AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

IMPLEMENTATION OF THE USA PATRIOT ACT: CRIME, TERRORISM AND THE AGE OF TECHNOLOGY

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 21, 2005

Serial No. 109–18

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

20–710 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 21, 2005

OPENING STATEMENT

Page

The Honorable Howard Coble, a Representative in Congress from the State of North Carolina, and Chairman, Subcommittee on Crime, Terrorism, and Homeland Security 1

The Honorable Robert C. Scott, a Representative in Congress from the State of Virginia, and Ranking Member, Subcommittee on Crime, Terrorism, and Homeland Security 2

WITNESSES

The Honorable Laura H. Parsky, Deputy Assistant Attorney General, U.S. Department of Justice

Oral Testimony 4

Prepared Statement 7

Mr. Steven M. Martinez, Deputy Assistant Director, Cyber Division, Federal Bureau of Investigation

Oral Testimony 27

Prepared Statement 29

Mr. Jim Dempsey, Executive Director, Center for Democracy and Technology

Oral Testimony 32

Prepared Statement 34

Mr. Peter Swire, Professor of Law, Ohio State University

Oral Testimony 38

Prepared Statement 41

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 75

Prepared Statement of the Honorable Maxine Waters, a Representative in Congress from the State of California 76

Submission by Peter Swire entitled "The System of Foreign Intelligence Surveillance Law," 72 *George Washington Law Review* 1306 (2004), available at *http://papers.ssrn.com/sol3/papers.cfm?abstract__* .....
id=586616 77

IMPLEMENTATION OF THE USA PATRIOT ACT: CRIME, TERRORISM AND THE AGE OF TECHNOLOGY

THURSDAY, APRIL 21, 2005

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

The Subcommittee met, pursuant to notice, at 10:03 a.m., in Room 2141, Rayburn House Office Building, the Honorable Howard Coble (Chair of the Subcommittee) presiding.

Mr. COBLE. Good morning, ladies and gentlemen. Good to have you all with us for our oversight hearing on the implementation of the USA PATRIOT Act, sections 209, 217, and 220 of the act that address crime, terrorism, and the age of technology.

Our Nation has a dependency problem, one that we need to nurture and protect. That dependency is on technology. Computers and related technology have improved every aspect of our lives, our health care, our education, our security, just to name a few.

This same technology also aids those who threaten our Nation and it facilitates terrorists and criminals alike. At the stroke of a key someone can cause millions of dollars of damage to our economy or shut down 911 systems of our emergency responders.

The threat has grown with the benefits of and dependency upon technology. Now, after September 11 attacks, the risks are greater. Even prior to the attacks the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security had been working on legislation to improve Federal law to protect the Nation from cybercrime and cyberterrorism.

In an almost prophetic effort this Subcommittee held three hearings on the growing threat of cybercrime and cyberterrorism in the summer of 2001, and was in the process of drafting legislation to meet those threats when the 9/11 attacks occurred.

These hearings highlighted that the Border Patrol and checkpoints at our airports and shipping ports cannot protect against cybercrime and terrorism.

This type of crime is borderless, knows no restraints, and can substantially harm the Nation's economy and our citizens.

To protect our privacy and our safety, law enforcement must be able to deal with new technology and the associated challenges. The borderless nature of cyberspace causes jurisdictional and in-

vestigative problems for law enforcement and facilitates often times criminal activity.

The law enforcement officials and private representatives at these hearings agreed that the criminal law needed to be updated and clarified.

In the PATRIOT Act, this Committee incorporated H.R. 2915, the legislation produced by the Subcommittee and then Chairman Lamar Smith in the summer of 2001. The PATRIOT Act updated criminal law to address the new challenges. These updates were designed to help law enforcement assess whether unlawful conduct is the result of criminal activity or terrorist activity and to respond appropriately.

The hearing today will discuss sections 209 that deals with stored electronic communications; 217 that addresses computer trespassers; and 220 that updates the service of search warrants for electronic communications.

These sections are set to expire on December 31 of this year.

I look forward to hearing from the testimonies from the witnesses, and now I'm pleased to recognize the distinguished Gentleman from Virginia, the Ranking Member, Mr. Bobby Scott.

Mr. SCOTT. Thank you, Mr. Chairman. And thank you again for scheduling another hearing on the USA PATRIOT Act. I think it's important that we have these hearings. I think we did a good job as a Committee when we passed the PATRIOT Act. Unfortunately, our work somehow dissolved between the Committee and the floor of the House. But we have taken in one of the points of this sunset which was to give us an opportunity to review our work product, and these hearings are certainly extremely important.

This hearing is about the investigation and prosecution of crimes through use of electronic evidence, section 209 of the act references seizure of voice mail messages pursuant to a warrant. However, that section authorizes access to much more than just voice mail and authorizes access through ways other than warrants, such as administrative, grand jury, and court issued subpoenas. And under the appropriate circumstances, there can also be the sneak and peak situations where they ate warrants, court subpoenas, or administrative subpoenas. So we're talking about a section that is not only misleading relative to the breadth of police powers that authorizes, but a title that is deceptive as to the extraordinary nature of those powers.

Quite frankly, Mr. Chairman, the more I review the extent of these powers that we have extended to law enforcement through provisions such as section 209, the more I am pleased with our decision to provide for a sunset on some of those powers in order that we may review in earnest what we have done so that law enforcement authorities who get access to our private information pursuant to these powers will be aware that we are reviewing their actions.

This is a section whose original purpose was to protect or electronic data against intrusion. Now, we see a big loophole that we carved out for the purpose of law enforcement access and the limitations on traditional methods of holding law enforcement accountable, such as prior notice for the right to quash and oversight of

a court through return reports to the court within a certain number of days.

And so I'm convinced that the sunset review in this area is absolutely essential to our oversight responsibilities to the public.

This is especially true in the areas of electronic and general technology given the growing impact of technology to our society. I have the same concerns about section 217, which allows an ISP to give law enforcement wide latitude to look at private electronic communications without court oversight or review.

It's one thing to call law enforcement to look at a trespass that is occurring. But it's another thing to call on law enforcement to look to see if anything suspicious is going on prior to a trespass actually occurring.

And while I can understand the efficiency of certain arguments for a nationwide search warrant authority in the area of electronic communications, I'm also concerned with the sufficiency of the notice and the right to challenge an oversight of such warrants.

Now for law enforcement, I think it's important to note that I think these powers should be available in appropriate circumstances. So I'm not calling for a sunset of those powers. However, the public's protection of their privacy as well as their safety, I'm saying that we need to look more precisely at the notice to oversight and reporting requirements for these powers and make appropriate adjustments.

We should also continue this kind of oversight through sunsets where we have to periodically look at the use of these powers in an arena of evolving technologies and where law enforcement is aware that the use of these powers will need to be scrutinized and justified.

And so, Mr. Chairman, I look forward to the testimony of our witnesses on how we might best do that and working with you on implementing our recommendations.

Mr. COBLE. I thank you, Mr. Scott.

Lady and gentlemen, it's the practice of the Subcommittee to swear in all witnesses appearing before us. So if you all would please stand and raise your right hands

[Witnesses sworn.]

Mr. COBLE. Let the record show that each of the witnesses answered in the affirmative. You may be seated.

We have a very distinguished panel today. And I will introduce them before we take testimony.

Our first witness is Ms. Laura H. Parsky, the Deputy Assistant Attorney General of the Criminal Division at the United States Department of Justice. In addition to serving at the Department of Justice, Ms. Parsky has served as Director of International Justice and Contingency Planning at the National Security Council. She was graduated from Yale University and obtained her law degree from Boalt Hall School of Law at the University of California at Berkeley. Following law school, Ms. Parsky clerked for the Honorable D. Lowell Jensen of the United States District Court for the Northern District of California.

Our second witness today is Mr. Steven Martinez, Deputy Assistant Director for the Cyber Division of the FBI. Prior to beginning his current position, Mr. Martinez served in many capacities within

the FBI, including managing the counter terrorism and counter intelligence efforts during the staging and commencement of Operation Iraqi Freedom. Mr. Martinez is a graduate of St. Mary's College of California and received a master's degree from the University of California at Berkeley.

Our next witness is Mr. Jim Dempsey, Executive Director of the Center for Democracy and Technology. Prior to joining the Center, Mr. Dempsey was a Deputy Director of the Center for National Security Studies and also served as Assistant Counsel to the House Judiciary Committee's Subcommittee on Civil and Constitutional Rights. Mr. Dempsey is a graduate of Yale University and the Harvard Law School.

Our final witness today is Mr. Peter Swire, Professor of Law at the Ohio State University's Moritz College of Law. Previously, 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 the Yale Law School. After graduating from law school, he clerked for Judge Ralph K. Winter, Jr., of the United States District Court—strike that—of the United States Court of Appeals for the Second Circuit.

Folks, it's mighty good to have all of you with us. As you all have been previously informed, we operate under the 5-minute rule here, and you will see the panels before you at the desk when amber light appears that is your notification that time is elapsing rapidly. And when the red light appears, the 5 minutes have expired. And have furthermore imposed the 5-minute rule against ourselves as well. So when we examine you, if you all could be terse, we would be appreciative of that.

Ms. Parsky, why don't you start us off?

TESTIMONY OF THE HONORABLE LAURA H. PARSKY, DEPUTY ASSISTANT ATTORNEY GENERAL, U.S. DEPARTMENT OF JUSTICE

Ms. PARSKY. Thank you. Good morning, Mr. Chairman, Ranking Member Scott and honorable Members of the Subcommittee.

It is my pleasure to appear before you to discuss sections 209, 217, and 220 of the PATRIOT Act, provisions that have authorized our laws to keep pace with new technologies. These provisions have made commonsense changes that have harmonized the treatment of similar situations, that have eliminated unnecessary and inefficient processes, and that have given back to victims the rights they deserve.

Together, they are a significant step forward in meeting the challenges of investigating and prosecuting crime in the 21st century.

Our world has changed in dramatic ways in recent years. On the one hand, as September 11th made tragically clear, we face the threat of terrorism on a scale that was previously unimaginable.

On the other hand, we have experienced tremendous technological advancement that has given us modern wonders like the Internet. It is because of both of these developments that the PATRIOT Act is vital to our country's safety.

As the world changes, so must our laws. We cannot go back to the days before September 11th, and we cannot turn back the clock

of the digital age. Likewise, we cannot regress to outdated laws that defy reason in today's world.

Sections 209, 217, and 220 are just the kinds of commonsense changes that we need to keep pace with technology. Prior to the PATRIOT Act, voice mails were subject to burdensome rules designed for ongoing access to live communications rather than those rules for a single access to other similar types of stored communications.

In fact, it was easier for law enforcement to get a warrant to go into a person's home and listen to messages on that person's answering machine than it was to obtain voice mail messages left—stored with a third party.

Section 209 fixed this inconsistency by making the rules for stored voice mail more consistent with those for other types of stored messages, such as electronic mail.

Section 217 also addresses new technology, the rise of computer networks, such as the Internet. Section 217 makes clear that Federal law will not shield a person who trespasses on the computer system of another. Section 217 puts the power to decide who may enter property back where it belongs: in the hands of the property owner, just as has always been the case for homeowners.

Finally, section 220 recognizes that today's modern communications technologies make it possible for records relating to an investigation in a particular jurisdiction to be stored in a distant jurisdiction, or in many cases in several distant jurisdictions.

Rather than sending investigators all over the country to explain the same set of facts over and over again to different prosecutors and different judges, section 220 allows the investigators and prosecutors who are most familiar with the case to obtain authorization to gather electronic records from a single judge in their own district, who is also most familiar with the facts of the case, just as has always been the case with other records subject to grand jury subpoenas. This provision just makes practical sense in today's world of electronic evidence.

In the three and a half years since Congress passed these provisions of the PATRIOT Act by overwhelming bipartisan majorities, we've had the opportunity to see these provisions in action. We have seen the modern tools Congress authorized through passage of the PATRIOT Act dramatically improve law enforcement's ability to protect the safety and security of the American people.

We have used these tools to disrupt terrorist networks and to prevent terrorist attacks, to bring down international drug conspiracies, and to rescue children in imminent danger.

Most significantly we have prevented another terrorist attack from striking us here at home. These are the facts, not fears.

The PATRIOT Act has made law enforcement more effective and more efficient. All this has been done without impacting any of the constitutional protections that we as Americans hold dear.

It is in this context that these tools must be evaluated. It is this record of accomplishments that should be first and foremost in your minds.

We cannot go back. If Congress fails to reauthorize the PATRIOT Act, we will revert to old rules that hamstring law enforcement

with inefficient processes and unnecessary delays in investigating 21st century crime.

The law would once again treat similar services differently without good cause, and, worse, the law would protect criminals at the expense of their victims' rights. If these provisions are not renewed, law enforcement will be less efficient and less effective in combating not only terrorism, but other serious offenses, such as cyber crime, child exploitation and kidnapping.

Our experience over the past three and a half years has proven the utility and rationality of these modernizations of our laws. In light of the very real threats we face today, we cannot afford to go back to when technology was outpacing law enforcement's tools.

Therefore, I ask that you continue to move our laws forward by reauthorizing sections 209, 217, and 220 of the PATRIOT Act. The Department of Justice appreciates this Subcommittee's leadership in making sure that our country's laws meet the challenges of today and of tomorrow.

Thank you for the opportunity to testify today and for your continuing support. I am happy to try to answer any questions you may have.

[The prepared statement of Ms. Parsky follows:]

PREPARED STATEMENT OF LAURA H. PARSKY

Statement of Laura H. Parsky
Deputy Assistant Attorney General
Criminal Division, U.S. Department of Justice
Before the U.S. House of Representatives, Committee on the Judiciary,
Subcommittee on Crime, Terrorism and Homeland Security

REAUTHORIZATION OF THE USA PATRIOT ACT TECHNOLOGY PROVISIONS

April 21, 2005

I. Introduction

Good morning, Mr. Chairman, Ranking Member Scott, and Honorable Members of the Subcommittee. It is my pleasure to appear before you to discuss some of the provisions of the PATRIOT Act that have modernized our laws to address new technologies.

In particular, you have invited me to discuss sections 209, 217, and 220 of the Act. Section 209 rendered the rules for stored voicemail messages more consistent with those for other types of stored messages such as electronic mail (e-mail) and answering machine messages. Prior to the Act, access to stored voicemails was unnecessarily encumbered by rules designed to apply to on-going access to live communications rather than the rules for a single access to stored communications. Section 217 recognized the growth of computer networks and makes clear that federal law will not shield a person who trespasses on the computer system of another. Section 217 put the power to

decide who may enter property back where it belongs, in the hands of the property owner, just as has been the case for real property owners throughout history. Finally, Section 220 recognized that today's modern communications technologies make it possible for records relating to an investigation to be dispersed across the country. Section 220 allowed the prosecutor and investigator most familiar with the case to prepare the affidavits and applications to seek a search warrant, while the judge most familiar with the investigation may authorize the warrant for related records.

In the three and a half years since Congress passed these provisions of the PATRIOT Act by overwhelming bipartisan majorities, we have had the opportunity to carefully assess the true utility of these new tools. I am here to report to you that we in law enforcement have found these tools critical to our mission to protect national security and the safety of our communities. As I will discuss further in a moment, we have used tools created in the PATRIOT Act to disrupt terrorist networks and to prevent terrorist attacks, to bring violent fugitives to justice, and to rescue children in imminent danger. The PATRIOT Act has allowed law enforcement to be more effective and more efficient. All this has been done without sacrificing any of the constitutional protections or invaluable privacy rights that we as Americans hold dear.

Members of the Subcommittee, we cannot go back. If Congress fails to re-authorize sections 209, 217 and 220 of the PATRIOT Act, we will revert to old rules that fail to account for today's technological innovations, that treat similar situations differently, and that create inefficient processes and unnecessary delay. The tools contained in the PATRIOT Act have been essential to the Department's top priorities, chief of which is to ensure public safety against threats both foreign and domestic. If these provisions are not renewed, the Department's ability to combat not only terrorism but also other serious offenses such as cybercrime, child pornography, and kidnapings will be less efficient and less effective. There are carefully adhered to limits on these authorities, and experience has proven their utility and rationality. In light of the very real threats we face today, we cannot afford to return to a time when technology was outpacing the tools of law enforcement. Therefore, I am here to ask that you preserve these critical tools in today's world of advancing technology and re-authorize these provisions of the PATRIOT Act.

II. Section 209 Harmonized the Treatment of Stored Voicemail Messages With That of Other Types of Stored Messages.

Section 209 provides a good example of how the PATRIOT Act modernized the law to recognize new technology. Prior to the Act, voicemail --

essentially a remote answering machine service -- was treated differently than other remote storage services, like e-mail, or even than more traditional answering machine messages. Answering machine messages can be obtained with an ordinary search warrant issued by a judge upon a showing of probable cause. Likewise, e-mail messages can be obtained with a search warrant. By contrast, however, voicemail messages were subject to the much more burdensome and restrictive process of obtaining a wiretap order.

The Wiretap Act (18 U.S.C. 2510 *et seq.*) was designed to address a very particular type of situation, the ongoing interception of real-time conversations. Given the power of this law enforcement technique, it is properly subject to strict limitations. However, the one-time access to stored communications, such as a voicemail message, does not implicate the same sensitivities associated with the ongoing interception of live telephonic communications; therefore, there is no basis for subjecting requests to retrieve voicemail messages to the same special protections as requests for wiretaps. This is especially true when law enforcement could obtain the same type of information with a search warrant had the information been stored on an answering machine in a person's home instead of with a third-party provider. Even where the additional requirements of the Wiretap Act could be met, law enforcement was forced to waste precious

time and resources to satisfy these more burdensome requirements.

