of Justice to expand roving wiretaps further, see Center for Democracy and Technology, *DOJ Proposes Further Surveillance Expansion Changes to Intelligence Authorization Would Again Increase FISA Eavesdropping*, Nov. 30, 2001, *available at* http://www.cdt.org/security/011130cdt.shtml.

The pen register and roving wiretap provisions, like the "significant purpose" test and Section 215, sunset on December 31, 2005, although existing investigations can proceed under the Patriot Act even if there is no extension of the statutory authority.[191]

B. New Guidelines in the Department of Justice

There have been numerous changes in the FBI and the Department of Justice since September 11 as the organizations have sought to respond to the terrorist threat. One overall pattern has been to discard earlier Department of Justice policies that set limits on foreign and domestic intelligence gathering. Proponents have seen these changes as overdue efforts to eliminate red tape. Critics have feared that important safeguards are being eliminated

The "wall" between foreign intelligence and law enforcement has come under particular challenge. Some changes began immediately after September 11. Previously, Justice Department guidelines had required the expert office of Justice, the OIPR, to be present at all meetings and discussions between the FBI and the Criminal Division for many FISA cases. After the attacks, OIPR no longer participated in all such meetings and instead reviewed a daily briefing book to inform itself and the Foreign Intelligence Surveillance Court about those discussions.[192]

The procedures for information sharing were greatly streamlined in "Intelligence Sharing Procedures" approved by Attorney General Ashcroft on March 6, 2002.[193] These new guidelines were designed "to permit the complete exchange of information and

---

[191] USA Patriot Act of 2001. P. L. No. 107-56, § 224, 115 Stat. 272, 295. The expanded NSL authority in Section 505 of the Patriot Act does not sunset. *See id.*
[192] *In re* All Matters to Foreign Intelligence Surveil., 218 F. Supp. 2d 611, 619 (Foreign Intel. Surv. Ct. 2002) [hereinafter *FISC Decision*].
[193] *See In re* Sealed Case, 310 F.3d 717, 729 (Foreign Int. Surv. Ct. Rev. 2002) [hereinafter *FISCR Decision*].

advice between intelligence and law enforcement officials."[194] They eliminated the prior restriction on prosecutors or other law enforcement officials "directing or controlling" the use of FISA surveillance.[195] They allowed the exchange of advice between the FBI, OIPR, and the Criminal Division regarding "the initiation, operation, continuation, or expansion of FISA searches or surveillance."[196] In short, the new guidelines sought to remove entirely the wall that limited information sharing between foreign intelligence and criminal investigations.

In May, 2002, Attorney General Ashcroft rolled back another set of limitations on surveillance that had been put in place during the 1970s. The Levi Guidelines of 1976 had set strict limitations on domestic security investigations, including rules designed to ensure that First Amendment activities were not improperly the subject of surveillance.[197] The new guidelines comprehensively revised the Levi Guidelines. Attorney General Ashcroft said that "terrorism prevention is the key objective under the revised guidelines."[198] He stressed that "unnecessary procedural red tape must not interfere with the effective detection, investigation, and prevention of terrorist activities."[199] An analysis by Jerry Berman and Jim Dempsey of the Center for Democracy and Technology highlighted three civil liberties concerns with the changes.[200] First, the

---

[194] *Id.*
[195] *Id.*
[196] *Id.*
[197] *See supra* note 132and accompanying text.
[198] Remarks of Attorney General John Ashcroft, *Attorney General Guidelines*, May 30, 2002, *available at* http://www.fas.org/irp/news/2002/05/ag053002.html.
[199] *Id.*
[200] Jerry Berman & James X. Dempsey, *CDT's Guide to the FBI Guidelines: Impact on Civil Liberties and Security – The Need for Congressional Oversight*, June 26, 2002, *available at* http://www.cdt.org/wiretap/020626guidelines.shtml. The concerns about infringement of the First Amendment that were so prominent in the Levi Guidelines were given much less weight in the new guidelines; "The law enforcement activities authorized by this Part do not include maintaining files on individuals *solely* for the purpose of monitoring activities protected by the First Amendment or the lawful exercise of any other rights secured by the Constitution or laws of the United States." John Ashcroft, *The*

guidelines gave new authority to FBI agents to attend public meetings and events of domestic groups without the need for suspicion of criminal or terrorist activity. Second, the guidelines authorized routine mining of commercial databases for personal information about citizens and organizations with no limitations on sharing and retention of that data. Finally, the guidelines reduced internal FBI supervision of the various stages of investigation, especially by expanding the use of preliminary inquiries where there is no reasonable indication of criminal or terrorist conduct.

C. Decisions by the FISA Courts

Passage of the Patriot Act and changes in the guidelines concerning the "wall" led to the first published decisions of the Foreign Intelligence Surveillance Court (FISC) and the Foreign Intelligence Surveillance Court of Review (FISCR).[201]

The FISC decision was issued in May, 2002 and became public as a result of oversight led by then-Chairman Leahy of the Senate Judiciary Committee.[202] The opinion, agreed to by all seven judges of the FISC, ordered detailed procedures to maintain the "wall" between foreign intelligence and criminal investigations.[203] The statutory basis for the decision was the requirement in FISA that there be minimization procedures.[204] The statute requires the Attorney General to create procedures "that are reasonably designed in light of the purpose and technique of the particular surveillance,

---

Attorney General's Guidelines on General Crimes, Racketeering Enterprise and Terrorism Enterprise Investigations, May 20, 2002, at 23 (emphasis added), *available at* http://www.usdoj.gov/olp/generalcrimes2.pdf. This language, which tracks the FISA restriction on surveillance "solely" on the basis of First Amendment activities, gives wide permission for surveillance that affects First Amendment activities. *See id.*

[201] *See* cases cited *supra* notes 192-193.

[202] *The USA Patriot Act in Practice: Shedding light on the FISA Process: Hearing Before the Committee on the Judiciary*, 107th Cong. (2002) (statement of Sen. Patrick Leahy, Chairman, Senate Comm. on Judiciary) http://www.fas.org/irp/congress/2002_hr/091002leahy.html.

[203] *FISC Decision*, 218 F. Supp. 2d 611, 622, 625 (Foreign Intel. Surv. Ct. 2002)

[204] *See id.* at 621; *see also* 50 U.S.C. § 1801(h)(1) & § 1821(4)(A).

to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information."[205] The court found that the March, 2002 guidelines for information sharing were not reasonably designed to meet the statutory requirement.[206]

One factor in the court's decision appears to have been its frustration about "an alarming number of instances" where the existing 1995 guidelines limiting information sharing had been violated.[207] In a series of reports to the court beginning in March, 2000 the government admitted to misstatements and omissions of material facts in over seventy-five FISA applications.[208] "In virtually every instance," the FISC wrote, "the government's misstatements and omissions . . . involved information sharing and unauthorized disseminations to criminal investigators and prosecutors."[209]

The FISC also clearly believed that the "wall" was an established and integral part of the overall structure of FISA.[210] The court relied on the text of FISA that referred to the need to "obtain, produce, and disseminate *foreign intelligence information*."[211] In the view of the FISC, the primary purpose of FISA surveillance must be foreign intelligence information. That information could later be used in criminal prosecutions only if it was initially collected with a foreign intelligence purpose in mind.

---

[205] 50 U.S.C. § 1801(h)(1) & § 1821(4)(A).
[206] *FISC Decision*, 218 F. Supp. 2d at 625.
[207] *Id.* at 620.
[208] *Id.* at 620-21. For instance, one certification by the FBI Director stated erroneously that the target of the FISA application was not under criminal investigation. After a meeting by the judges and the Department of Justice, one FBI agent was barred from appearing before the FISC as a FISA affiant and an investigation was opened by the Justice Department's Office of Professional Responsibility. *See id.*
[209] *Id.* at 621.
[210] The court wrote that the 1995 guidelines implementing the "wall" were "an integral part of the minimization process." *Id.* at 619.

That interpretation of the statute was rejected on appeal. The three judges in the FISCR, federal appellate judges named by Chief Justice Rehnquist, issued an opinion that was distinctly friendly to information sharing and hostile to any continuation of the "wall."[212] The court found that the distinction between surveillance for foreign intelligence and surveillance for law enforcement was a "false dichotomy" under FISA as enacted in 1978.[213] The overall effect of the opinion was to uphold the March, 2002 Ashcroft Guidelines against statutory and constitutional challenges.

The opinion dismissed the view, adopted by the FISC, that the 1978 version of FISA had contemplated some form of the "wall."[214] The FISCR referred to the "supposed barrier" against information sharing.[215] It said it was "quite puzzling" why the Department of Justice, since at least the 1980s, had read the statute to limit the use of FISA surveillance when intended for criminal prosecution.[216] The court then acknowledged that at least the First, Second, Fourth, and Eleventh Circuits had interpreted FISA to mean that "the primary purpose" of surveillance was supposed to be for foreign intelligence purposes.[217] In finding that all of these cases were incorrect on the doctrine, the FISCR said that it "is almost as if [these cases] assume that the government seeks foreign intelligence information (counterintelligence) for its own

---

[211] *Id.* at 622 (emphasis in original) (citations omitted).
[212] *See FISCR Decision*, 310 F.3d 717, 746 (Foreign Int. Surv. Ct. Rev. 2002).
[213] *Id.* at 725-735.
[214] *Id.* at 735.
[215] *Id.* at 721.
[216] *Id.* at 723.
[217] *Id.* at 725-727 (discussing United States v. Johnson, 952 F.2d 565, 572 (1st Cir. 1991); United States v. Pelton, 835 F.2d 1067, 1075-76 (4th Cir. 1987); United States v. Badia, 827 F.2d 1458, 1464 (11th Cir. 1987); United States v. Duggan, 743 F.2d 59 (2d Cir. 1984); United States v. Truong Dinh Hung, 629 F.2d 908 (4th Cir. 1980) (concerning surveillance done before enactment of FISA)).

sake—to expand its pool of knowledge—because there is no discussion of how the government would use that information outside criminal prosecutions."[218]

In my opinion, this quote ignores a common-sense and widely-shared alternative view. The alternative approach was explained by the FISC judges who address foreign intelligence surveillance on a daily basis – the text of the statute refers to the need to "obtain, produce, and disseminate foreign intelligence information."[219] As written in 1978, "the purpose" of the surveillance must be for foreign intelligence information.[220] Once that surveillance also happens to turn up evidence of criminal violations, then that information can be provided to law enforcement officials.[221]

This alternative explanation is consistent with the legislative history of the 1978 law, which was a compromise between advocates for law enforcement and civil liberties. A vivid concern from the civil liberties side was that the secret FISA wiretaps would expand into an unchecked power to do surveillance outside of the safeguards of Title III. The 1978 House Report clearly indicated the thinking at the time. It stated that "FISA surveillances 'are not primarily for the purpose of gathering evidence of a crime. They are to obtain foreign intelligence information, which when it concerns United States persons must be necessary to important national concerns.'"[222] In response to this seemingly clear quotation, the FISCR said only: "That, however, was an observation, not a proscription."[223] To put the matter rhetorically, the FISCR found it "quite puzzling" why the Department of Justice would comply with the "wall", even when multiple circuit

---

[218] *Id.* at 727.
[219] *See FISC Decision*, 218 F. Supp. 2d 611, 625 (Foreign Intel. Surv. Ct. 2002).
[220] *See id.*
[221] *See id.*
[222] *FISCR Decision*, 310 F.3d 717, 725 (Foreign Int. Surv. Ct. Rev. 2002) (quoting H.R. Rep. No. 95-1283, at 36 (1978)).
[223] *Id.*

courts had thus interpreted the new statute. I find it "quite puzzling" how the court could so easily dismiss the view that FISA was enacted to seek foreign intelligence information, and was not supposed to be a tool for any law enforcement official who wanted to avoid Title III and the other usual restrictions on domestic surveillance.