Section 209 of the PATRIOT Act made existing statutes technology-neutral by providing that access to voicemail messages not be subjected to a higher standard than access to e-mail or answering machine messages. Now investigators can go to a judge and obtain a search warrant to access voicemail messages stored by a third-party provider. Yet, section 209 preserved all of the checks and balances inherent in the process for accessing other stored communications, including ensuring that neutral judges evaluate such applications for probable cause when a search warrant is sought. Further, by applying the same rules to voicemail messages as to other stored communications, section 209 eliminated needlessly burdensome and anachronistic rules that threatened the ability of law enforcement to successfully and effectively investigate and prosecute serious crimes.

Since the passage of the PATRIOT Act, search warrants have been used in a variety of criminal cases to obtain voicemails that provided critical evidence. Investigators have obtained voicemail messages left for both foreign and domestic terrorists. In addition, warrants made possible by the Act have been used to investigate a large-scale international ecstasy smuggling ring. In another case, investigators were able to quickly obtain a warrant to retrieve the

voicemails of a defendant arrested in possession of hundreds of pounds of marijuana worth over half a million dollars on the street.

Allowing section 209 to expire, as will happen at the end of this year if Congress fails to act, would take us back to the irrationality of applying different rules for access to similar types of stored messages. Going back to requiring a wiretap order for access to stored voicemail messages would needlessly hamper law enforcement efforts to investigate crimes and obtain evidence in a timely manner. We need not and should not go back to this inconsistent, ineffective, and inefficient process.

III. Section 217 Gave Modern Computer Owners the Same Rights That Homeowners Have Always Had -- Ultimate Control Over Who May Enter Their Property.

Section 217 of the PATRIOT Act (the Hacker Trespass Provision) also brought criminal procedures up to date with modern technology. Homeowners have always had the right to decide who can and who cannot enter their property, including the right to decide whether or not to invite law enforcement onto their property to investigate a crime. Where someone breaks and enters into a home, the law does not protect the thief from police officers when the homeowner has invited in the police to catch the trespasser.

One would not expect that someone who breaks and enters into a

computer system would have any more right to be shielded from law enforcement than a common trespasser. The law certainly should not protect the purported privacy of a trespasser at the very same time he is violating the privacy of the computer owner, potentially accessing sensitive information ranging from trade secrets to medical information to personal letters.

Prior to the passage of the Hacker Trespass Provision, the law did not clearly provide that a computer owner could invite the assistance of law enforcement in monitoring computer hackers on his or her system. In what one legal commentator called a "bizarre result,"[1] it was possible for the intruder invading the privacy of a computer owner to himself claim that his invasion should be kept private from investigators.

The Hacker Trespass Provision left no doubt that a computer owner has the authority to control who is on his or her system. That right includes the ability to invite law enforcement to help combat hackers and other cyber-intruders. In keeping with the principle of preserving the computer owner's rights, the Hacker Trespass Provision did not *require* computer owners to involve law enforcement if they detect trespassers on their systems; it simply gave them the *option* to do so.

---

[1] Orin S. Kerr, *Are We Overprotecting Code? Thoughts on First-Generation Internet Law*, 57 Wash. & Lee L. Rev. 1287, 1300 (2000).

On the other hand, someone with no right to be on that system cannot be heard to complain when law enforcement uncovers his unauthorized activities.

In fact, the Hacker Trespass Provision did not adversely affect any legitimate privacy rights. Prior to the passage of the PATRIOT Act, the Wiretap Act already allowed computer owners to monitor activity on their machines to protect their rights and property. Thus, trespassers' communications were already subject to monitoring; it was simply unclear whether computer owners could obtain the assistance of law enforcement to conduct such monitoring. Because computer owners often lack the expertise, equipment, or financial resources required to monitor their systems themselves, they commonly have no effective way to exercise their rights to protect themselves from unauthorized attackers. The Hacker Trespass Provision ensured that computer owners could effectively protect their rights through the assistance of law enforcement.

The Hacker Trespass Provision also preserved the privacy of law-abiding computer users by sharply limiting the circumstances under which the provision applies. Law enforcement may only monitor a computer when invited to do so by the computer owner, and even then they may not agree to assist unless (1) they are engaged in a lawful investigation; (2) there is reason to believe that the communications will be relevant to that investigation; and (3) their activities will

not acquire any communications beyond those authorized. Moreover, the Hacker Trespass Provision provided a narrow definition of "computer trespasser," which excludes individuals who have a contractual relationship with the service provider. Therefore, for example, the Hacker Trespass Provision would not allow an Internet Service Provider to ask law enforcement to help monitor a hacking attack on its system that was initiated by one of its own subscribers. Nor can this provision be used if the configuration of the computer system would require the interception of non-consenting authorized users. Of course, the authority to intercept ceases at the conclusion of the investigation or when consent is withdrawn.

Since its enactment, the Hacker Trespass Provision has played a key role in sensitive national security matters, including investigations into hackers' attempts to compromise military computer systems. The Hacker Trespass Provision is also particularly helpful when computer hackers launch massive "denial of service" attacks that are designed to shut down web sites, computer networks, or even the entire Internet.

If Congress were to fail to act before the end of this year to preserve the Hacker Trespass Provision, we would revert to a law that protects criminal rights over victim rights. A computer hacker would be able to compromise the

legitimate privacy rights of his victims, and those victims would be denied law enforcement assistance in catching the perpetrator. As computer hacking becomes more widespread and the threat of cyber-terrorism grows, we simply cannot afford to take a step backward in our efforts to protect victims and to deter this serious crime.

IV. Section 220 Allowed Law Enforcement To Keep Pace With the Modern Reality of Remote Storage of On-line Communications.

Section 220 acknowledged the realities of our modern on-line world, where evidence can be stored anywhere in the country, and section 220 removed the barriers that had stood in the way of law enforcement's ability to respond quickly within those realities. Specifically, section 220 allowed courts with jurisdiction over an investigation to issue search warrants for electronic evidence stored outside of their own district.

Prior to the PATRIOT Act, some courts declined to issue search warrants for e-mail messages stored on servers in other districts. As a result, many time-sensitive investigations were delayed as new investigators, prosecutors, and judges in other districts with no prior familiarity with the investigation were brought up to speed. Moreover, requiring investigators to obtain warrants in the jurisdiction where an Internet Service Provider happened to locate its servers

placed enormous burdens on a few districts where major Internet Service Providers are located, such as the Northern District of California and the Eastern District of Virginia.

Section 220 provided a rational solution to these problems. Now, investigators have one place to go to seek a search warrant for electronic evidence, the district where the investigation is being conducted, rather than having to duplicate their efforts in other districts just because electronic records happen to be stored there. For instance, section 220 would allow a judge with jurisdiction over a murder investigation in Pennsylvania to issue a search warrant for e-mail messages pertaining to that investigation that happen to be stored on a server in Silicon Valley, California. Under this scenario, the judge in Pennsylvania most familiar with the investigation could issue the warrant, rather than a judge in the Northern District of California, who is completely unfamiliar with the case.

The Department of Justice has already utilized section 220 in extremely important terrorism investigations. As the Criminal Division's Assistant Attorney General, Christopher Wray, testified before the Senate's Committee on the Judiciary on October 21, 2003, section 220 proved useful in the Portland terror cell case, because "the judge who was most familiar with the case was able to

issue the search warrants for the defendants' e-mail accounts from providers in other districts, which dramatically sped up the investigation and reduced all sorts of unnecessary burdens on other prosecutors, agents and courts." This provision of the PATRIOT Act has been similarly useful in the "Virginia Jihad" case involving a Northern Virginia terror cell and in the case of the infamous "shoebomber" terrorist, Richard Reid.

In addition to terrorism cases, section 220 has also been used effectively in a vast array of criminal investigations where perpetrators generated electronic evidence in numerous distant jurisdictions through their on-line activities, whether or not their crimes actually occurred on-line. Take for example the recent case of a man who, armed with a sawed-off shotgun, abducted and sexually assaulted his estranged wife in West Virginia. He later fled West Virginia in a stolen car to avoid capture. While on the run, he continued to contact associates by e-mail using an Internet Service Provider whose e-mail servers happened to be located clear across the country in California. Using the authority provided by section 220, investigators in West Virginia were able to obtain a warrant quickly from a federal court in West Virginia for the disclosure of information regarding the armed fugitive's e-mail account. The Internet Service Provider quickly provided information revealing that the fugitive had logged

onto his e-mail account from South Carolina. Using that information, Deputy U.S. Marshals were able to arrest the fugitive the very next day. He later pleaded guilty in state court and was sentenced to imprisonment for a term of 30 years. The ability to obtain a warrant for e-mail records immediately, made possible by section 220 of the PATRIOT Act, was crucial to capturing this violent fugitive.

Section 220 has also been used to more effectively and more efficiently unravel a complicated international conspiracy to distribute child pornography. Investigators in New Jersey had probable cause to search a number of different computers used by a company that operated its own child pornography websites and provided credit card processing services to other child pornography websites. These computers were physically located in four separate judicial districts; however, a single magistrate in Newark, New Jersey signed search warrants for all four computers. The searches yielded records of tens of thousands of transactions on hundreds of child pornography and erotica websites. The investigation of these criminals exploiting children for profit would have been dramatically handicapped without section 220. With the assistance of the PATRIOT Act, nine individuals or corporations have been convicted of federal crimes. More significantly, the evidence gathered under section 220 has led to nearly a thousand more domestic and foreign arrests.

Section 220 has also dramatically reduced the administrative burdens on judicial districts that are home to large Internet Service Providers. Before the PATRIOT Act, these districts were inundated with search warrant requests for electronic evidence. For example, prior to the passage of the PATRIOT Act, the U.S. Attorney's Office in Alexandria, Virginia was receiving approximately 10 applications each month from United States Attorney's Offices in other districts for search warrants for records from Internet Service Providers. For each of these applications, both an Assistant United States Attorney and a law enforcement agent in the district had to learn all of the facts of another district's investigation in order to apply for the warrant. The result was that agents, attorneys, and judges spent many hours each month processing applications for investigations based in other districts. Thanks to section 220, these attorneys and agents can now spend their time investigating crime in their own districts rather than duplicating the efforts of other districts' investigations and processing unnecessary paperwork.

Contrary to concerns voiced by some, section 220 did not allow investigators to "shop" for sympathetic judges. Section 220 required that the court issuing a search warrant have jurisdiction over the investigation. Investigators may not pick and choose among any court in the country; they

must go to a court with proper jurisdiction. Moreover, nothing in section 220 affected the standard for issuing a search warrant. All of the same requirements apply regardless of whether the warrant is issued where the investigation is being conducted or where the records are located.

In today's world of advanced communications technology, it is imperative that law enforcement have modern tools to keep pace with criminals. Rather than requiring law enforcement to chase down electronic evidence across the country and causing unnecessary delay in time-sensitive investigations, Congress must re-authorize section 220.

V. Many of the Other Provisions of the PATRIOT Act Have Likewise Been Vital To Modernizing 20th Century Laws to Reflect 21st Century Realities.

The provisions I have just discussed are not the only ones in the PATRIOT Act that have modernized our laws and made our rules more consistent with changing technology. To illustrate, I want to touch on just two more of the provisions of the Act that typify the kind of reasonable corrections made by the PATRIOT Act: section 212, the Emergency Disclosure Provision, and section 210, which modernized the terms used to describe information that may be obtained with a subpoena.

Before the PATRIOT Act, an Internet Service Provider was limited in its

ability to voluntarily provide information to the government about an imminent danger, including terrorist plots. Section 212, the Emergency Disclosure Provision, now permits providers voluntarily to disclose subscriber records in life-threatening or other dangerous emergencies. This provision also corrected an anomaly in prior law under which an Internet Service Provider could voluntarily disclose the content of communications to protect itself against hacking, but could not voluntarily disclose stored customer records for the same purpose.

Since its passage, section 212 has repeatedly saved lives. Emergency disclosure has been used to investigate death threats in our schools, to recover victims in kidnaping cases, and to protect targeted government facilities against cyber-attack. But let me describe just one case in particular -- a case where emergency disclosure resulted in the rescue of a 13-year-old girl from her abductor. In early 2002, FBI agents in Pittsburgh received a report from local police that a 13-year-old girl had disappeared the previous day from her parents' home. A friend of the girl told investigators that the girl had discussed leaving home with a man she had met on-line. A few days later, an anonymous caller contacted the FBI and stated that he had chatted on-line recently with an individual claiming to have taken a girl from Pittsburgh. FBI agents in Pittsburgh quickly requested information from an Internet Service Provider

pursuant to section 212. With the information voluntarily provided in response to that request, agents were able to locate the perpetrator at his residence in Herndon, Virginia and rescue the child victim. The girl's abductor was arrested, pleaded guilty to charges including sexual exploitation of a minor, and was sentenced to a prison term of over 19 years.

Although section 210 of the PATRIOT Act is not scheduled to sunset, it provides another good example of how the PATRIOT Act has modernized and updated our laws. In particular, section 210 of the Act clarified the scope of subpoenas for records from electronic communication service providers, such as Internet Service Providers. Section 210 updated old terms that were specific to telephone communications in order to ensure that those terms do not stand in the way of law enforcement's obtaining equivalent types of information associated with modern communications. Thus, for instance, whereas prior law allowed law enforcement to obtain only "local and long distance telephone toll billing records," the PATRIOT Act included parallel terms for communications on computer networks, such as "records of session times and durations." Similarly, the law prior to the PATRIOT Act allowed law enforcement to use a subpoena to obtain the customer's "telephone number or other subscriber number or identity," but did not define what that phrase meant in the context of Internet

communications. Section 210 added "any temporarily assigned network address" to make clear that, among other things, Internet Protocol addresses are included.

These clarifications were put into action in Operation Hamlet, an investigation that dismantled an international ring of child molesters and rescued more than 100 child victims. To give just a few examples, this criminal network used the Internet to exchange photographs and video of their molestation of children, molestation that included children being sexually exploited by their own parents or by different individuals to whom the parents had offered their children for sex. In some instances, molesters would even offer a "live show" of their disgusting acts via a webcam. Subpoenas were issued to numerous Internet Service Providers during the investigation requesting information that was explicitly made subject to subpoena authority by the PATRIOT Act. Among the types of information investigators received were names and addresses, records of when molesters were on-line and for how long, and temporarily assigned network addresses that allowed law enforcement to tie particular customers to their on-line activities. With this information, much of which was unobtainable prior to the PATRIOT Act, investigators were able to identify many of the members of this ring and obtain

search and arrest warrants. Thus far, 26 searches have been conducted in the United States and 11 searches in other countries; and 23 persons have been indicted in the United States, resulting in 21 convictions and two individuals pending trial.

VI. Conclusion

As I have described above, the modern tools Congress authorized through passage of the PATRIOT Act have dramatically improved law enforcement's ability to protect the safety and security of the American people. With these tools, the Department of Justice has captured terrorists, brought violent criminals to justice, and rescued children from sexual exploitation. Most significantly, we have prevented another terrorist attack from striking us here at home. These are facts, not fears. It is in this context that these tools must be weighed. It is this record of accomplishments that should be first and foremost in your minds.

Our world is different today in ways both good and bad. On the one hand, we face the threat of terrorism on a scale that was previously unimaginable. On the other hand, we have experienced tremendous technological advancement that has given us modern wonders like the Internet. It is because of *both* of these developments that the PATRIOT Act is

vital to our nation's safety. We cannot go back to the days before September 11th, and we cannot turn back the clock of the Digital Age; likewise, we cannot regress to outdated laws that defy reason in today's world. Our experience over the past three and a half years clearly demonstrates the real benefits and necessity of the modern law enforcement tools provided in the PATRIOT Act. The Department of Justice appreciates this Subcommittee's leadership in making sure that our country's laws meet the challenges of today and of tomorrow by re-authorizing these provisions of the PATRIOT Act. Thank you for the opportunity to testify today and for your continuing support. I am happy to try to answer any questions you may have.

Mr. COBLE. Thank you, Ms. Parsky.

Mr. Martinez?

TESTIMONY OF STEVEN M. MARTINEZ, DEPUTY ASSISTANT DIRECTOR, CYBER DIVISION, FEDERAL BUREAU OF INVESTIGATION

Mr. MARTINEZ. Good morning, Mr. Chairman, Ranking Member Scott, and Members of the Subcommittee.

My name is Steven Martinez. I'm the Deputy Assistant Director of the FBI's Cyber Division. The primary mission of the Cyber Division is to protect the American public against a host of significant and potentially deadly high-tech crimes.

The uses of technology in our society are innumerable and their value immeasurable. The state of technology has been advancing rapidly over the past 20 years, much of it to the benefit of people living in all corners of the world.

Unfortunately, the picture is not always so bright.

Technology has also been used to harm people, while offering a particularly effective escape route. In this digital age, crimes can and do occur within seconds without the perpetrator ever getting anywhere physically close to the victim.

In such a setting, law enforcement must be equipped with the investigative tools necessary to meet, locate, and incapacitate the growing threat.

With this background in mind, I want to thank you for the opportunity to appear before you today to discuss certain sections of the USA PATRIOT Act which are scheduled to expire at the end of this year, specifically sections 209, 217, and 220. Going in numerical order, allow me to start with section 209.

Section 209 permits law enforcement officers to seize voice mail with a search warrant rather than a surveillance, or title III order. The importance of this provision is best understood in the context of how often terrorists and other criminals rely on technology to relay their plans to each other instead of risking face to face in-person meetings.