With that said, I find more persuasive the FISCR's finding that the Patriot Act changed the relevant law for sharing gathered intelligence with law enforcement. The new law stated that "a significant purpose" rather than "the purpose" had to be for foreign intelligence. The court wrote, "Congress was keenly aware that this amendment relaxed a requirement that the government show that its primary purpose was other than criminal prosecution."[224] While correctly finding that Congress intended to change the rules, the court made it surprisingly easy for the government to meet the standard of "a significant purpose." The government need show merely "a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes."[225] The court added, "So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test."[226] This interpretation of "significant purpose" gives little weight to what is "significant." It especially seems to ignore the decision by Congress to raise the Administration's proposed language of "a purpose" up to the stricter test of a "significant purpose."[227]

---

[224] *Id.* at 732. The court quotes Senator Leahy, who considered the change "very problematic," as saying that it "would make it easier for the FBI to use a FISA wiretap to obtain information where the Government's most important motivation for the wiretap is for use in a criminal prosecution." *Id.* at 733 (quoting 147 Cong. Rec. S10593 (Oct. 11, 2001)).
[225] *Id.* at 735.
[226] *Id.* The court noted that "if the court concluded that the government's *sole* objective was merely to gain evidence of past criminal conduct—even foreign intelligence crimes—to punish the agent rather than halt ongoing espionage or terrorist activity, the application should be denied." *Id.* (emphasis added).
[227] *See supra* notes 1599-64 and accompanying text (discussing amendment debate).

The last portion of the FISCR opinion addresses constitutional challenges advanced in amicus briefs submitted by the National Association of Criminal Defense Lawyers and by an alliance of groups led (alphabetically) by the American Civil Liberties Union.[228] It seems quite possible that a court more troubled by civil liberties issues than the FISCR panel would have found the constitutional challenges more compelling under the Fourth Amendment, First Amendment, and Due Process Clause. The FISCR, however, found the challenges without merit. It correctly noted that *Keith* addressed domestic security, not the constitutionality of surveillance of agents of foreign powers.[229] The court did not, though, address the complex line-drawing issues between domestic and foreign intelligence surveillance that the Supreme Court had noted in *Keith*.[230] The FISCR also did an overall "reasonableness" assessment of FISA surveillance under the Fourth Amendment in comparison with Title III.[231] In finding that FISA meets constitutional requirements, the court concluded that "in many significant respects the two statutes are equivalent, and in some, FISA contains additional protections."[232] The FISCR panel did not directly address the detailed analysis by the FISC that showed the crucial differences between the two regimes.[233]

In summary, the legal changes in the Patriot Act significantly expanded the potential range of searches under the foreign intelligence laws. The revised guidelines in the Department of Justice permit a broader range of domestic security surveillance. The

---

[228] The briefs are available at http://www.epic.org/privacy/terrorism/fisa/. The ACLU joined with the Center for Democracy and Technology, the Center for National Security Studies, the Electronic Privacy Information Center, and the Electronic Frontier Foundation. The Court permitted the amici to file briefs but allowed only the Department of Justice to appear at oral argument. *See id.*
[229] *See FISCR Decision*, 310 F.3d at 744.
[230] *See id.* at 744-45.
[231] *See id.* at 741-42.
[232] *Id.* at 741.
[233] FISC Decision, 218 F. Supp. 2d at 625.

FISCR decision rejected statutory and constitutional challenges to this greatly expanded sharing between foreign intelligence and law enforcement investigations.

V. The System of Foreign Intelligence Surveillance Law

The article to this point has explored the complex history that led to the 1978 passage of FISA and the 2001 changes contained in the Patriot Act. This Part creates a framework for analyzing the system of foreign intelligence surveillance law. The next Part examines specific proposals for reform.

A. Foreign Intelligence Law as a System for Both National Security and the Rule of Law

One way of understanding FISA is that it substitutes a systemic check on abuse for the case-by-case checks on abuse built into ordinary law enforcement actions. In a Title III case, a neutral magistrate decides whether to authorize a wiretap based on probable cause and other showings required by the statute.[234] The target of the wiretap receives notice after the wiretap is complete and has access to the transcripts in order to prepare the defense[235] The full protections of the American criminal justice system then apply, with rights provided by the Fourth, Fifth, and Sixth Amendments and from other sources. Critics of the current criminal system may believe that additional rights are constitutionally required or statutorily desirable, but the basic approach is one based on individual defendants being able to assert their rights in open court.[236]

These individualized protections clearly work less well for FISA cases. Many FISA surveillance orders never result in criminal prosecutions. In those instances, no one

---

[234] 18 U.S.C. § 2510.
[235] *See* 18 U.S.C. § 2518(8) & *supra* note 111.
[236] *E.g.*, Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 66 (1988).

outside of the government ever learns about the existence or nature of the surveillance. For those FISA orders that do create evidence for criminal cases, extraordinary procedures prevent defendants from seeing the nature of the evidence against them.[237] For example, the defendant cannot compare an original statement with the translation prepared by the government translator.[238] If the government translator exaggerates the threat in a defendant's statement, through bias or the lack of knowledge of a dialect's nuance, then there is no adversary system to correct the mistake.

Under FISA, a greater share of the safeguards against abuse occur at the system-wide level. System-wide, can Congress provide effective oversight of foreign intelligence surveillance? System-wide, do Attorney General Guidelines and other Justice Department oversight dictate appropriate checks on the FBI and other intelligence agencies? How well does the Office of Intelligence Policy and Review work? Do the judges on the Foreign Intelligence Surveillance Court provide helpful judicial supervision of the system, even without an adversary process? Whatever the answers to these questions, it is clear that, compared to criminal procedure, fewer of the safeguards happen at the individual ("retail") level, and more happen at the systemic ("wholesale") level.

If one considers FISA as part of a system for foreign intelligence law, then the two principal goals of the system are protecting national security and doing so in a manner consistent with the constitution, the rule of law, and civil liberties. In pursuing these goals, the individual components of the legal system might vary over time or based on differing judgments about efficacy or overall desirability. To give one example, broad surveillance might be accompanied by greater external oversight. An alternative but

[237] 50 U.S.C. § 1806; *see supra* notes 111-12 and accompanying text.
[238] *See* 50 U.S.C.A. § 1806.

roughly equivalent approach might have less intrusive oversight but also less broad access to records. To give another example, greater constitutional protections might be accompanied by fewer statutory limits, or fewer constitutional protections might be accompanied by more detailed statutory provisions. In short, there are alternative institutional approaches for seeking the twin goals of national security and the rule of law. The normative goal should be to assess the institutional choices to help develop an overall, sustainable system of foreign intelligence law.[239]

B. The Special Status of the 1978 Compromise

In considering alternative institutional approaches, I suggest that the appropriate baseline is the 1978 compromise that resulted in passage of FISA. As a matter of constitutional law, the Supreme Court provided its clearest guidance about the Fourth Amendment and electronic surveillance in the period just before 1978. The 1967 *Katz* and *Berger* decisions overruled *Olmstead* and emphasized the strong constitutional limits on how electronic surveillance could be used for law enforcement purposes.[240] The constitutional mandates for law enforcement wiretaps notably included notice to the target once a wiretap was concluded and the ability of defendants to confront the wiretap and other evidence against them.[241] The 1972 *Keith* case held that the Fourth Amendment requires a prior warrant for electronic surveillance in domestic security matters.[242] While bringing "domestic security" cases clearly within the scope of the Fourth Amendment, *Keith* expressed "no opinion as to . . . activities of foreign powers or

[239] For an extended and effective explanation of the usefulness of comparative institutional analysis, see NEIL K. KOMESAR, IMPERFECT ALTERNATIVES: CHOOSING INSTITUTIONS IN LAW, ECONOMICS, AND PUBLIC POLICY (1995).
[240] *See supra* notes 16-27 and accompanying text.
[241] *See supra* notes 111-12 and accompanying text.
[242] *See Keith*, 407 U.S. 297, 324 (1972).

their agents."[243] Congress precisely tracked *Keith* in enacting FISA in 1978 to apply to "foreign powers or their agents."[244] In doing so, Congress legislated in the zone left undefined by the Supreme Court, but did not apply the new FISA procedures to the law enforcement actions governed by *Katz* and *Berger*, or to the domestic security matters governed by *Keith*.

The 1978 compromise responded not only to these constitutional directions from the Supreme Court but also from what one might call the "constitutional moment" of the Watergate events.[245] The magnitude of the constitutional crisis is encapsulated by the resignation of President Nixon, the only such resignation in history. The Church Committee and other revelations of the period, as discussed above, cast unprecedented light on systematic problems in how surveillance was conducted, including: routine violations of law; expansion of surveillance, for preventive and other reasons; secrecy; use against political opponents; targeting and disruption of unpopular groups, including the civil rights movement; chilling of First Amendment rights; harm to individuals; distortion of data to influence government policy and public perceptions; issues of cost and ineffectiveness; and the risk of entrenching current leadership.[246]

In reaction to new constitutional doctrine and the constitutional magnitude of the Watergate crisis, Congress engaged in the most elaborate deliberation in its history on

---

[243] *Id.* at 321-22.
[244] *See supra* notes 97-99 and accompanying text.
[245] The term "constitutional moment" is associated with Bruce Ackerman. *See* 1 BRUCE ACKERMAN, WE THE PEOPLE: FOUNDATIONS 266-94 (1991). Use of the term here is not intended to take a definite position on the complex scholarly disputes about the details of Professor Ackerman's theory or of the history that surrounded the periods that Professor Ackerman chooses for special study. *See, e.g.*, Michael J. Klarman, *Constitutional Fact/Constitutional Fiction: A Critique of Bruce Ackerman's Theory of Constitutional Moments*, 44 STAN. L. REV. 759 (1992) (critiquing Ackerman position). Instead, the term usefully captures the unique historical moment of Watergate and the constitutional-style reforms that led to checks on the Imperial Presidency in measures such as greater openness of government and reduced secret surveillance.

how to legislate in the linked areas of domestic security, foreign intelligence, and law enforcement[247]. The intelligence agencies and other concerned parties expressed their views to Congress. FISA was a result of these intense deliberations. I believe there should be a burden of proof on those who would substantially change the system of foreign intelligence surveillance law from the 1978 compromise. Proponents of change should explain how proposed changes would be consistent with the Constitution and lead to an overall improvement in the system of foreign intelligence surveillance law.

C. To What Extent Did "Everything Change" After September 11?

Proponents of expanding FISA argue on a number of grounds that "everything has changed" since the attacks of September 11, 2001.[248] President Bush, in his address to Congress nine days later, called for expanded surveillance powers and said, "Americans have known surprise attacks, but never before on thousands of civilians. All of this was brought upon us in a single day, and night fell on a different world, a world where

---

[246] *See supra* text accompanying notes 61-85.

[247] *See generally*, *Subcommittee on the Rights of Americans*, 95th Cong. (1977) (considering the historical power to use surveillance inherent to the President and the Fourth Amendment rights that might outweigh it); *Surveillance Technology: Policy and Implications: An Analysis and Compendium of Materials,* 95th Cong. 378 (1977) (considering the benefits of other agencies having access to methods of surveillance); *Hearings before the Subcommittee on Legislation of the Permanent Select Committee on Intelligence*, 95th Cong. 3 (1978) (balancing the efficiency benefits of allowing more surveillance rights against the benefits of privacy) (statement of Robert McClory).

[248] For a rhetorical attack on the view that "everything has changed", see Magniloquence Against War!, *Everything has Changed, or Has It?, available at* http://irregulartimes.com/everything.html. For a recent set of academic essays on the subject, see September 11 in History: A Watershed Moment? (Mary L. Dudziak, ed. (2004). The historian and legal scholar Mary Dudziak stated: "The assumption that September 11 had been a moment of change was again ubiquitous. Yet, in an unscientific poll taken by the Web site for historians History News Network, 67 percent of respondents answered 'no' to the question, 'On balance, would you say that 9-11 changed America in a decisive way?' Only 28 percent thought that it had." Mary L. Dudziak, "Afterward: Remembering September 11," id. at 212. This article agrees with the majority of historians by putting the attacks of September 11 into historical context, both by giving the history of previous government abuse of surveillance powers, *supra* notes 58-85 and accompanying text, and by comparing the threat posed by terrorism after September 11 with the equivalent or greater threats that faced the United States in previous periods, *infra* notes 252-273 and accompanying text.

freedom itself is under attack."[249] In considering what may have changed and what may justify legal changes, prominent candidates include: the magnitude of the threat; the nature of the threat from terrorism rather than nation states; the domestic component of the threat, including "sleeper cells;" the failure of the previous intelligence system to prevent the attacks of September 11; and the need to respond to new threats more quickly, in "real time." After elaborating on claims that these threats justify greater surveillance powers, the discussion here explains significant counter-arguments.[250]

1. *Magnitude of the threat.* The attacks of September 11 resulted in the highest number of deaths of any foreign attack on U.S. soil. A great deal of government attention has focused since the attacks on the risks of "weapons of mass destruction", including discussion of the risk that terrorists will gain control of nuclear devices. In rhetorical terms, proponents of surveillance can ask: "What limits on surveillance do you want us to observe if we know that someone has a nuclear bomb somewhere in New York City?"

2. *Threat from terrorists rather than nation states.* During the Cold War, the global landscape was frozen to an extent into pro-Western and pro-Communist blocs. The greatest threats came from identified enemies, and the hot line and other institutions were developed for regularizing contacts between the opposing blocs. By contrast, the terrorist threat is inchoate and geographically in flux. In a world of asymmetrical warfare, greater surveillance can detect and respond to newly emerging threats.

3. *Sleeper cells and other domestic threats.* The threat today is not principally from foreign states and their hired agents. Instead, the hijackers on September 11 and the

[249] President George W. Bush, Address to a Joint Session of Congress (Sept. 20, 2001), *available at* http://www.everythingcomputers.com/presbushspeech.htm.

detection of a possible sleeper cell in Lackawanna, New York show that serious threats exist here at home.[251] Given the proven size of terrorist attacks, the emphasis must be on prevention of attacks before they occur.[252] Extensive surveillance before the commission of any crime is needed to achieve that prevention.

4. *The failure of the previous intelligence system.* A law professor is tempted to say "res ipsa loquitur." The attacks of September 11 happened, and what more needs to be said about the need to change the previous system for anti-terrorist intelligence gathering? In particular, the failure of the FBI and the CIA to "connect the dots"—caused in no small part by the "wall" that prevented information sharing—meant that key information in Moussaoui's computer was not read until after the attacks.[253] In the face of this crucial failure, the burden has been met for shifting to greater information sharing and preventive action.

5. *The need to respond in "real time".* Terrorists today communicate at the speed of the Internet. Al Qaeda has a flexible, global network to respond quickly and unpredictably to new opportunities for terrorism. In responding to these fast-moving threats, American intelligence agencies cannot afford to be slowed down by burdensome warrants and other paperwork requirements. Information must be shared in real time with the officials who need it, so that responses can match the nature of the threat.

---

[250] In developing the argument for the magnitude of the threat and the other arguments, I am attempting to present the arguments for greater surveillance in a coherent way, and the statements in the text do not necessarily reflect my own judgment about the facts.

[251] Six Yemeni-Americans living in Lackawanna, New York pled guilty in 2003 to providing material support to a terrorist organization. The six reportedly received weapons training in Afghanistan in the spring of 2001 and heard Osama bin Laden speak in person. Prosecutors suggested that the six might have constituted a sleeper cell, available for possible future terrorist attacks in the United States, but the six denied that accusation. *See* Phil Hirschkorn, *Al Qaeda trainee gets 10-year sentence*, Dec. 3, 2003, *available at* http://www.cnn.com/2003/LAW/12/03/buffalo.six.index.html.

[252] FBI Director Mueller said in 2003 that the prevention of terror attacks was the top priority of the agency. David Johnson, *9/11 Congressional Report Faults F.B.I.-C.I.A. Lapses*, N.Y. TIMES, July 23, 2003, at A12.

D. Some responses to the claim that "everything has changed."

Anyone considering this list of risks—the magnitude of the threat, its terrorist nature, the domestic threats, the previous failures, and the need to respond in real time—should seriously consider the possibility that important changes to the 1978 compromise are now due. The acts of our national leaders underscores the concern. Attorneys General Reno and Ashcroft, who disagree on many issues, both made fighting terrorism a priority. Anti-terrorism funding and the number of FISA orders increased rapidly under President Clinton,[254] and President George W. Bush has made fighting terrorism a centerpiece of his Administration's policies.

The difficult judgment, especially for anyone who does not have access to classified information about actual threats, is to assess the magnitude of the risks to national security and the effectiveness of surveillance powers to reduce those risks. This Article earlier showed reasons for believing that historically there has been excessive domestic surveillance against "subversives" and other domestic threats, but the risks facing the country today may be greater. Henry Kissinger is credited for the quip that "Even a paranoid has some real enemies."[255] The U.S. intelligence agencies are paid to be paranoid, to consider any possible threats against the nation. Even if they have sometimes exaggerated the risk in past periods, the risks today or the effectiveness of

---

[253] *See, e.g.*, Editorial, *Tearing Down Intelligence Walls*, CHI. TRIB., Nov. 9, 2003, at 8.

[254] On funding, for instance, "from fiscal years 1995 to 1998, the FBI more than doubled its allocation of resources for combating terrorism." General Accounting Office, *Combating Terrorism: FBI's Use of Federal Funds for Counterterrorism-Related Activities (FYs 1995-1998)*, 2 (Nov. 1998), *available at* http://www.gao.gov/archive/1999/gg99007.pdf.; *see also* Barton Gellman, *Struggles Inside the Government Defined Campaign*, WASH. POST, Dec. 20, 2001, at A1 (examining funding increases and other Clinton Administration anti-terrorism actions, concluding, "[b]y any measure available, Clinton left office having given greater priority to terrorism than any president before him."). For the rise in the number of FISA orders, *see supra* notes 152-155 and accompanying text.

[255] *See* Simpson's Contemporary Quotations (1988), *available at* http://www.bartleby.com/63/38/4638.html.

new surveillance tools may justify stronger surveillance measures. In addition, after the revelations of the 1970s, the watchdog capabilities of the press and the public may be greater, so that the risk of abuse may be lower now.

This uncertainty about the actual threats argues for a particular humility in recommending how to legislate on foreign intelligence surveillance when the current FISA provisions expire in 2005. Nonetheless, there are significant counter-arguments to the claim that "everything is different."

1. *The magnitude and non-nation state nature of the threat.* There is a natural human tendency to feel that the problems of the moment are particularly severe, yet the size of the terrorist threat seems smaller when seen in historical context. The most relevant historical comparisons are likely to the Palmer Raids after World War I, McCarthyism in the early 1950s and the civic disturbances of the Vietnam era.[256] The Palmer Raids and McCarthyism were direct responses to the fear of international communism.[257] The timing of those periods of anti-Communism was no accident. Each closely followed on a major Communist success – the Bolshevik Revolution of 1917 and the triumph of Mao in China in the late 1940s.[258] Compared with capturing the two largest countries in the world, nothing in the terrorist list of accomplishments comes close. The threat from the civic disturbances of the late 1960s and early 1970s is more difficult to quantify. At the sheer level of disturbance of daily life, however, the disruptions were clearly greater then than now. Most major cities suffered riots during this period and the *Keith* court itself, while upholding the Fourth Amendment

[256] *See generally* Nancy Murray & Sarah Wunsch, *Civil Liberties in Times of Crisis: Lessons from History*, 87 MASS. L. REV. 72 (2002).
[257] *See id.*

requirement for domestic surveillance, noted government statistics that there were 1,562 bombing incidents in the first half of 1971 alone, most of which involved Government related facilities.[259]

It is also questionable to assert that there is greater threat from terrorists than from an enemy nation state. At the level of logic, it seems likely that a large, well-organized enemy with a secure territory (i.e., a nation state) will pose a greater threat than a dispersed enemy that lacks a physical safe haven. That is why there is such emphasis on inhibiting the state sponsors of terrorism. At the historical level, the McCarthy period coincided with the demonstration that the Soviets had developed the atomic and then the hydrogen bomb, as well as a large-scale conventional war with the North Koreans and then the Chinese.[260] With the development of the intercontinental ballistic missile, the enemies of the United States developed the clear capacity to wipe out many American cities and perhaps all human life on Earth.[261] By comparison, the terrorist threat today, as severe as it is, is less all-encompassing.

2. *The threat domestically*. Many Americans today are struck by the insidious, domestic nature of the terrorist threat. The hijackers of September 11 lived in ordinary neighborhoods and carried out many commonplace daily activities. A member of a sleeper cell might be just down the block from your home at this moment. Faced with these agents of foreign interests acting at home, surely the special nature of this threat calls for new, strong measures.

---

[258] *See id.*
[259] *Keith*, 407 U.S. 297, 311 n.12 (1972). The Supreme Court noted that this statistic was subject to dispute and stated that the "precise level of this activity . . . is not relevant to the disposition of this case." *Id.*
[260] For an insightful history of the McCarthy period, see MARY L. DUDZIAK, COLD WAR CIVIL RIGHTS (2000).
[261] JONATHAN SCHELL, THE FATE OF THE EARTH 6 (1982).

In response, history shows that the earlier periods of high surveillance also involved threats that Americans believed were dangerously domestic yet linked with foreign influence. The Palmer Raids were directed in large measure at new immigrants from Eastern Europe who were suspected of being sympathetic to international Bolshevism.[262] In the 1950s, the fears stereotypically were of a Communist under every bed; more soberingly, historians today generally accept that Alger Hiss and other senior American officials indeed were spying for the Soviet Union, and a large number of Americans were linked with organizations that can now be identified as Communist fronts.[263] J. Edgar Hoover's relentless surveillance of Martin Luther King, Jr. during the 1960a seems to have been based in part on his belief that King was a Communist.[264] As the Vietnam War progressed, U.S. intelligence agencies continually tried to link domestic political opposition to Communist and other foreign influence.[265] This history doesn't discount the domestic threat, but it shows that domestic risk has been a staple of previous periods rather than being a new phenomenon of September 11.

3. *The failure of the previous intelligence system.* There is no brief answer to the question of whether the attacks of September 11 demonstrate a failure in the previous rules for foreign intelligence. In many ways, the inquiry into the proper system of foreign intelligence is the subject of this entire Article. A few points, however, can cast doubt on the res ipsa loquitur idea that the existence of the September 11 attacks demonstrates a need for substantial change in the legal framework directing surveillance.

---

[262] For a somewhat similar analysis, see Jonathan Rauch, *Osama Bin Laden, Meet Your Closest Kin: Karl Marx*, NAT'L J., July 13, 2002, *available at* http://reason.com/rauch/071302.shtml ("In many respects, militant Islam is weaker than Marxism was in its heyday.").
[263] For a detailed historical examination of Alger Hiss, see G. Edward White, *Alger Hiss's Campaign for Vindication*, 83 B.U. L. REV. 1 (2003).
[264] *See* RICHARD G. POWERS, SECRECY AND POWER: THE LIFE OF J. EDGAR HOOVER 375-80 (1987).
[265] *Id.* at 427.

First, publicly available information shows that the FBI and other intelligence agencies had successfully detected and halted attacks before September 11.[266] These successful actions provide context for the failure to prevent the September 11 attacks. Second, the failure to gain timely access to Moussaoui's computer seems to have resulted in part due to the FISC concerns that FISA applications had become misleading.[267] Accurate applications, rather than a wholesale change in the law, could be a sensible response to that sort of problem. Third, the Colleen Rowley whistleblowing indicates a variety of other problems within the intelligence system that could be solved without the need for enhanced surveillance powers.[268] Fourth, it is far from certain that the weaknesses of the system before September 11 resulted from an insufficiency of surveillance and other powers to gather information. Much of the criticism of the system, according to Congressional hearings, seems to be a lack of analysis rather than a lack of information.[269] For instance, there apparently was a large backlog of FISA intercepts that were not translated and analyzed in a timely fashion.[270] In such a setting, increased surveillance can lead, colloquially, to adding more hay to the haystack. Making the haystack bigger makes it no easier to find the needle.

4. *The need to respond in "real time."* There are at least two categories of responses to the claim that the need to respond more quickly makes "everything

---

[266] The most publicized such prevention was likely to stop the "millennium attacks" by associates of Osama bin Laden. Michael Isikoff et al., *Al Qaeda's Summer Plans*, NEWSWEEK, June 2, 2003, at 24. For a detailed recent account, see RICHARD A. CLARKE, AGAINST ALL ENEMIES 211-15 (2004).
[267] *See FISC Decision*, 218 F. Supp. 2d 611, 620-621 (Foreign Intel. Surv. Ct. 2002).
[268] *Hearing of the Senate Judiciary Committee: Oversight on Counterterrorism Efforts by the FBI*, 107th Cong. 78 (statement of Coleen Rowley) (June 6, 2002).
[269] *Hearing of the National Commission on Terrorist Attacks upon the United States, Panel IV: Governmental Organization and Domestic Intelligence*, 108th Cong. 92 (statement of John MacGaffin) (Dec. 8, 2003).
[270] House Select Homeland Security Committee, 9/11 Intelligence Report, 108th Cong. (statement of Eleanor Hill) (Sept. 10, 2003).

different" now. A factual basis for questioning whether everything has changed is the observation that the perils facing the nation feel urgent in every age. Consider the situation facing intelligence officials during the war against Hitler or in the midst of the Cuban missile crisis. In every age, it will be the rare official who says "our problems today are not very urgent, so we can use slow means for making intelligence assessments." The need for speed feels imperative in the midst of every crisis.