Section 209 provides a very good example of how the USA PATRIOT Act simply updated the law to reflect recent technological developments. The drafters of the act determined that obtaining voicemail stored on a third party's answering system is more similar to obtaining voicemail stored on a home answering machine, which requires a search warrant, more so than it is to monitoring somebody's telephone calls, which requires a title III order.

In passing this portion of the act, Congress made the statutory framework technology-neutral. Privacy rights are still well accounted for, since the section 209 allows investigators to apply for and receive a court-ordered search warrant to obtain voicemail pursuant to all of the pre-existing standards for the availability of search warrants, including a showing of probable cause.

With privacy rights left firmly intact, there is a distinct advantage to the public's safety when law enforcement can obtain evidence in a manner that is quicker than the title III process.

I would like to move next to section 217, the Hacker Trespasser Exception. Like section 209 before it, section 217 also makes the law technology-neutral.

Section 217 places cyber-trespassers—those who are breaking into computers—on the same footing as physical intruders. Section 217 allows the victims of computer-hacking crimes voluntarily to request law enforcement assistance in monitoring trespassers on their computers.

Just as burglary victims have long been able to invite officers into their homes to catch the thieves, hacking victims can now allow law enforcement officers into their computers to catch cyber-intruders.

Think for a moment how odd it would be if a homeowner yelled out to a police officer "Hey, there's a burglar in my house right now, help!", only to have the police respond, "Sorry, I have to apply for a court order first, try not to scare him off." The homeowner would be dumbfounded; the burglar would be long gone by time the police returned. This, in essence, is what was occurring prior to the PATRIOT Act.

It can be said that section 217, in a very significant way, enhances privacy. The essence of the section—to help catch hackers—serves a vital function in the FBI's ability to enforce data privacy laws. Hackers have no respect for your privacy or mine.

There has been an outpouring of concern from the American public to protect them from identity theft and to ensure that their personal records are secure. Congress has responded with a powerful array of laws that are designed to impose serious consequences on computer hackers. However, if law enforcement does not have the ability to quickly spot and then locate hackers, then the victim toll will mount and only hackers themselves, remaining anonymous, will be left with privacy.

The FBI understands the importance of preventing criminals from stealing and selling our information, and we are resolved to catch those who do. Section 217 is of enormous help in this regard.

Lastly, I would like to turn to section 220. Section 220 enables Federal courts—with jurisdiction over investigation—to issue a search warrant to compel the production of information, such as unopened e-mail, that is stored with a service provider located outside their district.

Now, for example, a judge with jurisdiction over a kidnapping investigation in Pittsburgh can issue a search warrant for e-mail messages that are stored on a server in California. As a result, investigators in Pennsylvania can ask the judge most familiar with the investigation to issue a warrant rather than having to ask an Assistant United States Attorney in California who's unfamiliar with the case, to ask a district judge in California, who also is unfamiliar with the case, to issue the warrant.

Lest you think this is merely a hypothetical example, it's not. Using section 220, our FBI office in Pittsburgh was able to obtain a warrant for information residing on a computer in California that ultimately led to the rescue of a teenage girl who was being sexually tortured in Virginia while being chained to a wall in somebody's basement.

The man who held her hostage is now in prison, serving close to 20 years. The girl's life was saved.

Other FBI Field Offices also have repeatedly stated that section 220 has been very beneficial to quickly obtain information required in their investigations.

Mr. Chairman and Members of the Committee, let me conclude my prepared remarks by saying that the provisions of the USA PATRIOT Act I have discussed today have proven significant to a number of our successes and I have every reason to believe that the need to retain these provisions in the future is also significant.

By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to enforce the law and protect lives, while at the same time protecting civil liberties. Thank you.

[The prepared statement of Mr. Martinez follows:]

PREPARED STATEMENT OF STEVEN M. MARTINEZ

Good morning Mr. Chairman, Ranking Member Scott, and members of the subcommittee.

My name is Steven Martinez and I am the Deputy Assistant Director of the FBI's Cyber Division. The primary mission of the Cyber Division is to supervise the Bureau's investigation of federal violations in which computer systems, including the Internet, are exploited by terrorists, foreign government intelligence operatives, and criminals. In short, our mission is to protect the American public against a host of significant and potentially deadly high-tech crimes.

The uses of technology in our society are innumerable and their value immeasurable. The state of technology has been advancing rapidly over the past twenty years, much of it to the benefit of people living in all corners of the world. Unfortunately, the picture is not always so bright. Technology has also been used to harm people, while offering a particularly effective escape route. In this digital age, crimes can and do occur within seconds without the perpetrator ever getting anywhere physically close to the victim. In such a setting, law enforcement must be equipped with the investigative tools necessary to meet, locate, and incapacitate this growing threat. Law enforcement must be prepared to face sophisticated enemies and criminals who are known to exploit technology because of its ability to keep them far away from the scene of the crime, spread apart even from one another, and who have the ability to delete any digital evidence of their actions at the push of a button.

With this background in mind, I want to thank you for the opportunity to appear before you today to discuss certain sections of the USA PATRIOT Act which are scheduled to expire at the end of this year, specifically sections 209, 217, and 220.

When Attorney General Gonzales testified before the House Judiciary Committee on April 6, 2005, he shared his firm view that each of the provisions of the USA PATRIOT Act that are scheduled to sunset at the end of this year must be made permanent. Director Mueller provided the FBI's perspective in a hearing before the Senate Judiciary Committee on April 5, 2005, and he too spoke of the crucial need to renew these provisions. Based on my knowledge of the interests, capabilities, and motives of those who, day in and day out, are attempting to do us harm by means of the Internet, I want to express my full agreement about the importance of the PATRIOT Act and the provisions I plan to address today. I believe that the Act's substantial merit can be demonstrated by what we already have experienced as a nation; still, it is equally true that the Act is essential so that we are prepared to confront the ever-evolving threat that no doubt will come.

SECTION 20—SEIZURE OF VOICE MAIL WITH A SEARCH WARRANT

Going in numerical order, allow me to start with section 209. Section 209 permits law enforcement officers to seize voice mail with a search warrant rather than a surveillance, or Title III, order. Section 209 provides a very good example of how the USA PATRIOT Act simply updated the law to reflect recent technological developments. The drafters of the Act determined that obtaining voicemail stored on a third party's answering system is more similar to obtaining voicemail stored on a home answering machine (which requires a search warrant) than it is to monitoring somebody's telephone calls (which requires a TIII order). In passing this portion of the Act, Congress made the statutory framework technology-neutral. Privacy rights are still well accounted for, since section 209 allows investigators to apply for and receive a court-ordered search warrant to obtain voicemail pursuant to all of the

pre-existing standards for the availability of search warrants, including a showing of probable cause. With privacy rights left firmly intact, there is a distinct advantage to the public's safety when law enforcement can obtain evidence in a manner that is quicker than the Title III process.

The importance of this provision is best understood in the context of how often terrorists and other criminals rely on technology to relay their plans to each other instead of risking face-to-face in-person meetings. Attorney General Gonzales gave a good sense of the diversity of those who would rely on the simple convenience of leaving voicemail in furtherance of their illegal activities when he pointed out that section 209 has already been relied upon to acquire messages left for domestic terrorists, foreign terrorists, and international drug smugglers.

Allowing section 209 to expire would once again lead to different treatment for voicemail messages stored on a third party's system than for the same message stored on a person's home answering machine. Doing so would needlessly hamper law enforcement efforts to investigate crimes.

SECTION 217—THE HACKER TRESPASSER EXCEPTION

I would like to move next to section 217, the hacker trespasser exception. Like section 209 before it, section 217 also makes the law technology-neutral. Section 217 places cyber-trespassers—those who are breaking into computers—on the same footing as physical intruders. Section 217 allows the victims of computer-hacking crimes voluntarily to request law enforcement assistance in monitoring trespassers on their computers. Just as burglary victims have long been able to invite officers into their homes to catch the thieves, hacking victims can now allow law enforcement officers into their computers to catch cyber-intruders. Think for a moment how odd it would be if a homeowner yelled out to a police officer "Hey, there's a burglar in my house right now, help!", only to have the police respond, "Sorry, I have to apply for a court order first, try not to scare him off." The homeowner would be dumbfounded, and the burglar would be long gone by time the police returned. This, in essence, is what was occurring prior to the PATRIOT Act.

It can be said that section 217, in a very significant way, enhances privacy. First, it is carefully crafted to ensure that law enforcement conducts monitoring against trespassers in a manner entirely consistent with protecting the privacy rights of law abiding citizens. Second, the essence of the section—to help catch hackers—serves a vital function in the FBI's ability to enforce data privacy laws.

With respect to the first point, the narrowly crafted scope of this legislation, section 217 preserves the privacy of law-abiding computer users by sharply limiting the circumstances under which the trespasser exception may be used. At its most fundamental level, section 217 requires consent. Law enforcement assistance is by invitation only. The computer crime victim is actually seeking the FBI's help. In addition, a law enforcement officer may not conduct monitoring based solely on the computer owner or operator's consent unless the law enforcement officer is engaged in a lawful investigation; has reason to believe that capturing the communications will be relevant to that investigation; and can ensure that the consensual monitoring will acquire only those communications that are transmitted to or from the hacker. On top of these requirements, section 217 then goes one step further. Based on the definition of a "computer trespasser," section 217 does not allow law enforcement to come to the immediate aid of victims who are being hacked by one or more of their own customers. In those cases the owner or operator of the computer system cannot provide sufficient consent to monitor the trespasser, even if the hacker/customer broke into areas of the computer he has no authority to see (including other customer account information).

Still, despite this last limitation, the hacker trespasser exception has been an important tool for law enforcement to obtain evidence based on the consent of the victim, much of which involves protecting people's privacy.

A diverse array of real-world examples from our criminal investigations demonstrate that this provision has been significant in order for the FBI to protect the privacy rights of individuals and businesses whose computers are being broken into for the purpose of stealing the personal data stored on their computers. Hackers have no respect for your privacy or mine. When hackers break into a computer network and obtain root access they get to look at, download, and even can make changes to, whatever information is on that network. Hackers can and do routinely steal social security numbers, credit card numbers, and drivers license numbers. Depending on the systems they break into, they can look at health care information and can change it at will. There has been an outpouring of concern from the American public to protect them from identity theft and to ensure that their personal records are secure. Congress has responded with a powerful array of laws that are

designed to impose serious consequences on computer hackers. However, if law enforcement does not have the ability to quickly spot and then locate hackers, then the victim toll will mount and only the hackers themselves, remaining anonymous, will be left with privacy. The FBI understands the importance of preventing criminals from stealing and selling our information, and we are resolved to catch those who do. Section 217 is of enormous help in this regard.

For example, under this provision, the FBI was able to monitor the communications of an international group of "carders" (individuals that use and trade stolen credit card information). The group used chat rooms and fraudulent websites to commit identity theft, but managed to provide themselves with privacy by using false names to get e-mail accounts. The most important tool in their bid to remain anonymous was their use of a proxy server they broke into and then reconfigured. The identity thieves used the proxy server to disguise where all of their Internet communications were coming from. The owner of the proxy server was himself a victim of the crime, his computer having essentially been hijacked and transformed into the hub of a criminal operation. When he determined that his computer had been hacked he provided the FBI with consent to monitor the intruder and hopefully to catch him. The computer owner's ability to bring in the FBI paid off, not just for him but for the countless other victims of the identity thief. By taking advantage of hacker trespasser monitoring, the FBI gathered leads that resulted in the discovery of the true identity of the subject. The subject was later indicted and is now awaiting trial.

Since its enactment, section 217 has played a key role in a variety of hacking cases, including investigations into hackers' attempts to compromise military computer systems. Allowing section 217 to expire at the end of this year would help computer hackers avoid justice and prevent law enforcement from responding quickly to victims who are themselves asking for help.

SECTION 220—SEARCH WARRANTS FOR ELECTRONIC EVIDENCE LOCATED IN ANOTHER DISTRICT

Lastly, I would like to turn to section 220 of the USA PATRIOT Act. Section 220 enables federal courts—with jurisdiction over an investigation—to issue a search warrant to compel the production of information (such as unopened e-mail) that is stored with a service provider located outside their district. The practical effect of this section is that our FBI Agents are no longer limited to applying for a search warrant solely from the court that sits where the service provider happens to be located.

Before discussing this section in depth, I think it is helpful to point out that the borderless nature of Internet crime means that more often than not ***the victim**** of a crime, the person who committed the crime, and ***the evidence**** of that crime are all located in different parts of the country (or indeed the world). Applying this fact in the context of a search warrant will demonstrate the utility and the necessity of section 220.

Prior to the PATRIOT Act, if an investigator wanted to obtain the contents of unopened e-mail from a service provider located in the United States, he or she needed to obtain a warrant from a court physically located in the same federal district as the service provider was located. To accomplish this, the FBI Agent working on the case (this Agent typically would be located where the victim is located) needed to brief another FBI Agent and prosecutor who were located in the ISP's jurisdiction (where the evidence happened to be electronically stored). The second FBI Agent and prosecutor then would appear before their local court to obtain the search warrant. This was a time and labor consuming process. Furthermore, because several of the largest email providers are located in a few districts, such as the Northern District of California and the Eastern District of Virginia, these FBI Agents, Prosecutors, and Judges were faced with a substantial workload dealing with cases in which neither the victim nor the criminal resided, and they had to be brought up to speed about the details of an investigation which, both beforehand and afterwards, they had no need to know.

Section 220 fixed this problem. It makes clear, for example, that a judge with jurisdiction over a kidnaping investigation in Pittsburgh can issue a search warrant for e-mail messages that are stored on a server in California. As a result, the investigators in Pennsylvania can ask the judge most familiar with the investigation to issue the warrant rather than having to ask an Assistant United States Attorney in California, who is unfamiliar with the case, to ask a district judge in California, who also is unfamiliar with the case, to issue the warrant. Lest you think this is merely a hypothetical example, it's not. Using section 220, our FBI office in Pittsburgh was able to obtain a warrant for information residing on a computer in Cali-

fornia that ultimately led to the rescue of a teenage girl who was being sexually tortured in Virginia while being chained to a wall in somebody's basement. The man who held her hostage is now in prison, serving close to 20 years. The girl's life was saved.

Other FBI Field Offices also have repeatedly stated that section 220 has been very beneficial to quickly obtain information required in their investigations. The value of this provision in terrorism cases already has been demonstrated time and again. In his April 6 testimony, Attorney General Gonzales pointed to its important application during investigations into the Portland Terror Cell, the "Virginia Jihad", and the Richard Reid "shoebomber" case.

It is imperative that section 220 be renewed. The provision expedites the investigative process and, in doing so, makes it more likely that evidence will still be available to law enforcement after it executes a court-authorized search warrant and obtains further leads; the provision frees up FBI, U.S. Attorney, and judicial personnel to more efficiently pursue other time-sensitive investigative matters; and, section 220 in no way lowers the protections that apply to the government's application for a search warrant.

CONCLUSION

Mr. Chairman and Members of the Committee, the provisions of the USA Patriot Act I have discussed today have proven significant to a number of our successes and I have every reason to believe that the need to retain these provisions in the future is also significant. By responsibly using the statutes provided by Congress, the FBI has made substantial progress in its ability to enforce the law and protect lives, while at the same time protecting civil liberties. In renewing those provisions scheduled to "sunset" at then end of this year, Congress will ensure that the FBI will continue to have the tools it needs to combat the very real threats to America and our fellow citizens. Thank you for your time today.

Mr. COBLE. Thank you, Mr. Martinez. Mr. Dempsey?

TESTIMONY OF JIM DEMPSEY, EXECUTIVE DIRECTOR, CENTER FOR DEMOCRACY AND TECHNOLOGY

Mr. DEMPSEY. Mr. Chairman, Representative Scott, Members of the Subcommittee, good morning.

Mr. COBLE. Hold. If you will just suspend just a minute, Mr. Dempsey, I wanted to recognize the presence of the Gentlemen from Florida, Ohio, and Arizona to my right and the Gentleman from Massachusetts to our left.

Go ahead, Mr. Dempsey, and you won't be penalized for that time.

Mr. DEMPSEY. Thank you, Mr. Chairman. We commend you, Mr. Chairman, and Members of the Subcommittee and the full Committee leadership for undertaking this series of hearings on the PATRIOT Act. From this kind of detailed, objective inquiry, we can attain the balance that was left aside in the haste and emotion in the weeks after 9/11.

My main point today is that while, of course, the law needs to keep pace with changing technology to ensure that the Government can get the information that it needs to prevent crime and terrorism, at the same time the law also needs to keep pace with changing technology to protect privacy, especially as technology changes in ways that make ever larger volumes of information available to the Government, particularly to acquire from third parties.

The PATRIOT Act addressed only one side of this equation. Now is the time for Congress to address the privacy issues and finish the job.

Perhaps the biggest change that is happening in technology that increases governmental access to information and that affects pri-

vacy is the storage of more and more information on computer networks, and under the control of third parties. The kind of information that you would normally keep in your file drawer, even on your laptop in your own possession, that information is increasingly moving out onto networks, onto web-based storage. And the law just draws a distinction, and I think a now outdated distinction, between interception of communications in transit and access to those communications in storage. And it draws a further distinction between whether the e-mail is opened or unopened. If it's opened, it gets less protection than if it's unopened. If it's older, it gets less protection than if it's new.

Our recommendation is that Congress should take the Justice Department's description of 209, for example, the so-called voicemail provision, take their explanation and their description of that at face value and make seizure of all stored communications subject to a warrant.