Fortunately, as a legal matter, FISA has always permitted emergency wiretaps.[271] Such wiretaps are now permitted if the Attorney General reasonably determines that an emergency situation requires surveillance to begin "before an order authorizing such surveillance can with due diligence be obtained."[272] An application is then made to a judge in the FISC "as soon as practicable, but not more than seventy-two hours after the Attorney General authorizes such surveillance."[273] This provision creates a legal basis for responding in real time under the current statute, with prompt judicial oversight. The number of emergency FISA orders has increased sharply since September 11. Over 170 emergency FISA orders were issued in the eighteen months after the attacks, three times the number authorized in the first twenty-three years of the statute.[274] In short, the need to respond quickly is felt imperative in every age, and the emergency FISA wiretaps provide a legal route to respond quickly.

E. Considerations Suggesting Caution in Expanding Surveillance Powers

---

[271] *See* 50 U.S.C. § 1805(f). A similar emergency provision exists for Title III wiretaps. 18 U.S.C. § 2518(7).
[272] 50 U.S.C. § 1805(f).
[273] *Id.* The time for an emergency order was extended from twenty-four to seventy-two hours in the Patriot Act, *supra* note 4, at § 314(a)(2)(B).
[274] Dan Eggen & Robert O'Harrow, Jr., *U.S. Steps Up Secret Surveillance*, WASH. POST, Mar. 23, 2003, at A1 (reporting on congressional testimony).

Before turning to proposals for reform, it is useful to discuss two considerations that suggest caution in believing that expanding surveillance powers is appropriate: the "ratcheting up" effect and the likelihood that long-term preferences for privacy protection are greater than short-term preferences.

The "ratcheting-up" effect. There are substantive and public choice reasons that lead to a "ratcheting-up," or increase, in surveillance authorities over time.[275] This racheting-up effect stems in part from the complexity of electronic surveillance law. Although this Article has focused on the differences between Title III and foreign intelligence surveillance, a complete account of wiretap and electronic surveillance law requires the description of numerous other distinctions. For instance, legal standards vary for: "wire" or "oral"versus "electronic" records; content of communications versus pen register information; "interception" of communications versus access to stored records; short-term versus long-term stored electronic communications; and so on.[276]

As a substantive matter, this complexity leads to numerous possible analogies for why surveillance powers should be expanded. We have already seen examples in the FISA context. Although the 1978 law provided only for surveillance of the content of electronic communications, Congress gradually expanded FISA to other tools commonly used in law enforcement, such as physical searches, pen register/trap and trace orders, stored records and other tangible things.[277] For each example, one can readily imagine

[275] For those of us in this electronic age who rarely work with physical machines, a "ratchet" is a device that acts in one direction only, such as where pressure is increased over time.
[276] For an overview of this complexity, see Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607 (2003).
[277] *See supra* notes 158-91and accompanying text (describing statutory expansions in the 1990s). In the Patriot Act, an example of a ratcheting up of surveillance power was the changed treatment of voice mail. Under Title III, stored voice recordings were considered "wire" communications, just like actual telephone calls. Under the Patriot Act, however, stored voice recordings were shifted to the category of "stored records," subject to easier access by law enforcement. U.S. Dept. of Justice, Computer Crime and

the policy argument—We allow these searches for ordinary crimes, even low-level drug crimes. Shouldn't we be able to have the same powers when fighting terrorism and protecting national security?[278] This "ratcheting up" effect is in addition to a more general reason why surveillance powers expand over time: intelligence agencies get part of a picture but are unable to understand the entire picture and thus seek and receive additional powers, with the hopes that the additional surveillance capabilities will be more effective at meeting the goal of preventing harm before it occurs.

The potential persuasiveness of these arguments for expansion is given greater effect due to the institutional or public choice realities of how surveillance legislation is enacted. The basic dynamic is that there are lawyers and other experts in the Justice Department and the intelligence agencies whose daily job is to work with the intricacies of the surveillance law. These professionals encounter obstacles in their daily work and develop proposed legislation to remove these obstacles. In many years these proposals for increased surveillance powers will not pass Congress due to general concerns about civil liberties. When a crisis hits, however, then there are strong pressures to "do

---

Intellectual Property Section, *Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001*, Nov. 5, 2001, *available at* http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm.

[278] One especially clear example of this form of policy argument came in the so-called "Patriot II" proposal by the Bush Administration that was leaked in early 2003. *See* Charles Lewis & Adam Mayle, *Justice Dept. Drafts Sweeping Expansion of Anti-Terrorism Act*, Feb. 7, 2003, *available at* http://www.publicintegrity.org/dtaweb/report.asp?ReportID=502&L1=10&L2=10&L3=0&L4=0&L5=0. The proposal, when leaked, was advanced enough that it had been circulated to senior officials including Speaker of the House Dennis Hastert and Vice President Richard Cheney. *Id.* Section 126 of that draft legislation is entitled "Equal Access to Consumer Credit Reports," and the draft's legislative history tried to explain that the government was seeking "equal access" to credit reports as is available to private-sector lenders. *See* Domestic Security Enhancement Act of 2003: Section-by-Section Analysis, 9, Jan. 9, 2003, *available at* http://www.publicintegrity.org/dtaweb/downloads/Story_01_020703_Doc_1.pdf. In testimony before the House Financial Services Committee, I explained a number of respects in which the government would have greater access, with fewer safeguards, than exists for the private sector. *See The Importance of the National Credit Reporting System to Consumers and the U.S. Economy: Hearing Before the H. Comm. on Fin. Svcs., Subcomm. on Fin. Institutions and Consumer Credit*, 108th Cong. 7-8 (2003), *available at*

something" to respond to the threat. At that instant, the dormant legislative proposals come out of the drawers. Legislation that would not otherwise be enacted thereby becomes law.

The clearest example of this phenomenon is the Patriot Act itself, which the Bush Administration introduced to Congress just six days after the attacks of September 11.[279] The great majority of the new surveillance provisions had been discussed within the Executive Branch and/or Congress in previous years and had not been adopted.[280] After the September 11 attacks, professional staff in the agencies simply went into their files and pulled out provisions they had been advocating previously. In the super-charged climate of the fall of 2001 many of these provisions received remarkably little scrutiny or public debate. This same pattern of suddenly enacting surveillance powers after an attack had happened before, such as in the wake of the Oklahoma City bombing.[281] In recognition of this pattern of ratcheting-up, an extra note of caution is appropriate before concluding that an additional round of broader surveillance powers is appropriate.

Short-term and long-term in privacy protection. The ratcheting-up effect is an example of a broader phenomenon in privacy law, the gap between short-term and long-term preferences. As I have previously discussed for private-sector privacy,[282] in the short run, faced with a modest advantage in convenience or cost, individuals are often

---

www.peterswire.net. This example shows both an example of a ratcheting-up argument and the need to subject such claims for "equal access" to informed scrutiny.

[279] For discussion of the timetable of consideration of the Patriot Act, see Peter P. Swire & Lauren B. Steinfeld, *Security and Privacy After September 11: The Health Care Example*, 86 MINN. L. REV. 1515, 1516-17 (2002).

[280] I personally saw many of the electronic surveillance provisions in the course of my work in 1999 until early 2001 in the Office of Management and Budget.

[281] *See supra* notes 150, 166, and accompanying text.

[282] Peter P. Swire, *Efficient Confidentiality for Privacy, Security, and Confidential Business Information*, 2003 BROOKINGS-WHARTON PAPERS ON FINANCIAL SERVICES 273, 294.

willing to disclose some of their personal information to companies.[283] In the long run, by contrast, many individuals strongly prefer a society characterized by significant privacy compared with a society characterized by pervasive disclosure and lack of privacy.[284] One indication of this long-term preference is a WALL STREET JOURNAL poll in late 1999 asking Americans what they feared most in the coming century. Among a dozen answers, such as nuclear holocaust and global terrorism, the most frequent answer was "loss of personal privacy."[285]

A similar tension exists in views towards additional surveillance. In the short-term, when asked whether they would support a specific measure to fight terrorism, many people would support the measure. Support for new security measures would be especially high in the midst of a crisis. On the other hand, especially as the crisis eases, many people would then support overall measures that reduce the risk of a Big Brother society. The "ratcheting-up" effect and the likely long-term preferences of the public for greater privacy protections fit together with the reasons developed above why "everything has likely *not* changed." They all provide reasons for skepticism about whether greater surveillance should be authorized.

VI. Proposals for Reform

In light of the discussion above of the history and structure of foreign intelligence surveillance law, we are now in the position to assess proposals for reform. Much of the discussion here will be on proposals that enhance the checks and balances in the system of foreign intelligence surveillance law. Considering such proposals is the role of

---

[283] *Id.*
[284] *Id.*
[285] Christy Harvey, *American Opinion (A Special Report): Optimism Outduels Pessimism*, WALL ST. J., Sept. 16, 1999, at A10.

Congress and others outside of the Executive Branch who seek to shape an overall system that will meet today's national security goals while also creating effective long-term ways to protect the rule of law and civil liberties.

Perhaps less obviously, proposed reforms may also strengthen the practical ability of the foreign intelligence agencies to accomplish their national security mission. The passage of FISA in 1978, for instance, regularized the use of foreign intelligence wiretaps and thus almost certainly enabled a larger number of such wiretaps than would have existed under the President's inherent authority to protect the national security. Conversely, the absence of legal standards creates the possibility that surveillance will take forms that, once exposed, lead to harsh limits on the future ability to conduct wiretaps and other information gathering. In the short-term the officials charged with running the system will rarely volunteer to subject themselves to greater oversight or stricter legal rules. In the long-term, however, a system operating under the rule of law may well be less prone to embarrassing excesses and possibly punitive reactions from Congress and the general public.[286]

The issues of reforming the system are not partisan. In thinking about what long-term system should exist, I invite the reader to consider whichever Attorney General in recent decades that the reader has trusted the least. It is well-known, for instance, that many Republicans expressed concerns about excessive Justice Department actions under Attorney General Reno, such as during the Waco incident. Many Democrats have expressed concerns about excessive surveillance by the Justice Department under Attorney General Ashcroft. Once one has that less-trusted Attorney General in mind,

[286] *See infra* notes 341-43 and accompanying text (explaining how events at the Abu Ghraib prison illustrate the long-term risks of failing to implement the rule of law).

whomever it may be, the job for system design is to create rules and institutions that will survive eight or more years of that sort of leadership. There is little need for checks and balances if one entirely trusts the Executive. The goal is a long-term system that will have checks and balances that are effective enough to survive periods of emergency or the temporary tenure of officials who seek to use excessive surveillance.

This Part will group possible reforms into five somewhat overlapping categories: (1) the practical expansion of FISA since 1978; (2) Section 215 and National Security Letter powers to get access to records and other tangible objects; (3) what to do about "the wall" between criminal and foreign intelligence investigations; (4) reforms to the Foreign Intelligence Surveillance Court system; and (5) ways to address the long-run secrecy of the FISA system. The effort here is to suggest a number of potential ways to improve the system rather than to insist that a few specific proposals are clearly desirable. Greater oversight of the system is needed, and a first use of the analysis in this article could be to assist in framing oversight inquiries. In light of the twin goals of protecting national security and upholding the rule of law, practical judgments will need to be made about which of the various reform proposals fit best together. The very significant changes since 1978, however, lead me to believe that a new set of checks and balances is almost certainly needed to replace the legal and practical limits that have fallen away over time.