The problem is that the way the law now works, if a stored voicemail is opened on your home answering machine—you listen to it, but you save it—it's protected fully by the fourth amendment, subject to a warrant. If it's opened on a third party server, it no longer is protected by the warrant requirement, which is why we say that section 209 is a little misleadingly named.

If that voicemail is older than 180 days or that e-mail is older than 180 days, it's not protected by the warrant requirement on the ISP computer, even though it is fully protected still if you've printed it out and put it in your file drawer, fully protected by the warrant requirement.

So Congress should eliminate this distinction, and, in fact, this Committee, the full Committee, did vote in 2000 to eliminate that distinction and to make all stored communications—whether opened or unopened, stored—I mean a long period of time or short period of time—subject to the same warrant requirement that the Justice Department refers to.

Turning just briefly to the interception of—and also to apply to those provisions some of the other protections in the law. Again, ensuring that the Government has the access, but, for example, we have absolutely no reporting on how often the Government accesses stored e-mail. We have very good and detailed statistical reports on live interceptions of e-mail and of phone calls through the annual wiretap report. But we really don't have a sense of access to stored communications. And as Professor Swire will describe now, with Voice Over IP, we're actually going to be seeing entire voice conversations stored for perhaps lengthy periods of time as the storage capacity is made available.

Section 217. This isn't quite like the homeowner. When the homeowner—the homeowner can invite the police into this property in order to find an intruder. But the homeowner cannot authorize the police to look in the pockets of the intruder. They cannot authorize the police to open up the briefcase of the intruder and read what's inside the briefcase. It requires another exception to the warrant requirement: search incident to an arrest, which we don't have here; protection of the officer, which we don't have here. So this isn't just like that homeowner search.

Nationwide service of warrants I think could be very nicely addressed by allowing those warrants to be challenged both in the jurisdiction in which they are issued and in the jurisdiction in which they are served. I think that's an equitable and minor change that would rebalance that.

Mr. Chairman, Members of the Committee, we look forward to working with you on these issues as we move forward between now and the end of the year. Thank you.

[The prepared statement of Mr. Dempsey follows:]

PREPARED STATEMENT OF JAMES X. DEMPSEY

Chairman Coble, Rep. Scott, Members of the Committee, thank you for the opportunity to testify at this important hearing. We want to commend the Subcommittee and the full Committee leadership for undertaking this series of hearings on the PATRIOT Act. From this kind of detailed, objective inquiry, we can attain the balance that was left aside in the haste and emotion of the weeks after 9/11.

Our main point today is that while, of course, the law needs to keep pace with changing technology to ensure that government agencies have access to information to prevent crime and terrorism, the law also needs to keep pace with changing technology to protect privacy, as technology makes ever larger volumes of information available for the government to acquire from third parties, without going to the subject of interest, as it used to have to do under the Fourth Amendment. The PATRIOT Act addressed only one side of this equation, making government access easier without counterbalancing privacy improvements. Now is the time for Congress to finish the job and address the privacy side of the equation.

In CDT's view, there are few if any provisions in the PATRIOT Act that are per se unreasonable. We see not a single power in the Act that should sunset. The question before us—and it is one of the most important questions in a democratic society—is what checks and balances should apply to those powers. With respect to the particular PATRIOT powers at issue in today's hearing, those time-honored checks and balances should include:

- Judicial review of intrusive techniques, preferably judicial approval before a search.
- Second, as a general rule, individuals should have notice when their communications are acquired by the government.
- Finally, government surveillance needs to be subject to Congressional oversight and some public accountability, including through more detailed unclassified reporting.

In one way or another, PATRIOT Act provisions fail to include these checks and balances.

PREVENTION OF TERRORISM DOES NOT REQUIRE SUSPENSION OF STANDARDS AND OVERSIGHT

At the outset, let me stress some basic points on which I hope there is widespread agreement:

- Terrorism poses a grave and imminent threat to our nation. There are people—almost certainly some in the United States—today planning additional terrorist attacks, perhaps involving biological, chemical or nuclear materials.
- The government must have strong investigative authorities to collect information to prevent terrorism. These authorities must include the ability to conduct electronic surveillance, carry out physical searches effectively, and obtain transactional records or business records pertaining to suspected terrorists.
- These authorities, however, must be guided by the Fourth Amendment, and subject to Executive and judicial controls as well as legislative oversight and a measure of public transparency.

THE LAW NEEDS TO KEEP PACE WITH TECHNOLOGY—BOTH TO PROVIDE APPROPRIATE TOOLS TO LAW ENFORCEMENT AND TO PROTECT PRIVACY

We have been told that this hearing will focus on three sections: 209 (misleadingly entitled "seizure of voice-mail pursuant to a warrant"); 217 (interception of computer trespasser communications); and 220 (nationwide service of search warrants for

electronic evidence). Sections 209, 217 and 220 are not among the most controversial provisions of the PATRIOT Act. The fact that they are subject to the sunset at all, while, for example, the "sneak and peek" authority in Section 213 and the national security letter expansions in Section 505 are not subject to the sunset, illustrates how the debate over the sunsets is somewhat misplaced.

As with most other sunsetted provisions, there is little call for denying government the access to information provided under Sections 209, 217 and 220. Rather, the questions posed by these sections are matters of checks and balances, related to the continuing but uneven effort to rationalize the standards for government access to electronic communications and stored records in the light of ongoing changes in technology. It is worth noting that Sections 209, 217 and 220 have no direct connection with terrorism. They apply to all criminal cases.

These sections highlight an overarching concern about the way in which amendments to the surveillance laws in recent years, and especially in the PATRIOT Act, have served as a "one-way ratchet" expanding government power without corresponding improvements in the checks and balances applicable to those powers. This has been a departure from Congress' traditional approach to electronic surveillance issues. In the first major wiretap statute, Title III of the 1968 Omnibus Crime Control Act; in the Electronic Communications Privacy Act of 1986; and even in the controversial Communications Assistance for Law Enforcement Act of 1994, Congress and the Justice Department agreed on the twin goals of ensuring law enforcement authority to intercept communications while also strengthening privacy protection standards, especially in light of changing technology.

This spirit of balance has unfortunately been lost. In recent years, time and again, the Department of Justice has proposed changes in the surveillance laws that reduce judicial oversight or increase Executive Branch discretion, and Congress has too often enacted them, without ever considering how these changes add up or whether other changes may be needed to increase privacy protections in response to advancements in technology that have made the government's surveillance more intrusive. Sometimes, as with the PATRIOT Act, this one-way expansion of government power occurs in a time of intense crisis. Sometimes, these changes occur stealthily, like the "John Doe roving tap" change that was added to FISA in December 2001 by the conference committee on the intelligence authorization act without having passed either the House or the Senate. Other one-sided and little debated expansions in the government's discretion include the expansion of ECPA's emergency disclosure authorities in the legislation creating the Department of Homeland Security, Pub. L. 107–296, Sec. 225(d). (That at least included a reporting requirement, which should be made annual.) A further exception to ECPA was made by Section 508(b) of the Prosecutorial Remedies and Other Tools to end the Exploitation of Children Today (PROTECT) Act of 2003, Pub. L. 108–21, which allowed disclosure without a warrant or subpoena of the contents of communications and subscriber identifying information to the National Center for Missing and Exploited Children, which in turn can disclose the information to law enforcement agencies. Changes to Title III's roving tap authority were adopted in the Intelligence Authorization Act for Fiscal Year 1999, Pub. L. 105–272, Title VI, Sec 604, Oct 20, 1998, 112 Stat 2413 (permitting roving taps to be implemented if "it is reasonable to presume that the person identified in the application is or was reasonably proximate to the instrument through which such communications will be or was transmitted"). And Section 731 of the 1996 anti-terrorism act excluded interception of wireless data transfers and of information about electronic funds transfers from the coverage of Title III.

Each of these changes is small in isolation, and each had a rationale. None, however, was considered in the context of other, long-recognized changes that need to be made to strengthen the privacy protections of the electronic surveillance laws, including:

- extending Title III's statutory suppression rule to electronic communications, a change even the Justice Department once supported;
- increasing the standard for pen registers and trap and trace devices, to give judges meaningful oversight, a change the full Judiciary Committee supported in 2000;
- eliminating the distinctions between opened and unopened email and between relatively fresh and older email, by bringing all stored email under a warrant standard, another change the Committee supported in 2000;
- establishing a probable cause standard for access to location information, a change this Committee also supported in 2000;

- requiring reporting on access to email, also supported by the Committee in 2000.

With this context in mind, it is easier to see why even some of the minor changes in the PATRIOT Act draw concern, for they are part of a steady stream of uni-directional amendments that are slowly eroding the protections and limits of the electronic privacy laws.

SECTION 209—SEIZURE OF VOICE-MAIL MESSAGES PURSUANT TO WARRANT

Section 209 is described as permitting the seizure of voicemail messages pursuant to a search warrant. Previously, while voicemail messages stored on an answering machine in one's home could be seized by a search warrant, access to voicemail messages stored with a service provider had required a Title III order, which offers higher protections. The theory behind section 209 is that stored voice messages should be treated the same as stored data.

On one level, Section 209 makes the rules technology neutral, which is usually desirable. If Section 209 is taken at face value, and if the only difference it effects is between a Title III order and a search warrant, both issued on probable cause, Section 209 does not represent a big change. For this reason, CDT has described Section 209 as one of the non-controversial provisions of the PATRIOT Act.

However, as Prof. Swire points out, Section 209 is misleadingly titled: Because the law that was amended by 209 draws some bizarre distinctions between read and unread email and between newer and older email, Section 209 means that a lot of stored voice communications will be available not with a warrant but under a mere subpoena.

Moreover, the Justice Department's explanation of Section 209 overlooks the importance of notice under the Fourth Amendment and under Title III, and the absence of notice under the rules applied to stored material held by a service provider. When voicemail stored on your home answering machine is seized, you are normally provided notice at the time of the search. You can examine the warrant and immediately assert your rights. When email or voicemail is seized from a service provider pursuant to a warrant, you as the subscriber may never be provided notice unless and until the government introduces the information against you at trial. If you were mistakenly targeted or the government chooses not to use the evidence, you need never be told of the search of your stored communications, so you have little meaningful opportunity to seek redress.

In the case of stored messages (whether email or voicemail), it is not even necessary from an investigative standpoint to deny contemporaneous notice in the way it is with live interception. Denial of notice is justified in the case of real-time interceptions because the effectiveness of the technique would be destroyed if the target were given contemporaneous notice. In the case of stored email or stored voice messages, the evidence is already created and, especially if notice is given immediately after seizure, the subject cannot destroy it. Denial of notice in the case of third party searches for stored email or voicemail is not justified.

Recommendation: Congress should take the Justice Department's description of Section 209 at face value, and make all seizure of stored communications, whether voice or email, subject to a warrant. It could do so by eliminating the difference between opened and unopened stored records and between records 180 days old or less and records more than 180 days old. It should take the Justice Department's arguments at face value and adopt truly technology neutral rules for voice and data, whether in transit or in storage, applying the protections afforded under Title III:

- minimization of non-relevant material,
- notice to persons whose communications have been intercepted,
- a statutory suppression rule, and
- detailed statistical reports to Congress and the public.

All of these protections apply to e-mail and voice when intercepted in transit. None of them apply to e-mail and voice seized from storage.

The Storage Revolution Is Rendering the Law Obsolete

A storage revolution is sweeping the field of information and communications technology. Service providers are offering very large quantities of online storage, for email and potentially for voicemail. Increasingly, technology users are storing information not in their homes or even on portable devices but on networks, under the control of service providers who can be served with compulsory process and never have to tell the subscribers that their privacy has been invaded. New Voice over Internet Protocol (VoIP) services may include the capability to store past voice con-

versations in a way never available before, further obliterating the distinction between real-time interception and access to stored communications.

Section 209 takes a seemingly small category of information out of the full protection of the Fourth Amendment and moves it under the lowered protections accorded to remotely stored communications and data. But stored voicemail is the tip of an iceberg. Increasingly, individuals are using stored email to store documents, including draft documents on computers operated by service providers and accessed through a Web interface.

Rather than allowing growing amounts of personal information to fall outside the traditional protections of the Fourth Amendment, it is time to revisit the rules for networked storage (whether of voice or data) and bring them more in line with traditional Fourth Amendment principles, by requiring contemporaneous notice as the norm and covering both newer records and older records (again, whether voice or data) under the same probable cause standard. That would be truly technology neutral and would have the advantage of not allowing technology advances to erode privacy protections.

Section 217—Interception of computer trespasser communications

Section 217 permits law enforcement agencies to carry out electronic surveillance of without a court order when the service provider permits the surveillance on the ground that a "trespasser" is using its system. Section 217 represents another in a steadily growing series of exceptions to the protections of the electronic communications privacy laws. (The emergency disclosure provision of Section 212 is another example.)

Section 217 and similar provisions essentially allow "off the books surveillance"—they define certain interceptions not to be interceptions, and certain disclosures not to be disclosures. Once an access to communications or data is excluded from the coverage of the surveillance laws, not only is it not subject to prior judicial approval, but also there are no other protections normally associated with electronic surveillance:

- There is never a report to a judge. (In contrast, under both Title III and FISA, when electronic surveillance is carried out on an emergency basis, an application must be filed after the fact.)
- There is no time limit placed on the disclosures or interceptions. (A Title III wiretap cannot continue for more than 30 days without new approval.)
- There is never notice to the person whose communications are intercepted or disclosed.
- There is no statutory suppression rule if the communications were improperly seized, and there would be no suppression remedy at all if the information is deemed to be outside the protection of the Fourth Amendment.
- The interceptions and disclosures are not reported to Congress or the public.

The Department of Justice, in its defense of Section 217, claims that the privacy of law-abiding computer users is protected because only the communications of the computer trespasser can be intercepted. But what if the system operator is wrong? What if there is a legitimate emergency, but law enforcement targets the wrong person? Under Section 217, a guilty person gets more notice than an innocent person—the guilty person is told of the surveillance or disclosure but the innocent person need never be notified.

Contrary to the Department's arguments, Section 217 is not analogous to the case of the home trespasser. While the homeowner can invite in the police onto his property, the homeowner cannot authorize the police to go through the trespasser's pockets or read the papers in his briefcase. To do so requires a separate Fourth Amendment basis, which would require a warrant unless one of the exceptions applied, and in the online context, there may be no other exception available.

Recommendation: While an emergency exception to the court order requirement may be appropriate for trespasser situations, interceptions under the trespasser rule should be treated as interceptions under Title III:

- As with other emergency interceptions, when electronic surveillance is carried out on an emergency basis, an application for judicial approval must be filed after the surveillance commences
- The length of interceptions should be limited to the time necessary to identify the trespasser or for 30 days, whichever is less
- Interceptions under the trespasser rules should be treated as interceptions for purposes of giving delayed notice to the person whose communications are intercepted.

- Interceptions under the trespasser rules should be treated as interceptions for purposes of the statutory suppression rule.
- Interceptions under the trespasser rule should be counted as interceptions for Title III purposes and included in the annual Wiretap Report.

Section 220—Nationwide service of search warrants for electronic evidence

Section 220 amended 18 U.S.C. 2703 to allow judges to issue search warrants for electronic evidence that can be executed outside of the district in which the issuing court is located. In a world where the center of an investigation may be in one state, but the target's ISP has its servers in another state, this makes obvious sense. Moreover, unlike Section 216, which authorizes a kind of roving pen register (one order can be served on multiple service providers in different districts until the government gets the full picture it wants), it seems that search warrants under Section 220 have to name the service provider upon whom they will be served. If it turns out that that provider does not have the records being sought, the government will have to obtain a new search warrant (as it would any time a search warrant does not turn up the expected evidence.)

However, as the Electronic Privacy Information Center has noted, Section 220 removes "an important legal safeguard by making it more difficult for a distant service provider to appear before the issuing court and object to legal or procedural defects. Indeed, it has become increasingly common for service providers to seek clarification from issuing courts when, in the face of rapidly evolving technological changes, many issues involving the privacy rights of their subscribers require careful judicial consideration. The burden would be particularly acute for smaller providers."

Recommendation: One solution to this problem is to allow a warrant to be challenged not only in the district in which it was issued but also in the district in which it is served. While the issuing judge may have a better sense of the factual basis for the order, a judge in the district in which the order is served may be in a better position to interpret or redefine the scope of the order in light of issues concerning the system of the service provider on whom the order is served.

Even aside from Section 220, whether search warrants for electronic evidence are issued for evidence inside or outside their jurisdictions, judges should question applicants to be sure that the warrant is narrowly drawn. Judges should use extra care in understanding what information is being sought, whether it will be copied or originals will be seized (interfering with ongoing business), and whether it is possible to disclose just certain fields or just records from a certain pertinent timeframe. These are analogous to questions that judges have the authority to consider in the case of physical searches, but judges need to understand computer systems in order to fully enforce the specificity requirement of the Fourth Amendment in the digital context. Judges should look more carefully at the return of service. While notice under 18 U.S. C. 2705(b) can be prohibited, judges should be hesitant to deny notice to the person to whom the records pertain, since the subscriber is really in the best position to raise legitimate concerns. This is just another way in which judges faced with the authorities of the PATRIOT Act can assert closer scrutiny and place conditions on the exercise of PATRIOT authorities without denying the government access to the information needed.