A. The Practical Expansion of FISA Since 1978

A brief review of the history shows the practical expansion of FISA since 1978, and points the way to possible reforms. Without intending to idealize the situation at that time, by the late 1970s a system of interlocking safeguards existed against excessive

surveillance. The Supreme Court had recently decided *Katz*, *Berger*, and *Keith*, showing its concern for constitutional standards in law enforcement and domestic security cases.[287] The Levi Guidelines protected against intrusions into First Amendment activities.[288] At a practical level, the early version of the "wall" limited the extent to which foreign intelligence surveillance was used as a routine tool of law enforcement.[289] The vivid memory of the Watergate revelations meant that the press, the Congress, and the members of the intelligence community all knew at a personal level the problems that could arise from excessive surveillance. The level of foreign intelligence surveillance was also at a relatively small scale, with 319 applications presented in 1980.[290]

The situation today is quite different. In the federal courts, the 2002 FISCR decision suggests few constitutional limits on FISA surveillance (although I believe that strong constitutional arguments exist against that decision).[291] The Levi Guidelines have given way to the 2002 Ashcroft Guidelines, which far more aggressively contemplate surveillance of First Amendment activities in the name of domestic security. The "wall" has come down entirely, to the extent that prosecutors can direct and control investigations that use FISA surveillance.[292] The memories of the 1970s have faded, with many veterans of that period having retired and with the pressing emergency of Al Qaeda seeming to many to make that history inapposite. The number of FISA applications jumped to 1228 in 2002, and Attorney General Ashcroft has announced his intension to

---

[287] *See supra* notes 21-26, 227-42 and accompanying text.
[288] *See supra* notes 131-34 and accompanying text.
[289] *See supra* notes 210-11 and accompanying text.
[290] *See* Electronic Privacy Information Center, *Foreign Intelligence Surveillance Act Orders 1979-2002*, *available at* http://www.epic.org/privacy/wiretap/stats/fisa_stats.html (giving annual statistics of FISA orders).
[291] *See supra* notes 212-21 and accompanying text.
[292] *See supra* notes 192-99 and accompanying text.

use FISA powers extensively in law enforcement actions.[293] The extension of FISA to any documents or tangible objects, and the accompanying rules preventing public disclosure of such searches, creates a legal structure for thoroughgoing secret surveillance of many domestic activities. In short, the extraordinary power of the President and Attorney General to conduct "national security" surveillance has become far more routine.

1. *Expand reporting on FISA surveillance.* One response to the known expansion of FISA surveillance is to seek greater Congressional and perhaps public knowledge of the scope of FISA activities by increasing the reporting requirements. The logic behind increased reporting is that greater oversight is needed where there is increased surveillance and potential infringement of civil liberties.

The current level of FISA reporting is considerably less than exists for Title III wiretaps or pen register and trap-and-trace orders.[294] For FISA, the public reports only give the annual number of applications made for electronic surveillance and the number of such orders granted, modified, or denied.[295] The Attorney General also reports semiannually to The House and Senate Intelligence Committees with a description of "each criminal case in which information acquired under [FISA] has been passed for law

---

[293] *Id.* Attorney General Ashcroft, in commenting on the FISCR decision, said, "The Court of Review's action revolutionizes our ability to investigate terrorists and prosecute terrorist acts." Department of Justice, *Attorney General Ashcroft News Conference Transcript regarding Decision of Foreign Intelligence Surveillance Court of Review*, Nov. 18, 2002, *available at* http://www.usdoj.gov/ag/speeches/2002/111802fisanewsconference.htm. The Attorney General said the FBI "will double the number of attorneys working in its National Security Law Unit to handle FISA applications" and he directed "each U.S. attorney's office [to] designate at least one prosecutor to be a point of contact for purposes of" FISA.

[294] *See supra* notes 187-88 and accompanying text.

[295] 50 U.S.C. § 1807.

enforcement purposes" and for "each criminal case in which information acquired under [FISA] has been authorized for use at trial."[296]

Greater reporting is required for pen register and trap-and-trace orders, which target to/from information such as the telephone numbers a person calls. These reports include the number of investigations involved, the offense specified in the order or application, and the identity of the applying investigative or law enforcement agency.[297]

Even more detailed reporting is required for Title III orders, which target the content of communications and are thus more intrusive than pen register orders. For each order, the judge submits a report to the Administrative Office of the United States Courts that includes: the fact the order was applied for; whether the order was granted, modified, or denied; the period of interceptions authorized as well as any extensions; the offense specified in the order; the identify of the applying officer and agency as well as the person authorizing the application; and the nature of the facilities from which communications were to be intercepted.[298] Annually, the Attorney General must make an additional report to the Administrative Office of the United States Courts. This report includes the information submitted by the judges as well as a general description of the interceptions made under an order. The general description is supposed to include: the approximate nature and frequency of incriminating communications intercepted; the approximate nature and frequency of other communications intercepted; the approximate

---

[296] *Id.* § 1808(a)(2).

[297] In full, the annual reports for pen register and trap-and-trace orders provide:

> (1) the period of interceptions authorized by the order, and the number and duration of any extensions of the order; (2) the offense specified in the order or application, or extension of an order; (3) the number of investigations involved; (4) the number and nature of the facilities affected; and (5) the identity, including district, of the applying investigative or law enforcement agency making the application and the person authorizing the order.

18 U.S.C. § 3126.

[298] *Id.* § 2519(1).

number of persons whose communications were intercepted; the number of orders in which encryption was encountered and whether such encryption foiled the investigation; and the approximate nature and cost of the manpower and other resources used in the interceptions.[299] The Attorney General is also supposed to report on: the number of arrests resulting from interceptions; the offenses for which arrests were made; the number of trials resulting from such interceptions; statistics on motions to suppress; and the number of convictions resulting from such interceptions.[300] The Administrative Office of U.S. Courts releases an annual report that gives statistics on the number of orders as well as a summary and analysis of the detailed data provided by judges and prosecutors.[301]

The more detailed reporting available on Title III orders may prove a useful model for expanded reporting for FISA orders. There are conflicting intuitions on whether greater reporting is appropriate for FISA. On the one hand, there is the tradition of secrecy for foreign intelligence activities. More detailed reporting might reveal the advanced sources and methods deployed for the most sensitive foreign intelligence investigations. It might also allow inferences about the level of surveillance of embassies and embassy personnel, potentially leading to diplomatic embarrassment. On the other hand, statistical reports about Title III are less important because the target of the surveillance learns about the wiretap after it is ended. With a FISA order, that individualized notice of the nature of the surveillance is absent, and systemic reporting thus becomes more important. Without systemic reporting, it will be difficult to learn if the extraordinary powers of FISA are being used in new and potentially disturbing ways.

---

[299] *Id.* § 2519(2)(b).
[300] *Id.* § 2519(2)(c)-(g).
[301] The annual reports are available at Administrative Office of the United States Courts, http://www.uscourts.gov/wiretap.html.

My own judgment on additional reporting is that the topic should at least be the subject of Congressional attention and oversight. The reporting used for pen registers and Title III provides a useful list of candidates for additional FISA reporting. Some categories of reporting could be made available to the public, while more sensitive categories of information might be supplied only to Congress. The strongest case for additional public reporting may be for criminal prosecutions that result from FISA orders. In such instances, defendants face unique difficulties in presenting their cases, likely including the inability to examine the surveillance tapes and other evidence used against them. There is thus special reason to keep the general public informed about the scope of FISA prosecutions.

2. *Defining "agent of a foreign power."* Comments I have heard in public from knowledgeable persons suggest that there has been ongoing expansion of who is considered an "agent of a foreign power."[302] Consider an individual who works in the United States for the Cali drug cartel. Is that person an "agent of a foreign power?" The Cali cartel is a highly organized group that physically controls a substantial amount of territory in Colombia.[303] Given these facts, one might well argue that the Cali cartel is more of a "foreign power" than the amorphous Al Qaeda network. If one accepts the Cali cartel as a "foreign power," and a major smuggler as an "agent of a foreign power," would a street-level cocaine dealer also qualify as its agent? There is no clear line in the statute stating that the dealer would not be so considered. To take another example, what about the activities of the so-called "Russian mafia?" Many organized crime groups have

[302] The definition of "agent of a foreign power" is given at 50 U.S.C. § 1801; *see supra* notes 91-92, 96-97 and accompanying text (discussing "agent of a foreign power").
[303] *See* CarrieLyn Donigan Guymon, *International Legal Mechanisms for Combating Transnational Organized Crime: The Need for a Multilateral Convention*, 18 BERKELEY J. INT'L L. 53, 59 (2000).

links to overseas operations. How small can the links back home be to still qualify that group's actions as on behalf of a foreign power?

These examples, it turns out, go to the heart of whether Title III will continue to be a significant part of the overall American system of electronic surveillance. The threat of organized crime was a principal justification in 1968 for the extraordinary intrusion of performing wiretaps under Title III.[304] Over time, narcotics and organized crime cases have constituted the vast bulk of federal Title III wiretaps. In 2002, for instance, narcotics cases numbered 406 (81%) and racketeering cases fifty-nine (12%) of the 497 total federal wiretaps.[305] Yet an expansion of the definition of "agent of a foreign power" could render Title III wiretaps almost obsolete. Many heroin, cocaine, and other drug cases are linked to imported narcotics. Many organized crime cases in this era of globalization have significant links to overseas activities. FISA orders already outnumbered Title III orders in 2003.[306] If most drug cases and organized crime cases shift to the secret world of FISA, then the constitutional teachings of *Katz* and *Berger* may have little effect.

In debates about U.S. wiretap law there is often an implicit assumption that Title III wiretaps are the "normal" means of surveillance, with FISA orders as an exception used for embassies and other foreign intelligence functions. The available statistics, though, show that in 2002 the federal government secured 497 Title III orders compared

---

[304] S. REP. NO. 90-1097, 1968 U.S.C.C.A.N. 2112, 2153-2163. "The major purpose of Title III is to combat organized crime" *Id.* at 2153

[305] Administrative Office of the United States Courts, *2002 Wiretap Report*, at Table III, *available at* http://www.uscourts.gov/wiretap02/contents.html. The comparable figures for 1998 were 458 (81%) narcotics and fifty-eight (10%) racketeering cases out of 566 orders. Administrative Office of the United States Courts, *1998 Wiretap Report*, at Table III *available at* http://www.uscourts.gov/wiretap98/contents.html.

[306] *See supra* note 9.

to 1228 FISA orders.[307] Title III orders were thus only 28.8% of the total for that year. One cannot tell from publicly available information how far the government is already going toward using FISA orders for narcotics and organized crime investigations within the United States. It is possible that many such cases already use FISA orders. It is also possible that an expanded definition of "agent of a foreign power" will mean that more such cases will be handled under FISA in the future. Because of the lesser constitutional and statutory protections existing in FISA investigations, Congress should use its oversight powers to learn more about the contours of what it takes for someone to be considered an "agent of a foreign power."

If this oversight shows that "ordinary" drug and organized crime cases are becoming foreign intelligence cases, then various reforms may be appropriate. One approach would be to require reporting concerning whether a Title III order would have been available for the investigation. A stricter step would be to introduce a prohibition on FISA use where Title III would suffice. A different approach would be to tighten the definition of "agent of a foreign power" to delineate when ordinary constitutional and Title III requirements would apply. In the absence of public knowledge about how the definition of "agent of a foreign power" is now interpreted, however, it is difficult to know what reforms, if any, are appropriate.

B. Section 215 and National Security Letter Powers to Get Records and Other Tangible Objects.

The Patriot Act substantially expanded the government power to obtain records and other tangible objects through Section 215 and National Security Letters. The expanded scope of these powers is controversial for two distinct reasons—the potentially

[307] 2002 Wiretap Report, *supra* note 305, at tbl. III; Electronic Privacy Information Center, *supra*, note 118.

routine use of foreign intelligence powers to seize any records and the "gag rule" that makes it a federal crime for the holder of the record to tell anyone, even the press, about the seizure.

1. *Expanding the use of National Security Letters.* As discussed above,[308] NSLs were expanded in Section 505 of the Patriot Act in the following ways: they no longer are limited to counter-intelligence operations; the relatively strict requirement of "specific and articulable facts" that the information pertain to an agent of a foreign power was lowered to the looser "relevant to an investigation" standard; records about persons other than agents of foreign powers are thus now subject to NSLs; and a Special Agent in Charge of an FBI branch office can authorize the NSL, rather than requiring approval from a more senior official at FBI headquarters. As discussed further below, NSLs also are subject to the "gag rule" prohibiting disclosure of the fact of the NSL by the record-holder.[309]

From the perspective of checks and balances, these expansions of NSLs leave many gaps. Most prominently, NSLs are implemented without judicial supervision. That lack of supervision, combined with the possibility of issuing an NSL without approval by FBI headquarters, creates the possibility of excessive surveillance by field offices. There appears to be no current statutory requirements of any record-keeping about the use of NSLs. For example, there is no reporting of the annual number of NSLs in the yearly FISA reports to Congress. To address these concerns, possible reforms of the NSL authority are discussed in the next section, together with the Section 215 provisions on record searches.

---

[308] *See supra* notes 1777-186 and accompanying text.
[309] *See supra* note 324 and accompanying text.

2. *Using FISA to obtain records and other tangible objects.* As discussed above,[310] the Patriot Act expanded the scope of FISA orders to records in important ways: the order can extend beyond travel records to "any tangible things (including books, records, papers, documents, and other items)"; the legal standard was lowered to merely being part of "an authorized investigation"; and the records may be those of any person, rather than requiring "specific and articulable facts that the person to whom the records pertain is a foreign power or an agent of a foreign power."[311] One consequence of the statutory change is the apparent permission of a FISA order to encompass entire databases, rather than the specific records of the target of an investigation.

Section 215 has drawn the greatest attention due to the law's potential to obtain library records.[312] The library records controversy is significant in its own right as a debate about whether government should have access at all to First Amendment materials. Government surveillance of reading smacks of the Thought Police and the worst fears of Big Brother government. Standard First Amendment jurisprudence recognizes the chilling effect on expression and political activity that can result from such surveillance.[313] One specific reform proposal, therefore, would be to exempt library records from the scope of Section 215.

The library records controversy is even more important because the same rules apply under Section 215 to library and all other records. Section 215 appears to override a wide array of existing laws that limit government access to personal information. For

---

[310] *See supra* notes 165-76 and accompanying text.
[311] *See* 50 U.S.C. § 501.
[312] *See generally* Kathryn Martin, Note, *The USA Patriot Act's Application to Library Patron Records*, 29 J. LEGIS. 283 (2003). Attorney General Ashcroft criticized the American Library Association and others for "baseless hysteria" about the government's ability to pry into the public's reading habits. Eric Lichtblau, *Ashcroft Mocks Librarians and Others Who Oppose Part of Counterterrorism Law*, N.Y. TIMES, Sept. 16, 2003, at A23.

example, existing procedures govern government access to medical records,[314] financial records,[315] and many other categories of records.[316] The medical privacy rule specifically allows disclosure to the government for intelligence investigations and for reasons of national security,[317] and the financial privacy laws allow delay of notice to the target of an investigation upon proper showings.[318] These procedures were crafted after attention to the special sensitivity and other characteristics of each category of record. Section 215, by contrast, is a blunt instrument that allows a single order to give access to all records that the government seeks as part of an investigation.

In response to public concern about use of Section 215 to gather library records, Attorney General Ashcroft reported in September, 2003 that the section had never been used since passage of the Patriot Act for library or any other records.[319] This lack of usage is reassuring because it shows that the Justice Department has not been using the new power for routine surveillance of library and other sensitive records. The lack of usage also supports the position that the Justice Department has not made the case for renewing Section 215 when the sunset expires. There are existing procedures for gathering records without using the extraordinary scope of Section 215. Absent some new showing by the Justice Department of the specific circumstances where Section 215 is needed, the provision should be allowed to sunset.

---

[313] *See* id. at 291.
[314] *See* Swire & Steinfeld, *supra* note 279, at 1516-17 (discussing national security and law enforcement aspects of the federal medical privacy regulation in the wake of the Patriot Act).
[315] *See* Right to Financial Privacy Act, 12 U.S.C. § 3401 et seq. (definitions).
[316] For one collection of U.S. privacy statutes, including the provisions for government access to records, see http://www.peterswire.net/pspriv.html.
[317] 45 C.F.R. § 164.512(k) (2002).
[318] 12 U.S.C. § 3409.
[319] A memorandum from Attorney General Ashcroft to FBI Director Mueller on the subject was released to the press on September 18, 2003, *available at* http://www.cdt.org/security/usapatriot/030918doj.shtml.

It is possible that the explanation for the lack of use of Section 215 has been the expanded use of NSLs. NSLs are narrower in scope than Section 215 orders, because NSLs only apply to specified communications and financial records.[320] NSLs are more worrisome from a civil liberties perspective, however, because of the lack of the judicial supervision that exists with a Section 215 order.[321] Oversight is appropriate for NSLs and Section 215 orders together, in order to determine what factual settings are fitted to each tool. At a minimum, there should be reporting on the use of NSLs and Section 215, as has been suggested already in Congress.[322]

In terms of other possible reforms, probing questions are appropriate to determine whether and in what circumstances NSLs and Section 215 orders are necessary at all. If the decision to keep some form of NSLs and Section 215 is made, however, then there are various reforms that would cabin some of the most disturbing aspects. For instance, there could be a specific carve-out from Section 215 for library records. There could be deference to the medical, financial, and other privacy laws on the books, so that the specific statutes would govern categories of records rather than using the lower standard of Section 215. Next, the standard for NSLs and Section 215 could return to the "specific and articulable facts" standard that existed before 2001, rather than leaving unchecked access to records that simply are part of an investigation. In addition, there could be minimization rules to assure the FISC that only records reasonably necessary to an investigation are sought by the government, rather than all records held by a library or other organization. In crafting minimization rules, possible procedures and promising

---

[320] *See supra* notes 177-86 and accompanying text.
[321] Id.
[322] For instance, Senators Leahy, Grassley, and Spector have sponsored S. 436 in the 108th Congress to require such reporting. *See* S. 436, 108th Cong. (2003).

new technologies could allow government access to the target's documents without turning over the entire database to the government[323]

The overarching concern with NSLs and Section 215 orders is the legal authorization for dragnets of entire databases. These searches can remain secret because notice is never given after the fact, and because the "gag rule" prevents the record-holders from revealing the existence or scope of the searches. Section 215 sunsets in 2005 but the expanded NSL powers do not. The nature and uses of these two provisions deserves careful attention in any Patriot Act reauthorization.

3. *The unjustified expansion of the "gag rule".* An especially troubling aspect of NSLs and Section 215 is the provision that makes it illegal for individuals or organizations to reveal that they have been asked by the government to provide documents or other tangible objects.[324] It appears that the law makes it criminal for a librarian or other person even to say that there has been a FISA request, without saying more about the nature of the request or the name of the target. This "gag rule" is an unjustified expansion of a special rule for wiretaps, and is contrary to the rules that have historically applied to government requests for records.

There has long been a specialized rule for wiretaps, under both Title III and FISA, that the telephone company and others who implement the wiretap are required to keep

---

[323] For example, there could be a minimization procedure where one team could look at the raw data and perform minimization while another team could keep the data for ongoing analysis. The FISC itself might also act as a rulemaker for the orders that come before it, specifying minimization rules just as federal courts play a role in drafting the rules of criminal and civil procedure and the rules of evidence.

A better solution may be to use new technologies that can use cryptographic tools to protect privacy while allowing limited sharing of information upon a proper showing of need. For a joint report on this topic by the Center for Democracy and Technology and the Heritage Foundation, see James X. Dempsey & Paul Rosenzweig, "Technologies That Can Protect Privacy as Information is Shared to Combat Terrorism," May 26, 2004, *available at* http://www.cdt.org/security/usapatriot/20040526technologies.pdf.

[324] 50 U.S.C.A. § 1861(d).

the wiretap secret while it is in operation.[325] The need for secrecy flows specifically from the recognition that the ongoing usefulness of the wiretap will disappear if its existence becomes known. Indeed, the special nature of ongoing surveillance is the primary reason why the Supreme Court exempted law enforcement wiretaps from the prior notice requirement of the Fourth Amendment, subject to the strict requirement of notice to the target after the wiretap is concluded.[326]

This secrecy requirement for those implementing the wiretap is entirely different than the legal rules that apply to ordinary government investigations. Suppose that a landlord is interviewed by police about the whereabouts of a tenant or a company is asked for records about its sales to a particular individual. The American approach in such instances is that the landlord or the company is permitted to talk about the investigation with the press or other persons. This ability to speak to the press or others is an important First Amendment right. Under the "gag rule" approach, that right is taken away and individuals subject to excessive searches must risk criminal sanctions even to report over-reaching or abuses of government authority.

The general American approach also places key limits on what a landlord or company may say. If a landlord tips off a tenant that the police are trying to catch the tenant, then the landlord is subject to punishment under obstruction of justice or similar statutes. This kind of targeted criminal sanction permits citizens to keep watch on possible over-reaching by the government, while also empowering the government to punish those who assist in criminal activity.

---

[325] 18 U.S.C. § 2511(2)(a)(ii).
[326] Katz v. United States, 389 U.S. 347, 355 n.16 (1967) (internal citations omitted).

The furor about FISA access to library and other records is based in part on the recognition that this sort of broad search power could expand over time into a routine practice of intrusive domestic surveillance. The combination of this essentially unlimited search power with the "gag rule" means that the most basic check against abuse—publicity—is removed. Similar "gag rules" have recently spread into other statutes.[327] Instead of multiplying these suppressions on speech, a far better approach is to have a focused inquiry on whether there are gaps in the obstruction of justice or similar laws. My recommendation is that the special circumstances that justify the "gag rule" for ongoing wiretaps do not apply to records searches such as those under Section 215 and the NSLs. Records searches are not typically ongoing in the same way as wiretaps, and they generally do not involve the sources and methods that have been so important to surreptitious electronic surveillance. Agents who make the records request can inform the record holder about obstruction of justice and other potentially relevant statutes. The law should be generally clear, however, that disclosure is permitted absent the special circumstances of assisting the targets of investigation.[328]

If that recommendation is not adopted, however, then there are measures that can reduce the risk of ongoing, extensive, and secret searches of records held in the private sector. For instance, there could be a six month time limit on the prohibition on

[327] *See* Homeland Security Act of 2002, Pub. L. No. 107-296, § 212(5), 116 Stat. 2135; *see also* GINA MARIE STEVENS, CONG. RESEARCH SERV., HOMELAND SECURITY ACT OF 2002: CRITICAL INFRASTRUCTURE INFORMATION ACT 12-13 (2003), http://www.fas.org/sgp/crs/RL31762.pdf (explaining the intersection of the Homeland Security Act's prohibition on disclosures by federal employees and the Whistleblower Protection Act).

[328] In crafting changes to the scope of the "gag rule," attention should be paid to the broad definition of "material support or resources" used in 18 U.S.C. § 2339A and §2339B. Parts of the statute were struck down as unconstitutionally void for vagueness in *Humanitarian Law Project v. Ashcroft*, 309 F. Supp. 2d 1185, 1198-1201 (C.D. Cal. 2004). The general prohibition against material assistance to terrorism, however, is analogous to the crime of obstruction of justice in the sense that impeding the terrorist investigation can give rise to criminal prosecution. Further study is likely needed to determine the extent to

disclosure, subject to a request to the FISC that a longer duration is necessary. This approach would be especially easy to understand and administer. There could be rules about the scope of disclosure, with permission perhaps to report the mere existence of a request without authorization to disclose the nature of the request. That approach could calm the concerns expressed by librarians, for instance, that they could -not even report to the American Library Association the number of requests that had been made. Similarly, disclosure might be permitted where the record holder reasonably believes that the disclosure would not reveal information detailed enough to materially assist the targets of an investigation. That approach might permit a large telephone company or Internet Service Provider, for instance, to reveal the number and type of searches without tipping off any targets that they had been the subject of an investigation.[329]

C. What To Do About "The Wall"?

Much of the recent FISA debate has concerned the extent to which "the wall" should exist between foreign intelligence and law enforcement investigations.[330] The discussion explains the contrasting positions, shows the dilemma they pose, and proposes a different statutory approach to resolve the dilemma.

1. *The logic of the conflicting positions.* There is great fervor and strong logic on both sides of the debate. Those who want maximum coordination of foreign intelligence and law enforcement stress four arguments. First, the sort of terrorism, espionage, and sabotage detected in foreign intelligence investigations are themselves often crimes, and

---

which the material assistance crime would adequate address the concerns of those who are inclined to support the "gag rule."

[329] These additional suggestions are offered as modest safeguards if the "gag rule" is maintained, rather than as affirmatively desirable proposals.

[330] *Hearing of the Senate Judiciary Committee: War Against Terrorism*, 108th Cong. 92 (statement of Attorney General John Ashcroft), Mar. 4, 2003 (advocating that "the wall" no longer exist).

it frustrates the basic mission of law enforcement to prevent this evidence from being used in criminal prosecutions. Second, prosecution for crimes can lead to arrest and imprisonment. This incapacitation is a powerful tool to disrupt ongoing terrorist operations. Third, the original FISA in 1978 included procedures for using FISA information in criminal cases, so there is historical precedent for information sharing. Finally, the events leading up to September 11, and especially the failure to find and use the information in Moussaoui's computer, show the urgent need to share information promptly between foreign intelligence and law enforcement investigations.