CONCLUSION

CDT supports the Security and Freedom Enhancement (SAFE) Act, a narrowly tailored bipartisan bill that would revise several provisions of the PATRIOT Act. It would retain all of the expanded authorities created by the Act but place important limits on them. It would protect the constitutional rights of American citizens while preserving the powers law enforcement needs to fight terrorism.

We look forward to working with this Subcommittee and the full Committee as you move forward in seeking to establish some of the checks and balances that were left behind in the haste and anxiety of October 2001.

Mr. COBLE. Thank you, Mr. Dempsey. Professor Swire.

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

Mr. SWIRE. Thank you, Mr. Chairman, and Mr. Ranking Member, and Members of the Committee. I appreciate very much the opportunity to testify before you today.

Most of my remarks today will be on section 209 of the PATRIOT Act, the section that expanded the Government's access to voicemail and many other telephone conversations without the need for a wiretap order.

Before turning to that, I will briefly comment on the other two sections that are the subject of today's hearing.

Both section 220, on nationwide service of warrants, and section 217, the computer trespasser exception, were considered in detail when I chaired a White House Working Group in 2000 on how to update surveillance law for the Internet Age. As my written testimony explains in greater detail, I generally support extension of section 220 although with some refinements that Jim Dempsey has in his written testimony.

For section 217, however, modifications should be made. Section 217 solves some important real-world problems. It lets a computer system owner ask the police for help when their system is under attack. With the owner's permission, law enforcement can surf over the shoulder of the system operator in order to spot the hacker and track him back through the Internet. That's the good news.

The bad news, though, is that there are no checks against abuse in the section. Section 217 says the police are only supposed to look at the communications of the hacker. But if the police look at other e-mail and web traffic they can still use all that information. They can use it in future investigations. They can use it in court. The incentives for law enforcement are to get permission to enter the system under 217, and then see how much they can get to see while they're there.

As my written testimony explains, there is a simple solution to this. It's the same solution that this Committee, the Judiciary Committee in full, passed in 2000, with only one dissenting vote. The simple solution is that the same suppression rule that applies to phone wiretaps should also apply to e-mails. If law enforcement breaks the legal rules, if they go too far and break the law, they should not get to use the fruits of the illegal search.

The rest of my time I'm going to spend on section 209. It turns out that section 209 has much broader ramifications than most people realize—than I realized before I was asked to testify this week.

Section 209 allows the Government to get access to voicemails and many telephone conversations with much less than a wiretap order. The actual textual change in 209 is simple. The old law said that stored electronic records were under looser rules of the Stored Communications Act. All the PATRIOT Act did was say stored wire or electronic records; wire means any voice, telephone calls, voicemail sorts of records.

In many instances under section 209 now, law enforcement can get your stored, but also stored voice now with a grand jury subpoena, where there's no judge involved at all or else with a judicial order that requires much less than probable cause.

Section 209 was given to the Congress and to the public as if it were only about voicemail. It does apply to voice mail, which are stored telephone communications, but that's not all. The key new thing I think we're learning is that section 209 applies to any and

all telephone conversations that are stored. The term "voice mail" does not exist in the statutory text, except in the title.

Should any of us care about stored telephone conversations? The answer is yes. The simple technological fact is that stored telephone conversations are becoming much more common due to changing phone technology. Every major telecomm company is part of this shift. SBC, Comcast, Verizon, Qwest—all of them are implementing right now major moves into this new phone technology. The new technology has a clumsy name, VOIP, which means Voice over Internet Protocol. What it means is that telephone conversations are shifting to this Internet protocol. What that means, in turn, is that telephone conversations are being stored at home and in the network for millions of Americans.

The numbers for this change are big and they are real. This is not Internet hype. The phone software called Skype has now recorded over 100 million downloads. Over 20 percent of all new business phones already use this technology, with estimates of over half of new business phones within 3 years. Growth rates in the residential sector are over 30 percent a year.

Because VOIP uses the Internet to transmit voice, all the tools that make the internet work come into play. The Internet tool that section 209 takes advantage of is called caching. Just as your web browser stores graphics and images in its caches, ordinary users can and will have their phone conversations stored or cached at the Internet network level. People won't even realize their phone conversations are being stored, putting their phone calls at risk of being seized with much less than a wiretap order.

What should be done with section 209? The first thing is that you shouldn't simply take my word for these changes. You should ask the Department of Justice. They're here today and my written testimony suggests questions you can pose to the Department. And this way, all of us will know what the new law really means.

My written testimony suggests possible changes to be done to address this concern, and in conclusion I thank the Committee for the opportunity to share these thoughts.

My written testimony contains citations to my law review and other writings on the PATRIOT Act, and if I can be of assistance in the future, please do not hesitate to ask.

[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 209*: Seizure of Voice-Mail Messages Pursuant to Warrants; *Section 217*: Interception of Computer Trespasser Communications; and *Section 220*: Out-of-District Service of Search Warrants for Electronic Evidence

April 20, 2005

Mr. Chairman, Mr. Ranking Member, I thank the Committee very much for the opportunity to testify before you today on Sections 209, 217, and 220 of the Patriot Act. This testimony gives my relevant background. It supports renewal of Section 220, the nationwide service of search warrants for electronic evidence. For Section 217, the computer trespasser exception, I believe that the exception should only be renewed if Congress takes a simple step to assure that it will be used only as intended. I therefore believe that any renewal of that provision should depend on also enacting a suppression remedy for electronic communications that are seized and go beyond the limited scope permitted by the provision. For Section 209, which is entitled "seizure of voice mail messages pursuant to warrants," this testimony suggests that the provision affects a much greater portion of telephone communications than has been previously understood. I therefore devote the bulk of my testimony to that issue.

Background

I am now Professor of Law and John Glenn Scholar of Public Policy Research at the Moritz College of Law of the Ohio State University. I am Director of that school's Washington summer internship program, and live in the Washington, D.C. area.

From 1999 until early 2001 I served as the Chief Counselor for Privacy in the U.S. Office of Management and Budget. In that role, I participated in numerous privacy, computer security, computer crime, and related issues. Of most relevance to today's hearing, early in 2000 I was asked by John Podesta, the President's Chief of Staff, to chair a 15-agency White House Working Group on how to update electronic surveillance law for the Internet Age. The Working Group met intensively over a period of several months.

The Administration's draft legislation was announced in June, 2000 and introduced as S. 3083. Roughly speaking, the Administration bill contained a third or a half of the increased surveillance powers that were later included in Title II of the Patriot Act. The Clinton Administration bill also contained important privacy protections. These privacy protections included treating "electronic" communications, such as e-mails and web surfing, with the same protective standards that apply to phone calls and other "wire" and "oral" communications. Our proposal at that time also included raising the standard somewhat for pen register and trap and trace orders.

After hearings, this Committee considered the issues in the fall of 2000. Interestingly, the Committee at that time criticized the Administration plan for being out-of-balance and not protective enough of citizen privacy. The Committee voted out H.R. 5018 overwhelmingly, with only one dissenting vote. The Committee bill notably included the same suppression remedy for "electronic" evidence that exists for "oral" and "wire" communications. The Committee also raised the standard for pen register and trap and trace orders, making clear that the judge should exercise discretion in granting such orders and stating that orders should be issued only where there are "specific and

articulable facts" to support the order. Despite the nearly unanimous Committee support, the bill ran out of time in the 106th Congress. As the House Judiciary Committee considers electronic surveillance issues this year, I believe that members and staff may find it informative to revisit the debates from the fall of 2000, in order to see how these precise issues were addressed during the extended deliberations that occurred at that time.

I left the government and returned to law teaching in January, 2001. After the attacks of September 11, I participated in the public debates surrounding the Patriot Act. Many of the issues in today's hearing were addressed in a paper I wrote at that time for the Brookings Institution, entitled "Administration Wiretap Proposal Hits the Right Issues But Goes Too Far," available at http://www.brookings.edu/dybdocroot/views/articles/fellows/2001_swire.htm. That paper discussed the computer trespasser exception in Section 217 and nationwide trap-and-trace orders in Section 220. The paper especially stressed the importance of including a sunset provision in the Patriot Act. The hearings this year, I believe, show the wisdom of Congress in doing that. If sunset provisions are not included in surveillance law, then the Department of Justice has little or no incentive to come to the Congress, explain clearly the current state of the law, and set priorities among its proposals for expanded surveillance authority. Including some sunset in this year's reform bill would give this Committee, the Congress, and the American people a better opportunity to set good policy and have informed debate on these issues again in the future.

Since passage of the Patriot Act, a large portion of my academic research has been on the new surveillance provisions. With Charles Kennedy, I wrote "State Wiretaps and Electronic Surveillance After September 11," 54 Hastings L.J. 971 (2003), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=416586. My longest article in this area is "The System of Foreign Intelligence Surveillance Law," 72 Geo. Wash. L. Rev. 1306 (2004), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=586616. This article presents the most detailed history and explanation to date of the Foreign Intelligence Surveillance Act, including over a dozen reform proposals that affect Sections 215, 218, 505 and other portions of the Patriot Act. As discussed below in this testimony, I wrote "*Katz* is Dead, Long Live *Katz*," 102 Mich. L. Rev. 904 (2004), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=490623. This article draws attention to the dramatic reduction in privacy for our phone calls that is resulting from changing technology. In addition, I have written on Sections 214 and 215 for the www.patriotdebates.com sponsored by the American Bar Association. Requests for printed copies of these writings can be sent to Ms. Carol Peirano, Moritz College of Law, 55 West 12th Ave., Columbus OH 43210. I hope that this writing, and other materials at www.peterswire.net, will be of use to the Committee and other interested persons as these important issues are considered.

Section 209, Incorrectly Titled "Seizure of Voice Mail Messages Pursuant to Warrants

It is especially important that the Committee direct its attention to the incorrect title of Section 209. In the Patriot Act, this section is called "Seizure of Voice Mail Messages Pursuant to Warrants." The Computer Crimes and Intellectual Property Section of the Department of Justice, in its Field Guidance on the Patriot Act, gives a more accurate title: "Obtaining Voice-mail and Other Stored Voice Communications." http://www.usdoj.gov/criminal/cybercrime/PatriotAct.htm. The fact that Section 209 applies to all stored voice communications makes it much more far-reaching than the misleading current title of Section 209 indicates.

Some brief history helps explain what is at stake. The 1928 case of *Olmstead v. United States*, 277 U.S. 438 (1928), held that wiretaps were not a "search" under the Fourth Amendment where they were conducted outside of the home. *Olmstead* was overruled in the famous cases of *Katz v. United States*, 389 U.S. 347 (1967), and *Berger v. New York*, 388 U.S. 41 (1967), which established that the Fourth Amendment does apply to telephone wiretaps and other communications where there is a "reasonable expectation of privacy." In 1968, Congress passed a federal wiretap statute in Title III of that year's crime bill. Title III set strict national rules for wiretaps of "wire" communications (such as phone calls) and "oral" communications (such as ordinary conversations that are bugged).

In 1986, Congress passed the Electronic Communications Privacy Act. ECPA extended many of Title III's protections to "electronic" communications, which include e-mail and web surfing. Notably, a strict Title III order is required before law enforcement can intercept electronic communications. Although most of the phone wiretap protections apply, three do not: (1) interceptions are permitted for any crime, rather than the list of serious felonies in 18 U.S.C. § 2516; (2) the high-level approval within the Justice Department required under 18 U.S.C. § 2518 is not required for "electronic" interceptions; and, most importantly, (3) the statutory suppression remedy under 18 U.S.C. § 2515 does not apply to "electronic" interceptions. The Clinton Administration proposal in 2000 would have changed these three provisions, providing the same privacy protections against wiretaps of e-mails as exists for phone calls. This Committee almost unanimously voted for those changes in 2000.

ECPA also created for the first time a federal regime that governs access to stored electronic communications. Congress correctly recognized that computers and other new information technology make it much more common for ordinary persons to have their communications stored in electronic form, often in the hands of an Internet Service Provider or some other third party. After lengthy debate, Congress decided in the Stored Communications Act to give these stored records less protection than applies to contemporaneous communications such as a phone call or an e-mail as it travels from sender to recipient.

The rules for government access to the contents of stored electronic communications are much less strict than for wiretaps of phone calls or bugging of oral communications. Instead of the special Title III wiretap requirements, an ordinary probable cause search warrant is sufficient to see e-mail and other stored electronic communications. In many instances, the contents of stored communications can be accessed by a grand jury subpoena or an order under 18 U.S.C. § 2703(d), which permits access to stored communications where there are "specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." For further discussion of the rules on stored communications, see Susan Freiwald, "Online Surveillance: Remembering the Lessons of the Wiretap Act," 56 Alabama L. Rev. 9 (2004) (emphasizing privacy perspective); Orin Kerr, "A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It," 72 Geo. Wash. L. Rev. 1208 (2004) (emphasizing law enforcement perspective).

It was against this backdrop that Congress enacted Section 209 of the Patriot Act. That provision makes a seemingly simple change to the law of stored communications. Previously, the contents of only stored *"electronic"* communications were available under the looser rules of the Stored Communications Act. Section 209 applies the looser rules to all stored *"wire or electronic"* communications. Even though the Patriot Act calls this provision "Seizure of Voice Mail Messages Pursuant to Search Warrant," there is no mention of "voice mail" in the statutory text, and many messages may be obtained with much less than a search warrant.

This precise change in the law was debated within the Clinton Administration in 2000 as we put together our legislative proposal. At that time, advocates for the change argued that the new power would be useful for investigating stored, unopened voice mails. They also argued that people have a lower expectation of privacy in a voice-mail than in a phone call, because people understand the possibility that someone else might hear the voice mail. On the other hand, opponents of the change argued that people expect privacy in a voice mail much as they do in a phone conversation – both are generally private communications and deserve the full protections that apply where there is a "reasonable expectation of privacy." Eventually, the change was not included in the legislative proposal.

Based on my continued research, I have come to believe that Section 209 sweeps far more broadly than has been publicly discussed. What if the contents of ordinary telephone calls become stored as a matter of routine? This storage is likely to become far more common with the imminent growth of Voice over Internet Protocol ("VoIP") telephone calls. VoIP uses the packet-switching network of the Internet to connect telephone calls rather than the traditional circuit-switching used by established phone systems. The Wall Street Journal has reported estimates that about 20% of new phones shipped to U.S. businesses now use VoIP technology, with that number exceeding 50% by 2007. Wall St. Journal, Jan. 12, 2004, at R7. Residential use will follow quickly, spurred by the expected low cost of international and other long-distance calls.

Use of VoIP is likely to result in a drastic increase in storage of the content of telephone calls for at least two reasons. First, the use of computers for making telephone calls makes it trivially easy for one party to store the contents of the conversation. This ease of storage comes at a time of plummeting cost of computer storage, as shown in the enormously greater size of today's typical hard drives. Ordinary users may store phone calls in the future the way they store e-mails and photos today or log their instant message sessions.

A second technological change with VoIP is the likelihood that there will be systematic "caching," or storage, of telephone communications at the network level. One existing product, for instance, is called "CacheEnforcer." CacheEnforcer stores communications for a group of users, such as for a company or a network operated by a university. Network managers, not individual users, determine the caching procedures. The caching can help the network in various ways including improving average network speed and assisting in network security. The product website says: "Because the CacheEnforcer sits in front of your WAN [wide area network] or Internet link, all outbound traffic passes through it. By setting appropriate policies on the CacheEnforcer, network managers, not individual users, determine the appropriate caching policies for the entire network." www.allot.com/html/products_cacheenforcer.shtm. Once "all outbound traffic" can be stored, then many, many telephone calls will be subject to the lower protections for stored records.

In a recent article in the Michigan Law Review, I discussed how these trends undermine the constitutional protections for the privacy of telephone conversations. "*Katz* is Dead, Long Live *Katz*," 102 Mich. L. Rev. 904 (2004), available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=490623. Because the Supreme Court has found that people lack a "reasonable expectation of privacy" in some stored records, e.g., Smith v. Maryland, 442 U.S. 735 (1979) (stored lists of phone numbers dialed), there is a serious risk that the stored phone calls of our near future will no longer be protected by the Fourth Amendment. If that is the case – and current doctrine suggests it is – then it is entirely up to Congress to define the standards for accessing these phone calls. *See* Patricia L. Bellia, "Surveillance Law Through Cyberlaw's Lens," 72 Geo. Wash. L. Rev. 1375 (2004) (analyzing *Miller* and related doctrine).

If Section 209 is retained in its current form, then the stored phone calls of our near future will be available to law enforcement with less than a probable cause warrant. Now we see how misleading it is to describe Section 209 as "seizure of voice mail messages pursuant to warrants." Section 209 applies to *all* stored "wire" communications (that is, to all stored telephone communications), and not just to voice mail. In addition, Section 209 would often allow law enforcement access to these conversations with less than a warrant, such as through a 2703(d) order.

What is to be done with Section 209? To avoid deception, the first step is to rename it to match the statutory text: "Seizure of stored telephone communications with less than a wiretap order." Next, this Committee should place questions to the

Department of Justice to confirm its understanding of the issues discussed here. At the end of my testimony I have proposed a set of questions to help uncover the actual effect of Section 209 on telephone communications. Asking these questions will go a long way toward creating a shared understanding of what is and is not implicated by a renewal of Section 209. That shared understanding, in turn, is essential to any informed consideration of what legislative steps to take.

In terms of possible actions, one option of course would be to let the provision sunset. The argument in favor of this option is that Section 209 is a wide-ranging authorization for the government to listen to phone conversations with less than a wiretap order. In light of that large effect on listener privacy, the relatively small gains to law enforcement due to access to voice mails quite possibly are not worth it.

A second option would be actually to amend the statute to match its current name – voice mails placed by one person could be governed by Section 2703, but communications among two or more parties would be governed by the wiretap laws. To address one practical issue raised by the Department of Justice in its Field Guidance on Section 209, it may be possible for law enforcement in good faith to open files where it does not reasonably believe that the files contain stored wire communications, but then apply the statutory suppression remedy of Section 2515 to prevent use of the inadvertently-opened files in subsequent investigations and proceedings.

Based on responses by the Department of Justice, it may be possible to develop other options that meet priority law enforcement needs without opening a large fraction of telephone calls to surveillance with less than a wiretap order.

Section 217, The Computer Trespasser Exception

I am sympathetic to having some form of the computer trespasser exception in Section 217, but the current version lacks logical safeguards against abuse. The discussion here gives the rationale for the provision, and then explains the needed safeguards, which should include written authorization, reporting requirements, and a statutory suppression remedy.

The problems that led to creation of Section 217 are discussed in my 2001 article "Administration Wiretap Proposal Hits the Right Issues But Goes Too Far," available at http://www.brookings.edu/dybdocroot/views/articles/fellows/2001_swire.htm, and in Orin S. Kerr, "Internet Surveillance Law After the USA PATRIOT Act: The Big Brother That Isn't," 97 Nw. U. L. Rev. 607 (2003). In brief, problems arose in how law enforcement could work with the owners of computer systems that are under attack. The pre-2001 law generally allowed a system owner to monitor the system to prevent and respond to attacks. It also allowed a system owner to turn over to police evidence of criminal attacks that had already occurred. What the pre-2001 law did not allow, however, was for law enforcement to "look over the shoulder" or "surf behind" the owner of the computer system. The policy concern about "looking over the shoulder" is that it can lead to too much surveillance. Law enforcement and system owners could agree that

the law enforcement officials would be permanently stationed in communication companies, monitoring anything suspicious. A particular concern is that system owners might feel pressured to allow law enforcement officials on the premises, leading to virtually unlimited wiretapping.

The pre-2001 rules were frustrating for system owners who wanted to ask the police for help with computer attacks. If intruders are coming into a system regularly, for instance, the owner might want the police to lie in wait for the attack and then use a trap and trace order to follow the intruder back to the source. Before 2001, however, the police could not take up residence and wait for a future attack. The problem was especially acute for the Department of Defense, which is subject to an enormous number of hacking attacks and which could not coordinate easily with law enforcement under the pre-2001 rules. The pre-2001 law also posed problems for smaller enterprises, which often lack the technical expertise to defend their own systems against attack and thus wish to have police help.

The idea of the computer trespasser exception first surfaced within the Department of Justice in 1999. We discussed it within the Administration during 2000, but it was not a subject of Congressional hearings and we did not include it in our 2000 proposal. The idea was included in the Bush Administration's proposal and was enacted in the Patriot Act. Because the idea was so new, it was properly made subject to the sunset provision, so that this Committee and the entire Congress can consider how to proceed.

In considering Section 217, I believe the Committee should have two simple goals in mind: (1) Section 217 should enable system owners and law enforcement to coordinate effectively in facing hacker attacks; and (2) Section 217 should not become a license for widespread wiretapping by law enforcement. My view is that the current language does an effective job of meeting the first goal. The current language, however, lacks the logical safeguards that are needed to achieve the second goal, and I therefore propose three modifications.

First, the authorization from the owner or operator of the system should be in writing. Currently, one of the requirements to use the computer trespasser exception is that "the owner or operator of the protected computer authorizes the interception." My proposed change is to insert "in writing" after "interception." This simple step will be eminently routine in ordinary investigations. It will provide the name of the person inside the organization who takes responsibility for inviting law enforcement to review the e-mails and other computer traffic at the organization. If there is any dispute after the fact about what happened, law enforcement will have the benefit of being able to show the authorization. The system owner or operator will have the benefit of knowing that an employee has taken a proven, written step to authorize law enforcement to enter. That will reduce the risk that any law enforcement officers will talk their way into a computer system without true consent by the system owner. In addition, customers and users of the system will have the benefit of knowing that the system owner actually did consent to having communications monitored. Overall, a simple writing requirement reduces the

risk of irregularity before the monitoring of communications occurs.

Second, Section 217 should have reporting requirements to Congress and the public. So far as I know, there is currently no public information about how often and in what contexts Section 217 has been used. This sort of public reporting would reduce the risk that Section 217 will be used in a widespread way to wiretap communications.

Third, and most importantly, there should be a statutory suppression remedy for exceeding the scope of permitted wiretapping. I will briefly explain the reasons to have a suppression remedy generally for "electronic" communications, and then show why the need is especially compelling with respect to Section 217.

Since 1968, Title III has had the suppression remedy of 18 U.S.C. § 2515 for all "wire" and "oral" communications. This rule was initially introduced in the wake of extensive evidence of persistent and illegal wiretaps under previous law, such as the abundant documentation in the American Bar Association study led by Samuel Dash. In the ECPA compromise in 1986, interception of e-mails and other "electronic" communications were made subject to the strict Title III standards, except the suppression remedy was not included. The Clinton Administration recommended the suppression remedy to Congress in 2000, and this Committee approved it with only one dissenting vote. Then, unfortunately, the provision was not included in the Bush Administration proposal in 2001 and it is not current law.

The lack of a suppression remedy means that law enforcement can violate the wiretap laws with respect to e-mail and web surfing with essentially no legal repercussion. The likelihood of criminal prosecution against a law enforcement official for wiretapping is remote or non-existent – the first such prosecution has not yet been brought. Any suppression remedy under the Fourth Amendment is highly speculative at this time, when it is not even clear that the courts would find a constitutional "reasonable expectation of privacy" in e-mails. This lack of a statutory suppression remedy obviously creates a risk to due process and privacy, because the fruit of illegal access to e-mail can be used in investigations and introduced in court. Importantly, as Professor Orin Kerr has persuasively argued, the lack of a suppression remedy also impedes law enforcement. The reason is that there is a great lack of clarity of how the law applies to new technology. Having a suppression remedy, in the eyes of former DOJ prosecutor Kerr, would assist investigations because the lines of permitted and prohibited behavior would be clarified. Kerr also points out that current interpretation of the surveillance law for "electronic" communications largely occurs in civil cases, and having a suppression remedy would allow the Department of Justice a much greater and more effective role in shaping that law over time. Orin S. Kerr, "Lifting the 'Fog' of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law," 54 Hastings L.J. 805 (2003).

The compelling case for a statutory suppression remedy is even stronger with respect to Section 217. The current version of Section 217 essentially assumes that law enforcement will always follow its conditions. Section 217 requires: (1) authorization by

the owner or operator; (2) a lawful investigation; (3) reasonable grounds to believe the intercepted communications will be relevant to an investigation; and (4) such interception does not acquire other communications. What happens if law enforcement violates one or more of those requirements? Nothing. To take a glaring example, suppose that law enforcement arm-twists a major ISP to let law enforcement camp at the ISP and look at all the e-mails. Under current Section 217, all of the e-mails of all of the users could become grist for future investigations. All of them could be used in subsequent trials, against ordinary e-mail users who had no connection at all to computer hacking.

The members of this Committee and I share the hope and belief that this sort of violation of wiretapping laws is not occurring today. But this Committee has the responsibility to craft the legal rules to prevent that abuse in the future. The current Section 217 has no safeguards against widespread "electronic" wiretapping. Section 217 permits owners of computer systems to invite law enforcement in to help with proper investigations. Those goals of Section 217 can be achieved while also assuring that Section 217 does not become an excuse for law enforcement to enter computer systems and look at so many other personal communications.

Section 220, Nationwide Service of Search Warrants for Electronic Evidence

The Committee has also asked me to comment on Section 220, which allows nationwide service of search warrants for electronic evidence. I will briefly explain my understanding of the rationale for the provision, which I support.

In 1986, when ECPA was passed, the local telephone company could generally fulfill a trap and trace order - the call came from a readily-identified phone number in a unified phone network. By 2001, the network had become far more complicated. To trace the source of an e-mail, law enforcement first had to serve a trap and trace order on the local Internet service provider. That provider then might tell police that the e-mail came from a backbone provider, who got it from another backbone provider, who got it from another service provider elsewhere, who might finally be able to identify the sender of the e-mail.

Before 2001, law enforcement had to get one court order from a judge at the first stage, and a separate court order from another judge at each stage later on. This was time-consuming, expensive, and largely redundant because the first federal judge had already approved the order. The Clinton Administration in 2000 and the Bush Administration in 2001 thus both proposed to allow one order to be effective nationwide, back to the source of the particular communication.

One criticism I have heard of this change is that prosecutors might shop around for a judge who will approve an order based on slender evidence. I have heard no evidence to support that this is happening. Oversight questions to the Department of Justice are appropriate to learn whether the Department has concentrated its requests for nationwide orders in front of certain judges. If such a pattern does exist, the Department

should be requested to explain the reasons for it and what measures it has taken to prevent forum-shopping abuse.

Conclusion

I thank the Committee for inviting me to testify today, and commend the detailed examination of the Patriot Act that is occurring this year. If I can be of any further assistance to the Committee as it proceeds, I would be honored to do so.

Mr. COBLE. Thank you, professor, and we've been joined by the Gentlelady from California, Ms. Waters.

We will probably, folks, have a second round today. This is a very important subject matter, so we'll probably do a second round.

Ms. Parsky, your written testimony provides a good description of the distinction between communications subject to a wire tap communication—subject to stored communications.

You state that the Wire Tap Act—and I assume that you refer to wiretaps generally—was designed to address a very particular type of situation: the ongoing interception of real-time conversations. You then distinguish ongoing interception of real-time with the one time access to stored communications, such as voicemail.

Now, if I understand Professor Swire's claims, he argued that the possibility—that with the possibility of future technology, store telephone calls over the computer—the distinction between wiretaps and stored communications will be lost.

Cannot a person already record their phone calls through high-tech message machines?

Ms. PARSKY. Mr. Chairman, you raise a very important issue, which I think actually there are two issues raised by Professor Swire that I'd like to clarify.

One is that to the extent that individual parties choose to store or to record conversations that they may have, whether it be over VOIP, which uses an Internet protocol, or over a normal telephone, over a wire system, once those communications are stored by the individual in either world they are subject to a search warrant. There's nothing that's special or different about VOIP in that context.

You could just as easily have a conversation with—between two parties and one of the parties has a—makes a consensual recording of that conversation and stores it on a cassette in their home.

The other important thing to point out is that VOIP does not change the obligations that are on service providers, whether they be a cable company or a telephone company; that to the extent that there's any interception and seizure of communications beyond that which is necessary to the provision of the services, they're violating the Wiretap Act, and there are consequences for that.

So I think that there is much ado about the new technologies that are coming up in our future. But, in fact, there's really nothing different except for the protocol. The same laws, the same restrictions would apply.

Mr. COBLE. Thank you. Professor Swire, is—you indicate that 209 applies to all stored telephone communications and not just the voicemail. Is not the real distinction that law enforcement receives the stored communication through a one-time access request rather than ongoing interception?

Mr. SWIRE. That's the distinction the Justice Department is supporting. That means that if your phone conversations are stored at the network level by your ISP in the future, they'll be accessible under that Stored Communications Act. Up until now, those phone conversations that went through the telephone network, you needed a wiretap order to hear what Jim Dempsey and I were saying.

Tomorrow, if it's stored at the network level, the Justice Department can get it, in some cases with a grand jury subpoena or other lower than search warrant requirements.

Mr. DEMPSEY. Mr. Chairman, could I speak to this question?

Mr. COBLE. Sure.

Mr. DEMPSEY. Cause this is a very good line of questioning.

One distinction is between the sort of real-time interception and the stored.

Another distinction looks to where is it stored. If you store a voicemail, an e-mail, a document in your office or in your home, no matter how old it is, no matter what you've done with it, if you've read it or not read it, it's protected fully by the fourth amendment and requires a warrant. If you store it outside of your home—if it's stored in the basement of the Capitol Building or stored on a server of the telephone company, which increasingly it is—it's not protected by the fourth amendment. It doesn't require a warrant, particularly after you've read that e-mail or listened to that telephone call, and to get one—it's not so much—there is a distinction between ongoing and one-time. But to get one piece of paper from your office, a warrant is required. To get one recorded phone call from your office, a warrant is required. You have to get it from——

Mr. COBLE. My time is about to expire. I don't want to overlook Mr. Martinez, since the other three—are you going to weigh in, Mr. Martinez?

Mr. MARTINEZ. Well, again, I think one of the things that we need to recall is that we are talking often of situations where consent is acquired, in fact, is initiated by a victim. And so this is a different situation than where we would initiate an investigation, you know, go through the effort to obtain a wiretap warrant.

So I think we do need to recognize that there are real victims in these types of situations and that consent is often the entry point that we have as the law enforcement agency.

Mr. COBLE. My time has expired. The Gentleman from Virginia.

Mr. SCOTT. Thank you, Mr. Chairman. Let's put a little bit—put this in perspective. Either search warrant versus a wiretap warrant, what is the exact difference between the two. I mean the wire tap you have to have—go to the judge, get a probable cause, listen in. It's limited. Search warrant can be done administratively without a judge looking over from time to time?

Mr. DEMPSEY. Well, Congressman, in both cases, it requires a finding of probable cause by a judge. In the case of a wiretap, at least for voice communications, it requires in the Federal case, it only applies to a certain number of serious crimes—a list of about a hundred of the most serious crimes. It requires senior Justice Department approval. There are periodic reports to the judge. There's a statutory suppression rule in addition to whatever fourth amendment suppression rule there is. And there are these fairly detailed and useful reports to Congress about the use of the technique.

Mr. SCOTT. Mr. Martinez, are there any things such as an administrative search warrant?

Mr. MARTINEZ. An administrative search warrant? There are administrative subpoenas, but again a search warrant connotes that a law enforcement officer has had to make findings of facts, pro-

vided that in an affidavit, and it is reviewed and becomes an order of the court to take action.

Mr. SCOTT. That's the search warrant. Now, if you're going to this ISP off site, do you need a search warrant—you don't need a search warrant?

Mr. DEMPSEY. If the communication is an unopened e-mail 180 days old or less, you need a search warrant. If it's an opened e-mail, you use a subpoena. If it's more than 180 days old, you use a subpoena.

Mr. SWIRE. Can I make a real quick point on that. I don't think we know what an unopened phone call looks like. That's never been defined. But if I've talked with you on the phone, the Justice Department may think that's already been opened, and they might get it under the lower standard. That's obviously something to clarify.

Mr. SCOTT. Well, let's—Mr. Dempsey, you kind of talked about letting the police into my house and letting them look around is different from letting them look into the crooks' pockets. Let me know if I got this wrong. I looked at it a little different. I looked at it not as me letting the police into the house. I live in an apartment building. How about the apartment superintendent letting them into my apartment. Isn't that more akin to what's going on when AOL let's you into my e-mails going back and forth?

Mr. DEMPSEY. I think that's a very interesting way of looking at it. It may be another appropriate way. It is true—and I think appropriate—that system administrators have the right to monitor their own systems. I think maybe the supervisor of the apartment, if he believes you're away, and an intruder breaks into your apartment, the supervisor of the building can call the police and say someone is in so and so's apartment.

Mr. SCOTT. In that case, you've got kind of an assumed permission that if there's a leak, the water is flowing out of my front door and I'm not there, the superintendent can go in. Over my objection without me knowing, can the building superintendent let the police into my apartment to wander around?

Mr. DEMPSEY. I think there are some circumstances probably in which they can.

Mr. SCOTT. But that's not the normal situation.

Mr. DEMPSEY. Now, it would be—let me say one of the ways in which people have talked about section 217, this trespasser provision, is as an emergency provision, particularly in the case of computer crime, in which time is of the essence; the hacker may be in and out; you need to get the information quickly.

But if that's the justification—if we're looking at a sort of an emergency exception—a funny smell is coming from your apartment or there's terrible noises coming from your apartment, screaming—in those kinds of situations, there might be grounds to enter without a warrant. But as in emergency wiretaps generally, there should be then go to the judge, take care of the emergency, then go to the judge, get the order, count it as an interception, bring it under the other rules, count it—report it to Congress, et cetera.

Mr. SCOTT. Yeah, but you got to have a check and balance. If you call it an emergency and go get something, and it wasn't an emer-

gency, you got the exclusionary rule looking at you. So you don't have an incentive to trip over the fourth amendment.

Mr. DEMPSEY. Correct.

Mr. SCOTT. Because if you found something, you can't use it, so there's no incentive—and that's kind of the policing mechanism you have if there's no incentive, you don't do it.

Mr. DEMPSEY. And here——

Mr. SCOTT. But there is an incentive to cheat and get in there. If you can use it, then there are no sanctions because you're not going to be able to sue the police—a guilty person is not going to sue the police, and get any——

Mr. DEMPSEY. Well, there are two or three provisions in the PATRIOT Act that I would sort of call "off the books" surveillance. What we do is we define it not as an interception or not as a disclosure, and then once we do that under the statutory structure, all of the other protections are eliminated, including the suppression rule. And what I think Professor Swire and I are saying is recognize the trespasser concept to some extent, but build around it some more checks and balances.

Mr. SCOTT. It's well known that e-mails kind of survive in cyberspace somewhere after you thought you had erased them. Are voicemails similarly preserved some kind of way? If you got a Verizon——

Mr. SWIRE. It depends on what Verizon or SBC does in their system. As you move towards——

Mr. SCOTT. You mean we don't know?

Mr. SWIRE. I don't know.