The principal argument on the other side is that criminal prosecutions should be based on the normal rules of criminal procedure, not on evidence gathered in a secret court system. The norm should be the usual constitutional protections rather than the exceptional circumstances that arise in foreign intelligence investigations. Notably, the Fourth Amendment creates a baseline where targets of investigations should receive notice of government searches, either at the time of the search or as soon as practicable afterwards in the case of wiretaps. The Sixth Amendment creates a norm that defendants should confront the witnesses and evidence against them, yet the FISA procedures limit defendants' ability to cross-examine the evidence. The First Amendment should provide assurances of freedom of thought and of the press, without the chilling effect of having "an FBI agent behind every mailbox."[331]

From this perspective, "the wall" serves essential purposes. First, despite the FISCR's holding to the contrary, removal of "the wall" may violate the Constitution for investigations that are primarily not for foreign intelligence purposes. At some point an investigation is so thoroughly domestic and criminal that the usual Fourth Amendment

and other protections apply. Future review in other courts may find that investigations that are not primarily for foreign intelligence purposes do trigger constitutional protections. Second, "the wall" may be important in preventing the spread of the secret FISA system over time. As of 2002, 71% of the federal electronic surveillance orders were FISA orders rather than Title III orders.[332] The Patriot Act reduction of safeguards in the FISA system means that this figure may climb in the future.

Third, ongoing expansion of the definition of "agent of a foreign power" may mean that an ever-increasing proportion of investigations might be shoe-horned into the FISA formula. This shift may exist due to a general trend toward transnational relationships in an era of globalization. It may also exist under pressure to authorize FISA orders even in the case of slight and speculative links to Al Qaeda or other terrorist organizations. Fourth, the history described in Part I above shows the risks of abuse that come with an expanding, secretive system of surveillance that is justified by national security and the fear of subversion. In short, the concern is that the American system of the Bill of Rights can become a secret surveillance system where defendants do not learn of the surveillance and do not confront the evidence against them.

2. *Framing the current dilemma.* The conflicting positions create an apparent dilemma – "the wall" is necessary to avoid the slippery slope into a pervasive secret surveillance system, but "the wall" prevents necessary coordination of law enforcement and foreign intelligence in the war against terrorism. A particular problem is that, early in an investigation, it may be difficult or impossible for investigators to know whether the evidence will eventually be used for intelligence purposes or else in an actual

---

[331] *See supra* note 78.
[332] *See supra* notes 1533-55.

prosecution. For instance, imagine that a FISA wiretap is sought for a group of foreign agents who are planning a bomb attack. On these facts, there would be a strong foreign intelligence purpose, to frustrate the foreign attack. In addition, there would be a strong law enforcement basis for surveillance, to create evidence that would prove conspiracy beyond a reasonable doubt. On these facts, it would be difficult for officials to certify honestly that "the primary purpose" of the surveillance was for foreign intelligence rather than law enforcement. The honest official might say that the surveillance has a dual use – both to create actionable foreign intelligence information and to create evidence for later prosecution.

Faced with this possibility of dual use, the Patriot Act amendment was to require only that "a significant purpose" of the surveillance be for foreign intelligence. Under the new standard, an official could honestly affirm both a significant purpose for foreign intelligence and a likely use for law enforcement. The problem with the "significant purpose" standard, however, is that it allows too much use of secret FISA surveillance for ordinary crimes. The FISCR interpreted the new statute in a broad way: "So long as the government entertains a realistic option of dealing with the agent other than through criminal prosecution, it satisfies the significant purpose test."[333] The range of "realistic options" would seem to be so broad, however, that FISA orders could issue for an enormous range of investigations that ordinarily would be handled in the criminal system. For instance, "realistic options" for investigators would include: continued surveillance

[333] *FISCR Decision*, at 735. *See also supra* notes 21212-33 and accompanying text (critiquing FISCR decision). The FISCR also said that the government need show "a measurable foreign intelligence purpose, other than just criminal prosecution of even foreign intelligence crimes." *FISCR Decision*, at 735. These easy showings of "significant purpose" would seem to ignore the decision by Congress to raise the Bush Administration's proposed language of "a purpose" up to what would have seemed to be the stricter test of a "significant purpose." *See supra* notes 160-64 and accompanying text.

of the target; using surveillance of this target to learn more about possible associates; and efforts to "turn" the target into an informer. These techniques are the bread and butter of criminal law enforcement. Under the language of the FISCR opinion, any of these "realistic options" would appear to be enough to justify a FISA order. The Patriot Act amendment, as interpreted by the FISCR, thus allows the slippery slope to occur. A potentially immense range of law enforcement surveillance could shift into the secret FISA system.

3. Resolving the dilemma by focusing on the foreign intelligence value of the surveillance. To resolve the dilemma, the proposal here is to focus on the appropriateness of an application as a foreign intelligence investigation, rather than seeking to measure the amount of dual use for law enforcement purposes. The essential goal is to issue FISA orders when they are "worth it" for foreign intelligence purposes. The previous approaches, based on "primary" or "significant" purpose, suffer the defect that it is difficult to guess at the beginning of an investigation whether a FISA order will result in evidence of a crime, foreign intelligence information, or both. The better approach is to ask those seeking the FISA order to certify that the extraordinary, secret surveillance order be used where there is a significant foreign intelligence reason for the order.

To achieve this goal, some new statutory language would need to be added to FISA. Under current law, an order may issue where there is probable cause that the person surveilled is an "agent of a foreign power."[334] As discussed above,[335] this standard has become too minimal in today's transnational environment, where the term

[334] 50 U.S.C. § 1801 (2000).
[335] *See supra* notes 302-06 and accompanying text.

"foreign power" can apply to so many non-state actors and where "agent of a foreign power" might extend to a large fraction of drug dealers, organized crime members, and other common criminals. Simply retaining the "significant purpose" test would allow the slippery slope to occur, making it too easy for secret FISA surveillance to become the norm for law enforcement investigations within the United States.

The missing legislative piece is a requirement within FISA that the surveillance be: (1) important enough and (2) justifiable on foreign intelligence grounds. Under Title III, the "important enough" element is built into the statute, notably by the requirement that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous."[336] The FISA equivalent is considerably looser, with the application requiring only a certification "that such information cannot reasonably be obtained by normal investigative techniques."[337] The flaw in this current FISA language is that it allows the slippery slope to occur. A prosecutor investigating a domestic crime can apply for a FISA order if a wiretap will produce information not reasonably available by normal investigative techniques and if the prosecutor can meet the easy standard of "probable cause" that the target is "an agent of a foreign power."

The proposal here, then, is to amend FISA to include a requirement that an application certify that "the information sought is expected to be sufficiently important for foreign intelligence purposes to justify" the initial (and any subsequent) FISA order. In order to keep FISA focused on foreign intelligence surveillance, the usefulness for foreign intelligence purposes would be measured regardless of the usefulness for law

[336] 18 U.S.C. § 2518(3)(C). *See supra* 100-24 and accompanying text (comparing Title III and FISA legal requirements).

enforcement purposes. Three scenarios illustrate the usefulness of the proposed amendment. First, surveillance of a foreign embassy or employees of that embassy would fit within the proposed amendment – the foreign intelligence purposes of watching potential spies in the United States is obvious. Second, the surveillance of suspected Al Qaeda operatives would also meet the test. There are strong foreign intelligence reasons to learn about suspected terrorists. Even if the investigation eventually leads to criminal prosecution, this surveillance is justifiable on foreign intelligence grounds. Third, the use of FISA against drug dealers (potential agents of the Cali cartel) or organized crime mobsters (potential agents of the Russian mafia) would likely be blocked by the FISA amendment. Even if these individuals are considered "agents of a foreign power," it will be difficult to convince the FISC judges that this surveillance is "sufficiently important for foreign intelligence purposes" to justify a FISA order. The amendment proposed here would provide the FISC judges a basis for telling the Justice Department to seek a Title III order if a wiretap is needed.

The proposal here adopts the spirit but not the letter of the "primary purpose" test that existed until the Patriot Act. The spirit of that test, in my view, was to assure that the extraordinary FISA procedures be used only where investigator were seeking to advance foreign intelligence goals. The problem with the letter of the earlier language, however, was that "the wall" sometimes made it too difficult to share information based on the happenstance that investigators might eventually decide that the best way to handle the threat posed by a foreign agent was through prosecution The proposal here does not prohibit a prosecutor or FBI agent from directing or controlling an investigation, so long as that investigation has the requisite importance for foreign intelligence.

---

[337] 50 U.S.C. § 1804(7)(C).

Another virtue of the proposal here is that it can be used when the government seeks to renew or extend a surveillance order. Suppose that an investigation at first seems to be promising in terms of producing foreign intelligence information. The order might result in information that is helpful purely for law enforcement but where there is little prospect of useful foreign intelligence information. In such an instance, any future wiretap order would appropriately issue under Title III rather than staying in the FISA system.

D. Improved Procedures for the Foreign Intelligence Surveillance Court System.

Experience with the FISA system since 1978, and especially lessons from the FISC and FISCR reported decisions, provides the basis for suggesting reforms for the procedures for handling FISA orders and the use of FISA information in the criminal system.

1. *More of an adversarial system in the FISC.* The details of FISC procedures are not publicly available. Department of Justice officials seeking FISA orders present documents to the FISC judges. Members of the Department's Office of Intelligence Policy and Review serve certain staff functions for the Court. There is no adversarial process, however, and no one is specifically tasked with critiquing the order as it is sought.

Especially as FISA orders are used more aggressively as a means to create evidence for criminal trials, this lack of adversariness becomes more problematic. Congress may thus wish to authorize specifically the creation of a "Team B" or "devil's advocate" role within the FISC process. As a related possibility, the statute might

specifically authorize the FISC judges to ask for that sort of representation in a particular case where they believe it would assist the Court. The devil's advocate would presumably have gone through full security clearance. For instance, the advocate might serve for a period of years and then return to other functions within the Department of Justice. Oversight could be available after the fact to determine the extent to which this innovation has proved helpful.

2. *Adversary counsel in FISCR appeals.* The first case appealed to the FISCR showed a clear gap in existing procedures. Amici were permitted by the Court to submit briefs. There was no statutory mechanism, however, that permitted amici or any party opposing the government to participate in an oral argument. Important proceedings at the Court of Appeals level deserve the possibility of oral argument. Even if some or all of the oral argument of the Department of Justice is closed for security reasons, there can be a separate session involving amici or other parties. In addition, where amici or other parties are represented by persons with security clearances, then the FISCR might decide to include cleared counsel into the entire argument.

3. *Possible certification to the FISC in criminal cases.* The published FISC opinion provides a picture of that court as developing considerable experience in foreign intelligence matters and considerable awareness of the quality of the evidence being presented before it. It makes sense going forward to take greater advantage of the expertise in the FISC as an institutional way to assure sound decisionmaking on a daily basis.

One new role for the FISC could be to review the evidence in cases where a district judge today faces a motion to suppress information deriving from a FISA order.

It may be difficult for a district court judge, who may never have seen a FISA case before, to assess the extent to which proper procedures were followed in developing evidence in a particular criminal case. One idea for reform would be to permit that district judge, sua sponte or on a motion by defense counsel, to certify the question to the FISC. The FISC could then make a more informed ruling on the suppression motion, drawing on its experience in the original granting of that particular FISA order and on its experience across the broad range of FISA cases. One advantage of this procedure is that the FISC could compare the representations made to it at the stage of issuing the FISA order with the way that the investigation actually worked out in a criminal prosecution. If there were misrepresentations in the original FISA application, as happened in the over seventy-five cases referred to in the FISC opinion,[338] then the FISC judges would be in a position to detect the problem.

4. *Create a statutory basis for minimization and other rulemaking by the FISC.* Article III courts, as part of their inherent authority, play a central role in defining the rules that affect the necessary operations of the courts. Notably, Article III judges play an important role in defining the Federal Rules of Civil Procedure, the Federal Rules of Criminal Procedure, the Federal Rules of Evidence, and the rules applying to contempt of court.[339] It is interesting to consider the extent to which the Article III judges in the FISC should be understood, as a constitutional matter, to have inherent authority to set forth analogous rules for how they implement their judicial role in the FISC. The FISC judges may not wish, as a matter of prudence, to make such a claim. Nonetheless, Congress can

[338] *See FISC Decision*, 218 F. Supp. 2d 611, 620 (Foreign Intel. Surv. Ct. 2002).
[339] The methods for creating rules are set forth in the Rules Enabling Act. 28 U.S.C. §§ 2071-2077 (2000). For information on the drafting of the federal rules of procedure and evidence, see the collection of materials maintained by the Administrative Office of the United States Courts, *available at*

consider the extent to which the FISC judges, based on their existing role in the FISA process and their accumulated expertise in foreign intelligence surveillance, should have rulemaking and related supervisory powers over how the FISC operates.