Mr. SCOTT. We don't know if our voicemails are preserved in cyberspace. Anybody know? We have another round, gentlemen.

Mr. MARTINEZ. I think that you'd find in the industry that there are different means of doing that in different technologies for storage and different reasons that they might have for storing, including billing purposes and that type of thing.

But if I may for a minute, I don't know if the analogy or the contrast between an emergency situation and one that is not emergency is really the appropriate one, because we don't want to take away from the victim, and again we talk about systems administrators. They're in the best position to determine whether or not their system is under attack. And there are instances where they may have evaluated that they have a situation where they can record all that—all the traffic and at a later date, because it's not considered particularly virulent to their system provide that to law enforcement and say I think I may have had an attack. It doesn't appear to have been a great one.

Or they may determine that they are under a current attack and there's information being exfiltrated in real-time. We're forcing a distinction upon them that really ought to be up to them to decide. You know do I have a more expedient situation. But what we don't want take away from them is our ability to address it quickly and try to mitigate—help mitigate it for them.

Mr. COBLE. The Gentleman's time has expired. And as I said, we'll do another round. The Gentleman from Arizona, Mr. Flake.

Mr. FLAKE. Thank you, Mr. Chairman—the witnesses.

Ms. Parsky, under section 209 how long can law enforcement go without notifying a subscriber or a customer that their stored communications have been accessed? How long is it? Is it indefinitely? And if not, how long is the longest time that it's happened?

Ms. PARSKY. Well, excuse me, under section 209 actually is not the provision and the PATRIOT Act is not the provision that makes that determination. It's actually determined by ECPA. And under ECPA, there is a requirement that for stored electronic communications or wire communications, section 209 then brings in the wire communications, either you need to access them with a search warrant if they are unopened or within the first 180 days, in which case there would be notice with the search warrant, or if they are older than 180 days, then you have to provide notice and a court order. So it's not a search warrant, but the provision of ECPA requires notice if a search warrant is not used.

Mr. FLAKE. So under no circumstance is anyone's stored electronic communication accessed without their knowledge.

Ms. PARSKY. Well——

Mr. DEMPSEY. Congressman, if I—could I respond?

Mr. FLAKE. Sure. Please.

Mr. DEMPSEY. I think in the case of a warrant, the notice is served on the service provider with the warrant. There's no notice to the customer ever——

Mr. FLAKE. That's what I——

Mr. DEMPSEY. —unless the evidence is used against them in court.

Mr. FLAKE. That's my question.

Ms. PARSKY. That's correct.

Mr. FLAKE. When will the customer know?

Ms. PARSKY. Well, as with any business records that might be stored by a third party, if you have a bank, for instance and there's a grand jury subpoena and law enforcement has, you know, lawful right to access those records that are being stored by a third party, the customer, the owner of those records, would not get notice either. So this isn't applying anything different.

Mr. FLAKE. But this is—it is different, though.

Mr. SWIRE. But this is the world of stored records we're moving to, and we're hearing that the customers never find out under these grand jury subpoenas and other things. This is what would apply to an increasing number of ordinary phone calls going forward.

Mr. FLAKE. This is different. I would maintain that if you have an account at a bank, obviously you're a customer of that bank. Maybe you don't know that the bank is being monitored or surveilled or information is being gathered, but in this circumstance, you are the target. But, yet, because law enforcement gets it from a third party, then you, the target, are not informed, and you're saying that that is the case; that can be the case for an indefinite period of time?

Ms. PARSKY. That's correct. If you are the target, whether it's a voicemail message that's being stored, or it's your bank records being stored, you would have notice if there are criminal charges brought, and that's part of the Government's case, through the discovery process.

Mr. FLAKE. But not until the criminal charges are brought?

Ms. PARSKY. Right.

Mr. FLAKE. Surveillance——

Ms. PARSKY. It's comparable in the physical world or in the electronic world.

Mr. FLAKE. Mr. Dempsey, you care to——

Mr. DEMPSEY. Well, which means that in the case of the individual whose records are wrongly acquired, who's never charged with a crime, the person who really would want to have some recourse, he may never be told.

Mr. FLAKE. Does that trouble you, Mr. Martinez? You seem to indicate concern for the victims quite a bit. Would somebody be considered who was wrongly believed to have information that would make them a suspect, but then never—they never find out that they were being surveilled?

Mr. MARTINEZ. Well, I think one analogy I could draw is in the world of physical surveillance. You know we follow bad guys, and they make contact with both other bad guys and other unwitting people that might not be part of their conspiracy. And so there is going to be times when we do have information or do see information that might not regard the actual crime that we—but what we're interested in is evidence. And we're going to boil it down to evidence, and I think that's the approach we would take.

Mr. FLAKE. Ms. Parsky, what delays were experienced prior to section 209 that made section 209 necessary?

Ms. PARSKY. Well, I think that there is the basic fact that the procedures for obtaining a wiretap, which are procedures that are put in place for the very special circumstance and the increased expectation of privacy and invasion of that privacy when you have an ongoing interception of live communications. And because of that, what the Wiretap Act puts in place additional procedures, additional protections to the Constitution that are resource intensive and time consuming.

With respect to a search warrant, there still are constitutional protections. There's still a standard of probable cause that needs to be met, and it's still presented to a neutral magistrate to make a neutral decision, but there aren't all the same hoops that need to be jumped through because it's a stored communication which, not under the PATRIOT Act, but, you know, over 20 years ago, was determined does not meet the same level of protection as an ongoing interception.

Mr. COBLE. The Gentleman's time has expired. The Gentleman from Massachusetts, Mr. Delahunt.

Mr. DELAHUNT. Yes, thank you, and this is again, Mr. Chairman, I want to compliment you and the Ranking Member for providing us with a very informative panel, much like the one we just had the other day.

Mr. COBLE. Thanks.

Mr. DELAHUNT. You know some of us understand the law well. And from past experience, we've been involved in these kind of investigations involving electronic eavesdropping, et cetera, and we're familiar with the act.

I think what you have to understand is that many on this panel, and I presume in Congress, are illiterate when it comes to the tech-

nologies. I, for example, don't know how to use e-mail. I don't have what do you call it a Palm Pilot or a Blackberry. I don't know how to turn on a computer. So I'm really at a disadvantage in the sense that I understand the law, but I really don't understand the technologies.

But I think the overarching concern—and I think it's been expressed rather well by both Mr. Dempsey and Professor Swire—the issue here is really one of privacy. And fundamentally, I think our purpose should be—and in this recent colloquy that you had I think with Mr. Flake involving notification—there's another piece of this, too, and that's the issue of transparency. I think much of the concern that the American people have is what's happening. You know, people like myself really don't know what's happening, because we're not familiar with the technologies. But we have this very profound unease that something is happening, and it may be untoward and it may be intrusive of our privacy.

So I think what we ought to be doing is examining how we deal with the concerns that the American people have in terms of their privacy. I think we address that through as much transparency as we can without imposing impediments that are really unreasonable on the Government. And I would suggest that's the kind of balance that we want to strike. I see the—this particular—the issues that we've been discussing here today as an opportunity to do just that. I mean why—what's magical about 180 days? And that is—is that really a false distinction? I don't know. I—you know.

Mr. SWIRE. Congressman, can I?

Mr. DELAHUNT. Sure.

Mr. SWIRE. In preparing for the testimony, I went back and looked at the Committee report from 2000 or H.R. 5018. That's when this Committee, the full Committee, in great detail looked at many of these issues. That Committee report is written in pretty plain English. It explains a lot of these issues and hits some of the——

Mr. DELAHUNT. I was on the Committee at the time, and I was very proud of the fact that the Committee came out with a—I think a fine piece of legislation unanimously and one I think that was very thoughtful and many of us were very much engaged in that. But I think the reauthorization process now provides us an opportunity to do some clean up and anticipate, like VOIP. I mean I don't even know what VOIP is. I mean I can't even imagine. What do you? What do you sit in front of a screen and talk to the screen? I don't know.

Mr. SWIRE. No. It's really great now. You'll use a regular handset. You'll think it's a phone call, but it's going through the Internet.

Mr. DELAHUNT. Well, that's good. I mean I don't have a clue.

Ms. PARSKY. If I may, I'd like to address the privacy issues that you raise and I think one important thing here is that we stay focused on the PATRIOT Act and the sunset provisions of the PATRIOT Act.

Mr. DELAHUNT. Now, see that's where I disagree with you. Okay. I think we have—we can amend the PATRIOT Act without just addressing those provisions that are sunset. I think we have an opportunity here to do something again without imposing an impedi-

ment on the Government, but if we just focus on these particular sections without implicating ECPA and all these other rather significant ancillary pieces of our statutory scheme that by necessity are implicated, we're really not going to, I think, come up with a product that I think reassures the American people that their privacy is being protected, for example. That's my point.

Mr. DEMPSEY. Congressman, if I could, just on the question of transparency. I think you're 100 percent correct. There are two ways that we provide transparency.

One, which Congressman Flake was referring to——

Mr. DELAHUNT. Notification.

Mr. DEMPSEY. —notice to the individual. Under the wiretap law, the surveillance is conducted in secret. Absolutely. The technique would be ineffective. It would be worthless unless there were that secrecy.

Mr. DELAHUNT. Right.

Mr. DEMPSEY. But after, as you know, the investigation is closed, then notice is provided to people whose communications were intercepted whether they are charged with a crime or not.

But for some of these other provisions, we do not have that kind of notice. And, for example, in the trespasser case, section 217 says that the trespasser interception is not an interception to be counted, to be notified, to be reported to a judge, et cetera. I think that could be addressed.

The second way we do transparency is by reports to Congress. And I think partly the sunset has helped to draw some of that information out, but now if these authorities are going to continue, and they probably should continue, there needs to be that kind of statutory reporting obligation that says how often are they being used, how many individuals' communications are being implicated, et cetera.

Mr. COBLE. The Gentleman's time has expired. You may continue that for the second round, Mr. Dempsey. I want to say to my friend from Massachusetts you have assuaged my discomfort. I am relieved to know that I am not the lone Member of Congress who does not possess a Palm Pilot. [Laughter.]

Mr. DELAHUNT. In fact, we are the brotherhood.

Mr. COBLE. The Gentlelady from California, Ms. Waters.

Ms. WATERS. Well, thank you very much.

Ms. Parsky and Mr. Martinez, since sections 209, 217, and 220 are not specified as tools solely to combat terrorism and terrorism-related activities, how many times have these sections been used in non-terrorist criminal investigations? If the USA PATRIOT Act was passed to aid in terrorism and terrorism-related investigations, then what are the purposes for sections 220, 217, and 209 if these sections do not limit investigations strictly to terrorism and terrorism-related investigations?

Ms. PARSKY. Let me begin and then Mr. Martinez I'm sure will have some followup. But the first thing that I think is important to make clear is that the PATRIOT Act contains provisions that are specifically addressed to terrorism, but it also contains provisions that are not specifically addressed to terrorism, and because there are those specifications in certain provisions, the other provisions by necessity are necessity are modernizations of all of the criminal

procedures; and that if there had been an intent that it only be applied to terrorism, it would have been stated as such. These provisions that we're talking about today are some of those very provisions that are intended just to modernize the tools that are available to law enforcement to protect our communities across the board, not just the terrorists.

Ms. WATERS. May I interrupt for one moment? I want to be clear that you're saying that the stored communications that have been referenced here so many times today—the telephone calls, et cetera—may be accessed without notification to the party that is the target of the investigation, and this information may be used in any shape, form, or fashion that the interceptor would like to use it for?

Ms. PARSKY. Absolutely. What this does is it applies the same normal rules that would apply to any criminal investigation.

Ms. WATERS. No. No. No. But this is without notification—well. This is information—these are facts. It's not as if you have an investigation to seek facts. Whatever is on the record is on the record. The telephone calls are there. The messages are there—what have you. They're accessed. I don't know about it. You don't need a warrant to get it. You can use it any way that you want to. Perhaps you have an investigation about terrorism. There is not terrorism, but you find that somebody may have committed another infraction or it could be considered a crime. Then you take this information and you pass it on to another law enforcement agency. Is that what you're saying?

Ms. PARSKY. Well, what I'm saying is that the same rules that have applied for years——

Ms. WATERS. Well, we haven't had these rules.

Ms. PARSKY. No, but the rules aside from the PATRIOT Act. The same rules that have applied to electronic mail, that have applied to physical records that are stored with a third party, these exact same rules. All the PATRIOT Act does is it says that you treat the same all types of stored communications, whether they are wire, whether they are electronic, whether they are physical or physical records. There's nothing new here.

Ms. WATERS. It is something new——

Ms. PARSKY. The same notice provisions apply.

Ms. WATERS. Well, let me just stop you again. As I understand it, under those circumstances, you have a limited period of time by which you can engage in the so-called search or investigation. I may be wrong. But this could go on forever and ever and ever; is that correct? Is that a difference?

Ms. PARSKY. There's nothing in the PATRIOT Act that changes the length of time that it may take for an investigation to be carried through. That's dictated by the facts of the case. But there are—I mean there are very significant cases. There are child pornography cases. There are places where we have rescued children from their molesters because of the very critical modernizations that were provided through the PATRIOT Act.

Ms. WATERS. Yeah. But, I'm not talking about that. What I'm talking about is this: you access my telephone messages. You use them in any way that you want to, not just for terrorism, but like you said, it's meant to apply to, you know, cases in the same man-

ner that prior to the PATRIOT Act. You can do anything you want with that information. You can share it. You can give it to anybody you want to give it to, and you can continue to access that information for as long as you want to without having to report to a court or anything. Is that what you're telling me?

Ms. PARSKY. No. That's not correct at all. What happens is the exact same standards apply whether it is a wire communication, an electronic communication or a physical record. You still need to go to a court to get a court order, a search warrant. You still need to provide notice with that search warrant to the same extent——

Ms. WATERS. And that's good for how long? Thirty days?

Ms. PARSKY. Which? The search warrant?

Ms. WATERS. Yes.

Ms. PARSKY. The search warrant has to be served within 10 days, and then you obtain the evidence that is stored.

Ms. WATERS. And how long can you look for the evidence?

Ms. PARSKY. The search gives you access for that one period of time to go and collect the stored records within the scope of the search warrant. So you are limited by the terms of the search warrant to a particular scope. You are limited to the investigation that you are carrying on, and there are other protections that are built into our system so, in fact, you cannot go and do whatever you want with it or disclose it to whomever you want. There are Privacy Act implications. And you're——

Ms. WATERS. What if you go to a provider, looking for information, and for whatever reasons, however they store that information, however they categorize that information, it's not easily found. You have to—they have to do a number of things to access the information, and how long can that go on? Do they have to give you the information in 10 days, 15 days, 30 days? Or can you work with them to get you that information over the next year?

Ms. PARSKY. Well, if it's a search warrant, you go in and you obtain the information. If it's a subpoena, then there is a return date on the subpoena, and by the return date, they need to return to the grand jury the records that have been requested.

Ms. WATERS. I'm talking about search warrant now I guess. I'm talking about search warrant.

Ms. PARSKY. In the search warrant, we go in and we obtain it ourselves. We don't give them a certain amount of time to provide it to us, because then we risk that they would destroy the records.

Mr. DEMPSEY. Yeah, actually, Congresswoman, if I may say just on that one point with the service provider: actually Congress changed the law recently to allow the service of warrants by fax. So they are faxed into the service provider without the presence of an officer there.

I think really what we're looking at here is sort of a confluence of three different things. One is the specific provisions of the PATRIOT Act that we're talking about today, relatively narrow changes. But I've been trying to say that they interface with other changes in technology that need to be addressed.

Third, they also interface with other provisions of the PATRIOT Act, for example, section 203, which was the subject of a hearing the other day, so that in terms of what can be done with this information, it's not only limited any longer to law enforcement uses. It

can be disclosed if it constitutes information about foreign affairs. It can be disclosed to national security, military, protective, immigration or intelligence agencies.

Mr. COBLE. Well, the Gentlelady's time has expired. We can continue this in the second round.

We'll start our second round now.

The courts have long recognized that providers of communications services possess a fundamental right to take reasonable measures to protect themselves and their properties against the illegal acts of trespassers. Now, I don't mean this to sound as subjective as it's going to sound, but who has the reasonable expectation of privacy under section 217? The owner of the computer or the criminal or terrorist hacking into the computer? Start with you, Ms. Parsky.

Ms. PARSKY. Thank you. You raise a very important point, and I think particularly when we're talking about privacy rights here, and when we're focusing on the provisions of the PATRIOT Act that are subject to pre-authorization. Section 217 is a critical provision to protect privacy. It's a critical provision to protect the privacy not only of the service provider whose property is being unlawfully accessed. That's what the hacker trespasser is doing. But, you know, we are living in a time when there are all sorts of computer hacking incidents that are subjecting consumers and individuals to the potential for identity theft. So that to the extent that you have this hacker then accessing the individual account holder's information and providing very private information to others to conduct criminal activity, this is allowing law enforcement to protect those privacy rights of the consumers.

Mr. COBLE. Which was vague prior to the act?

Ms. PARSKY. That's correct.

Mr. COBLE. Let me hear from the rest of the panelists.

Ms. MARTINEZ. Congressman, if I can follow up on that. Again, in working—the FBI works very hard to garner good relationships with e-commerce businesses so that we can get the information we need to go at cyber crime, and there are some incentives and disincentives for them to do it.

One of the things that I think we're starting to agree upon is that e-commerce businesses have a responsibility to protect the—both their intellectual property, but also the vast amount of personal information that they might store in the course of their normal business.