An especially important example of such possible rulemaking would be in the area of minimization. That was the topic of the opinion that the FISC made public—a concern by the judges that the statutory requirement that surveillance be minimized was not being met in practice. The lack of minimization may be a large problem going forward, especially if "the wall" stays down completely and NSLs and Section 215 orders permit access to entire databases of records. There is thus a long-run concern that secret FISA orders will be used expansively to intrude into an array of domestic matters. Having enforced minimization procedures is a long-established way to focus the surveillance on where it is justified, but not to have open-ended surveillance.

Creation of minimization or other FISC court rules might build on procedures analogous to those used for the federal rules of procedure and evidence. Judges could draft rules subject to comment by the Department of Justice. To the extent possible, the public could comment as well. The rules could actually be implemented after consideration in Congress.

E. Additional Oversight Mechanisms.

The reforms proposed above have suggested ways to change the FISC procedures. More rigorous procedures, closer to the criminal model, are appropriate as the use of FISA grows and as it is more aggressively used for explicitly law enforcement purposes. The final set of reforms concerns how to assure long-term oversight of FISA.

---

http://www.uscourts.gov/rules/index.html.

1. *Reporting on uses of FISA for criminal investigations and prosecutions.* As discussed above, there needs to be greater reporting to Congress and the public of how FISA is used in criminal cases. Without this basic information, it will be difficult for the public and the courts to assess the extent to which the extraordinary foreign intelligence power is being used for "ordinary" criminal investigations. The Title III rules for reporting on the number of prosecutions and convictions are a good model.

2. *Disclosure of legal theories.* The sources and methods used in foreign intelligence investigations are generally sensitive and require secrecy. The names of the targets of the investigation also require secrecy, especially during the period of an active wiretap. The argument for the secrecy of legal theories, however, is much weaker. If the Department of Justice or FBI is taking a novel legal position about the scope of their powers, then the case for Congressional and public oversight is especially strong. A statute could require notice to Congress and/or the public of new legal arguments presented to the FISC. A related, and perhaps more thoughtful, approach would be to allow the FISC to determine whether to release information about legal theories. In that way, the Department of Justice could argue to Article III judges about whether there would be harm to the national security from release of the information.

3. *Judiciary Committee oversight.* Historically, the Senate and House Intelligence Committees have been the principal oversight committees for foreign intelligence surveillance. Especially if the "wall" stays down, then the Senate and House Judiciary Committees should have a much greater role in oversight. The Judiciary Committees are familiar with the many issues of law enforcement that are outside of the scope of the Intelligence Committees' scope.

4. *Consider greater use of Inspector General oversight after the fact.* There can be greater after-the-fact review of the operation of FISA from within the Justice Department or other elements of the intelligence community. A statute might require this sort of oversight, for instance, every three years by the existing Office of the Inspector General or a special office that could be created for foreign intelligence activities. The report of that oversight could be given to the Congressional Intelligence and Judiciary Committees.

5. *Consider providing notice of FISA surveillance significantly after the fact.* For domestic wiretaps, the Fourth Amendment generally requires prompt notice to the target after the wiretap is concluded. For national classified information, even top secret information, there are declassification procedures with presumptions of release to the public after a stated number of years.[340] Yet, anomalously, for FISA the surveillance remains secret permanently.

Serious consideration should be given to changing the permanent nature of secrecy for at least some FISA surveillance. Procedures can be created similar to declassification procedures. For instance, especially in cases that have resulted in criminal prosecution, there might be a presumption of release to the target and/or the public five years after the surveillance concludes. The presumption of release could be rebutted upon a particularized showing that this particular surveillance should not be made public. The particularized showing, which might be made to the FISC, might be that similar surveillance on the same target (e.g., the same embassy) is continuing or that release of the information would compromise sources and methods. Upon such showing,

[340] *See* 50 U.S.C. § 435.

the FISC might decide to release all of the surveillance, release redacted portions (such as to protect sources and methods), or keep the existence of the surveillance secret.

In making this proposal, I am not wedded to the details of how after-the-fact surveillance would be released. The growing use of FISA generally, and especially its growing use in law enforcement cases, makes it more important than in 1978 to have effective mechanisms that ensure that the system does not slip into the sort of routine and excessive surveillance that has existed in previous periods. The threat of eventual declassification may serve as an effective check of temptations to over-use FISA powers for political or other improper ends. The reality of eventual declassification may serve the function of the Church Committee hearings, providing evidence that is an essential corrective measure aimed at tendencies of a surveillance system to err on the side of over-use.

Conclusion

As this article was in the late stages of editing, the world press was filled with pictures and stories about interrogation abuses by members of the U.S. military in the Iraqi prison of Abu Ghraib. In October, 2003 the top U.S. military official in Iraq signed a classified memorandum that called on intelligence officials to assume control over the "lighting, heating … food, clothing and shelter" of those being questioned.[341] According to press reports, the subsequent merging of the military intelligence and military police roles was a crucial factor in creating the abuses.[342] Although it is too soon to predict the

[341] R. Jeffrey Smith, "Memo Gave Intelligence Bigger Role, Increased Pressure Sought on Prisoners," Wash. Post, May 21, 2004, at A17 (quoting memorandum from Lt. General Ricardo S. Sanchez).
[342] *E.g.*, Seymour M. Hersh, "Torture at Abu Ghraib," The New Yorker, May 10, 2004, at 42 (discussing report by Major General Antonio M. Taguba and other sources that stressed how military police were supposed to "set the conditions" for military intelligence interrogations).

precise legislative reaction to Abu Ghraib, strict new rules will almost certainly be drafted for military prisons and interrogations.

The tragic events at Abu Ghraib provide vivid lessons for the system of foreign intelligence surveillance law. First, the events of Abu Ghraib demonstrate once again the crucial importance of the rule of law in intelligence and police activities. The history of "The Lawless State" from the time of J. Edgar Hoover now has its counterpart in the lawless activities of interrogators in Iraq. In both instances, abuses were more likely to flourish in settings marked by a lack of clear rules, broad claims of executive discretion, and a philosophy that prevention of future harms justified historically unprecedented measures.[343]

Second, Abu Ghraib lets us see the dangers of blurring the boundaries between intelligence and police functions. For the military police at Abu Ghraib, the usual rules for running a prison became subservient to military intelligence goals in which they had not been trained. For the military intelligence personnel at Abu Ghraib, their control over the "lighting, heating … food, clothing and shelter" of prisoners meant that the usual limits on physical treatment of prisoners did not exist. The result of the blended roles was terrible – the restraints and training that usually guide each group did not apply.

---

[343] *See supra* notes 57-84 and accompanying text for a discussion during the period of "The Lawless State" of the lack of clear rules, the claims to inherent Executive discretion to set national security wiretaps, and the centrality of preventing harm, especially by "subversives." Since September 11, the amendments to the Patriot Act discussed *supra* at notes 154-87 and accompanying text, have a unifying theme of granting greater discretion to the Executive Branch, with less judicial oversight. The return in the FBI to a strategy of prevention has been clearly stated by FBI Director Mueller, who has made clear "In essence, we need a different approach that puts prevention above all else." Robert S. Mueller, III, "Press Availability on the FBI's Reorganization," May 29, 2002, *available at* http://www.fbi.gov/pressrel/speeches/speech052902.htm.

For the events at Abu Ghraib, the reports available to date indicate: a lack of clear rules about the relative roles of military intelligence and military policy; executive discretion as indicated by reports that senior officials did not support application of Geneva Conventions to prisoners held at Abu Ghraib; and a philosophy that extraordinary measures were justified to gain intelligence information from the persons held there. *See generally* Hersh, *supra* note 342.

Third, the pragmatic truth is that both national security and civil liberties are fostered by well-drafted procedures for surveillance and interrogation. In assessing the effects of the interrogation techniques at Abu Ghraib, any short-terms gains for military intelligence were surely minimal compared to the long-term damage. The damage manifested itself in human rights violations and the loss of American prestige in Iraq and the world. It also will almost certainly manifest itself in greater restrictions in the future on the system of military prisons and interrogations. Even from the narrow perspective of increasing the level of military intelligence, the short-run gain from extreme techniques will almost certainly turn out to be less than the long-run loss.

The reform proposals in this article build on precisely these three lessons: the importance of the rule of law; the risk of blurring intelligence and police functions; and the benefits for both national security and civil liberties from creating effective institutions and rules before a scandal occurs. Concerning the rule of law, this article has proposed a number of measures that would create a more effective system of checks and balances. For instance, proposals include: greater reporting and oversight; clearer rules of procedure within the Foreign Intelligence Surveillance Court and on appeal; abolition of Section 215 searches (or at least strict limits) in order to prevent fishing expeditions among U.S. persons; and greater use of Inspector General oversight or declassification of information after the fact.

Concerning the risks of blurring the boundaries between intelligence and police functions, the experience at Abu Ghraib lends new urgency to preventing "the wall" from coming down entirely. With no wall, it will be too easy for the eager prosecutor or FBI agent to minimize the importance of law enforcement procedures in the name of helping

intelligence. It will be too easy for the intelligence officer, eager to "connect the dots" in the war on terrorism, to brush aside the stricter rules created by statute and the Constitution that are supposed to apply to U.S. persons. Hence the reform proposal in this article, to permit the use of the extraordinary FISA powers only upon a certification that "the information sought is expected to be sufficiently important for foreign intelligence purposes" to justify a FISA order. Information used for foreign intelligence would once again be the organizing principle of what would be pursued with FISA authorities. In recognition of the importance of sharing information in pursuit of that goal, bureaucratic requirements of separation would not be required so long as the surveillance was justifiable on foreign intelligence grounds. Greater reporting and oversight of how FISA was used in criminal cases could provide accompanying safeguards.

In terms of the third lesson, how to meet the goals of both national security and civil liberties, the lesson of Abu Ghraib confirms the experience in 1978 from the passage of FISA. The organizing principle in 1978 was that FISA would protect civil liberties, by involving Article III judges in issuance of surveillance orders and providing other statutory safeguards. FISA would also protect national security. By regularizing and legitimizing the ways that foreign intelligence surveillance could proceed, the 1978 Act paved the way for a greater quantity of foreign intelligence orders over time. The experience of Abu Ghraib shows the opposite effect when procedures are badly drafted and have insufficient checks and balances. From a civil liberties perspective, the poor procedures contributed to human rights abuses. From a national security perspective, the

poor procedures jeopardized the military mission in Iraq and quite possibly will result in a backlash that will impose very strict limits on future interrogation techniques.

My discussions (on background) with counter-terrorism officials reveal significant concern about a full removal of "the wall." They have expressed concern about the blurring of intelligence and law enforcement functions: prosecutors and agents have usually not been well-trained in intelligence issues, and their eagerness to use the strong tools of FISA could easily lead to mistakes and over-disclosure of secret sources and methods. Cognizant of the achievements of the 1978 law, they have also expressed concern about the long-run effect of weakening the checks and balances in the FISA system. If FISA gets used excessively or badly in the law enforcement arena, the intelligence professionals are concerned about an eventual backlash. Over-use in the criminal sphere could easily lead to excessive restrictions for the core intelligence activities.

In summary, this article has presented the first full history and explanation of the development of the system of FISA and the system of foreign intelligence surveillance law. More than thirty years after "The Lawless State" came to light, it is important to remind a new generation about the proven abuses that have occurred in the name of executive discretion and the need to prevent harm. Experience with "The Lawless State" led to creation of the 1978 version of FISA, which both established significant safeguards on national security surveillance and allowed that surveillance to proceed once proper procedures were met. The events of September 11 triggered a new legal era for foreign intelligence surveillance, with major expansion of FISA and the use of National Security

Letters. The rationale for this expansion – that "everything had changed" due to the attacks – is both tempting to believe and subject to serious doubt upon examination.

Where should we go next? This article has stressed three themes that emerge from the history of FISA and the abuses at Abu Ghraib: the importance of rule of law; the dangers of blending intelligence and police activities; and the benefits for both national security and civil liberties of prescribing effective safeguards in advance. Based on these three principles, the article has proposed a range of possible legal reforms. Although not all of the proposals are likely to be enacted, it is important to build substantial new checks and balances into the FISA system. The history of previous cycles shows the temptation of surveillance systems to justify an ever-increasing scope of activity, in the hopes that just a little bit more surveillance will catch the terrorists or prevent an attack. Human nature has not fundamentally changed since the Palmer Raids, the McCarthy era, or the revelations of the 1970s. Unless effective institutions are created to limit domestic preventive surveillance, we will likely slip over time into a renewed practice of excessive surveillance. New checks and balances are required to handle new and expanded powers of the Executive to keep watch on citizens and keep secret what it learns and how it learns it. The forthcoming sunset of the FISA provisions is a unique historical opportunity to create those checks and balances.