Again, this expands their ability to be a responsible corporate citizen, to get information to us that might allow us to act quickly to stop an attack that might very well expose hundreds of thousands, millions of personal records. So again, anything we do that would reduce our ability, especially the timeliness of our ability, to address those types of situations when a consenting party comes to us and makes us aware of a problem, I think would be—would go against being able to protect privacy of citizens in general

Mr. COBLE. Thank you, sir. Mr. Dempsey?

Mr. DEMPSEY. Mr. Chairman, I agree with Mr. Martinez. But the question is what if they're wrong? What if the system operator is wrong and points the finger at the wrong person? What if law enforcement comes in and acts over broadly? I'm saying respond to

the emergency, recognize the seriousness of the computer crime, but build some checks and balances in that gives some redress when a mistake is made.

Mr. COBLE. Professor?

Mr. SWIRE. Thank you. It's the expectations of privacy of all those phone users, e-mail users, credit card people. That's where the ordinary citizen's privacy is at stake. And right now, if the Government looks through those, either by mistake or because they want to look through those, they can take that information. They can use it in future investigations. They can use it in court. And the statutory suppression rule that this Committee has previously passed addresses that so that you have a rule that says they should follow the law and not be over broad in their searches.

Mr. COBLE. Ms. Parsky, your facial response tells me you want to weigh in again, and you may.

Ms. PARSKY. Thank you. Well, one thing to make clear is that this isn't just about an emergency. This is the equivalent of a normal consent situation. And there are numerous, you know, vast arrays of examples where in a physical world, there is a citizen or a company that provides law enforcement with a tip, and we need our citizens to bring crimes to our attention. They don't always pan out. There is always the potential that there will be access to information about individuals who don't end up having criminal culpability.

Mr. COBLE. I thank you for that.

Ms. PARSKY. Thank you.

Mr. COBLE. Let me beat the red light by putting another question to Mr. Dempsey.

Mr. Dempsey, in your written testimony, you stated that section 220 of the USA PATRIOT Act makes obvious sense. Elaborate in some detail on that if you will.

Mr. DEMPSEY. Well, I think we do have nationwide communication systems and for a crime in California the evidence may be—the electronic evidence may be stored in Virginia.

It is appropriate I think for a judge in California to issue that warrant to be served in Virginia, to send the evidence back to California where the locus of the investigation is. My only concern is that a little bit tips the balance in the other direction, and if the service provider gets a warrant that looks over broad, that looks burdensome, that may sweep too broadly or it may be unclear, the person in California issuing the warrant may not have understood the computer network of the person in Virginia.

The person in Virginia, they want to do the right thing. But they also want to be careful. They should have the opportunity to go to a judge in Virginia or in California, but certainly in Virginia where they are and say we want to cooperate. We will give it over, but we—it should be focused a little bit more.

Mr. COBLE. I got you. I thank you. My time has expired. The Gentleman from Virginia.

Mr. SCOTT. Thank you, Mr. Chairman. We keep talking about how you're going to use the information as the kind of violation of privacy that you actually use it. Some of us may think that just looking at, because we're not talking about robots. We're talking about somebody who could be your neighbors and people are kind

of thinking terrorism. Let's kind of think mental health records and medical records that people—that your neighbors may be looking at if they happen to work for the FBI. And when you think of it in that nature, I mean sometimes you don't want people looking at your medical records and your mental health records, and your private communications with your friends, colleagues, or spouse. You may not want the—your neighbors to know that you're having marital problems and all that kind of stuff. So just the idea that you get to look at it, I mean. And then after you get to sharing it all—and we're not even getting into that—but some people are going to be looking at your very private communications. And you don't know going in what's going to pop out of that e-mail.

Ms. MARTINEZ. If I may address that very example, I think health records is a good one. There have been intrusions into medical facilities and health records have been compromised. In working a computer intrusion investigation, it would be very important for us to determine what type of data was targeted. And it may very well be that we determine that very specific health records of very specific individuals were targeted. But without us being able to do the investigation and drill to that level of detail we wouldn't know and that would impede our ability to work that case back to identify——

Mr. SCOTT. You don't know—you don't know when you start reading your—I mean it—doesn't the e-mail from me to my doctor or from a person to his priest doesn't start off by saying personal information enclosed. Caution. Warrant required. You just start reading and start tripping over all this information that could affect—it could be your neighbor. You know you didn't know that about your neighbor.

Mr. SWIRE. Congressman, can I—one of the things that the Government's position has been if the record is stored, then you're pretty much out of luck. You're under much less luck than you used to be. Once it's stored, there's no constitutional protections—reasonable expectation to privacy—you've handed that over to a third party. Once it's stored, you're under the Stored Communications Act at best. You're not getting wiretap protections anymore.

So they're saying once these things get stored——

Mr. SCOTT. And you can do it by subpoena. You don't even need a search warrant? Is that right?

Mr. SWIRE. It depends on the time, and they have different things, but a lot of times you can do it through a grand jury subpoena, through this 2703(d) order, or you can do it through a search warrant. The Government gets to choose.

Mr. SCOTT. Now, we keep talking about these delayed notices. If you trip over this embarrassing information about your neighbor and don't use it and don't notify anybody, there are, in fact, no sanctions if you're not going to use the information; is that right?

Ms. PARSKY. Well, if I may, I think one important thing to keep in mind here, particularly when we're talking about section 217 is that we're talking about, number one, the fact that when you have these communications that are going on on a service provider's network, there is already the ability for the service provider to monitor those communications. So regardless of whether law enforcement is involved, you have the service provider monitoring. But in

section 217, we're talking about the additional situation where these private records, whether they be, you know, medical records or personal notes to a neighbor, those are being also accessed by a trespasser.

So the additional insertion of law enforcement into that calculus actually adds more protections because law enforcement——

Mr. SCOTT. But you're kind of getting over broad——

Ms. PARSKY. —is subject to other restrictions that criminals are not.

Mr. SCOTT. Do you need a trespasser to trigger all of these search warrants and subpoenas?

Ms. PARSKY. Section 217 is specific to hacker trespassers and that is where the system—the system provider—the service provider can—they have the ability to monitor the communications. They can provide the consent to law enforcement to assist them in protecting their own property.

Mr. SCOTT. So if AOL is listening into—is reading all of my e-mails, then they can invite law enforcement to look over their shoulder as they look at my e-mails?

Ms. PARSKY. Rather than their collecting it and providing it to law enforcement afterwards, when law enforcement doesn't have the ability to help protect them and to help solve the crime.

Mr. SCOTT. If AOL has a privacy agreement with me, then they can't do that.

Ms. PARSKY. That's correct. That's a contractual matter.

Mr. SWIRE. AOL can read your e-mail only for the purpose of protecting their service or their rights or for purposes of protecting the security of their system. But I think we've sort of shifted over a little bit—mushed up 209 and 217. Two seventeen is limited to trespasser cases. 209, the warrant or subpoena access, is for all investigations. And I think though one of the issues you were getting at with the question of the medical records, et cetera, the real-time interception cases have almost a two-layered protection. You get the warrant, which has the particularity required by the fourth amendment giving the Government the right to get into somebody's communications stream.

The law imposes what is almost an extra protection, which is the minimization requirement, which says that you can only record specifically what is incriminating. There is no real minimization requirement on the stored records side. The minimization requirement is in title III, not on the Stored Records Act.

So one you're in there and particularly because you don't know what you're getting until you actually open it. You don't know whether it's relevant or not until you actually look at it. The Government I think does acquire a lot of information in a stored capacity, bring it back, sit there, open it, go through it, and at that point there, they are looking at and they have in their possession a lot of material that turns out to be extraneous.

Mr. SCOTT. Mr. Chairman, let me just say that one of the problems after you get in there and start reading and reading if you do not use the—if you don't want to use the material, there is not requirement—there's no sanction for continuing to read.

Mr. DEMPSEY. Not really.

Mr. SCOTT. With a requirement of a warrant going in, you don't know what you're going to get so if you mess up, if you break into somebody's house and get—find the drugs, you can't use the drugs under the exclusionary rules. So you have no incentive to break in.

Under this, with this delayed notice and all that, if you find some goodies, you can find the notice. But if you don't find anything, there is no sanctions.

Mr. DEMPSEY. Right.

Mr. COBLE. Well, the Gentleman's time has expired. Ms. Parsky, you and Mr. Martinez want to weigh in before I recognize the Gentleman from Massachusetts?

Ms. PARSKY. I think we both want to make a couple of brief comments. I thank you very much.

Mr. COBLE. And briefly if you can because we've got to move along.

Ms. PARSKY. Very briefly. But the one thing that I think is important to understand is that if you have a search warrant, there is very specific requirement that it be relevant to criminal activity and that there be a defined scope for that search warrant. So you don't go in and you're able to inspect or search or seize anything you want. You go in within the scope of the search warrant and there is the ability for someone to challenge whether, in fact, you stayed within the scope.

Mr. SCOTT. Yes, but that doesn't apply to a subpoena?

Ms. PARSKY. But that applies to a search warrant whether it's for physical records or electronic records and to the same extent that you might have a search warrant to search physical files and you may have to open up the file to see if what's in there is within the scope of your search warrant, the same applies to the electronic world. I think Mr. Martinez.

Mr. MARTINEZ. And I think to follow up on that. Again, I'll make the analogy with the physical seizure of health records. You may, in the course of an investigation, try to determine if there are victims that are part of the health organization's records, and you may see some information about someone's very, very personal health profile. Again, if it doesn't go the specific violation that I'm trying to prove or determine elements of, I don't know that I would have a positive requirement to then go back and tell everyone whose record I looked at that I set aside because it wasn't pertinent to my investigation that I looked at your health record.

We'd go on to the next one and aggregate evidence and move on from there.

Mr. SWIRE. May I have one sentence just to follow? Under new technology, we're storing lots and lots more things than we used to. That may mean the laws about stored records deserves some reexamination.

Mr. COBLE. The Gentleman's time has expired. The Gentleman from Massachusetts, Mr. Delahunt.

Mr. DELAHUNT. Yeah. I think that goes to—you know, and I appreciate the distinctions obviously between electronic records and physical records.

But people understand a physical record. As I indicated earlier, there's a lot of us that really can't put our—we don't grasp the ex-

tent of and the volume of electronic records. That's where the unease of the American people are in terms of their privacy.

And I think that was the debate and the discussion, that's what we have to remember, and we have to—if we're going to—and I think we should. Okay. If we're going to give law enforcement the updated means to conduct investigations, at some time we have to do this in a way that's thoughtful enough to balance the concerns that Americans have about privacy. And the best we can do is, you know, in my judgment, is transparency and notification. If we do that, even though it's burdensome, it doesn't impede the investigation.

You know, Mr. Martinez, I mean everything that's done post the investigation by virtue of that definition doesn't impede the Government from, you know, fulfilling its role in terms of protecting the American people or, you know, enhancing public safety. I mean that's what I'm suggesting here.

Mr. MARTINEZ. Well, I want to make one point about the emerging new technologies. I think as we look at technologies emerge, we have to be very careful to determine whether that technology is really unique. Does it really present a set of circumstances that did not exist before or that hasn't been analyzed and very, very carefully thought through before, because—just because it is a new technology, it doesn't necessarily mean that there isn't already an existing paradigm in the law to handle it.

So I wouldn't want to make the assumption—you know, when we transition from an analog telephone to cellular telephone—you know, we still had conversations going over it.

Now, there were a lot of implications to that. The technology was indeed different, but I think much of the circumstance was similar to what existed before.

Mr. DELAHUNT. But it's the speed.

Ms. PARSKY. Well, I think as an important——

Mr. DELAHUNT. The problem you have in terms of the transmission, the communication itself is so quick and so instantaneous, you need to be upgraded. Okay. And I think what we have to do is look at concomitant ways to again ensure that those privacy rights and—if there's anything about the American people and in terms of the essence of our democracy it's the right to privacy. If you don't have privacy, that's the beginning in my judgment of totalitarianism. Okay.

And that's why Americans emphasize so much this checks and balances issue and this transparency. And that I think is the framework, the mind set that should come to this. Before my time runs out, what I'm going to do is adopt the questions that were presented by Prof. Swire as mine. And I'm asking you, and I'm going to put this on you, Ms. Parsky, to respond to those questions in writing. In the past, under other Attorneys General, I've made those requests. Somehow it gets lost in the black hole. But this is a new Attorney General, a new Administration. I would hope that those questions, which are now Delahunt's questions, okay, would be responded to and, you know, please would you direct the answers to those questions to me? I'll give Mr. Coble and Mr. Scott—you can *Cc:* them. Right? But I think they're good questions, be-

cause I think they go to the clarify—I think really what some of this is about is clarification.

Ms. PARSKY. If I may just briefly respond quickly or follow up on what Mr. Martinez said. I think that it's important to recognize that there are still laws that we can apply to these new and complicated technologies. And as Professor Swire says, yes, with, you know, Internet protocol and with packets of information, it may be easier to store information. That doesn't mean that it's authorized to store information. So even if a network administrator may be able to store it, the same rules still apply in terms of what kind of contractual relationship, what kind of consent those working under that network administrator have entered into and that have——

Mr. DELAHUNT. And I understand that, and I'm sympathetic, and I understand that.

You know, I think what we hear from Mr. Scott in terms of his concerns about mental health records. I think we need to explain, you know, the concept of minimization and what it means whether we're intercepting a telephone conversation and how the concept of minimization in terms of review of records applies to electronic records.

Mr. DEMPSEY. Congressman, I think that one of the things you mentioned was speed and volume. And it goes to Representative Scott's questions. Well, I remember a couple of years ago, FBI Director Freeh was testifying in support of his budget request and talking about how the FBI needed more money to process the data that they were collecting, and he cited one case——

Mr. DELAHUNT. Well, didn't he get a new computer for that?

Mr. DEMPSEY. Well, different issue. Different issue, Congressman.

One case the FBI seized enough electronic information that if it were printed out, it would have filled the Library of Congress one and one half times over. That was FBI Director Freeh's testimony. That was the volume of stored records that were available to them in that one investigation.

Mr. COBLE. The Gentleman's time has expired. The Gentlelady from California, Ms. Waters.

Ms. WATERS. Thank you very much, Mr. Chairman. First, I'd like to ask unanimous consent to enter my statement into the record.

Mr. COBLE. Without objection.

Ms. WATERS. And secondly, I think the discussion was going in a direction that I have great interest. I think that we all have a very special need to believe that we have control over our lives, and it is very disconcerting to think about people having access to every tidbit of information about your life because they are able to store your telephone conversations, your e-mail messages, and on and on and on. It's just pretty overwhelming.

And so I think we certainly need to understand the new technology and who has the ability to store what and for how long. And whether or not, you know, there is certain kind of permission needed in some cases to be able to give that information or share that information.

And I do think that perhaps we need to look at this new body of law relative to this new technology so if nothing more comes out

of it then disclosure to the client. We get credit reports. I mean we force credit card companies to give us a report every year to tell us what they're holding and what they're advising people about us.

For our medical records, our doctors have to have written permission from us to give it to somebody, I just think we need to find out what—well, we need to develop this body of law that will help us feel we have some control. I recognize the need for, you know, the criminal justice system to be able to access certain things through warrants and subpoenas, but I do think I have a right to know whether or not my computer or company or my server is holding information and what form it's in, and how long it's held. Some of those things I think are just very basic to being able to have some kind of contractual relationship with those who are holding significant information about you.

I think I would feel better if I just had disclosure, because I understand that the technology works in different ways and we don't know what technology is being used by what companies. Then I may have a right to choose a particular company because they don't keep certain information or they discard information after a certain period of time. So I think we should——

Mr. COBLE. Would the Gentlelady suspend for a moment?

Ms. WATERS. Yes.

Mr. COBLE. Reverting to Mr. Delahunt's suggestion, the record will remain open for 7 days folks so we can have exchange and this will be ongoing. This is not the day of finality on this matter by any means.

Ms. WATERS. So I—let me ask, Mr. Delahunt, when you referred to Mr. Swire's questions, I don't know what those were, but are they included in——

Mr. DELAHUNT. They are an appendix to his testimony.

Ms. WATERS. Do they relate to the concerns that I——

Mr. DELAHUNT. Some of them do.

Ms. WATERS. Just, and if I may, I have a few more seconds left here, Mr. Swire. Could you comment on what I tried to communicate just a few moments ago about possible disclosure or having some choices in the selection of companies that I deal with, et cetera, et cetera.

Mr. SWIRE. I have two comments. One is when it comes to stored records, this Committee in the fall of 2000, in H.R. 5018, passed I think unanimously or almost unanimously a number of provisions about stored records, and there's a Committee report about that. So that might be a place to look where Republicans and Democrats worked together that year.

On disclosure, that comes up to issues of should every company have privacy policies they communicate out there. We do have most companies with privacy policies. There's no Federal laws that say they have to do that, and a lot of companies have over time watered those down in the last three or 4 years because they don't want to be constrained if they feel like using data later. And I think if you look at those privacy policies in general they're less detailed and less full today than they were 3 or 4 years ago, and that might be something for people to look at also.

Ms. WATERS. Well, that's a good idea. Let me just say based on some of the recently developed laws, we are supposed to be given an opportunity to opt-in or opt-out——

Mr. SWIRE. Yes.

Ms. WATERS. —on information that's shared about us. But I don't think it gets to the stored information at all. I'll go back and take a look at that.

Mr. SWIRE. For your medical data and financial data, the stored records at the bank or the hospital, those are subject to some of those choices the Congress put into law.

Mr. DEMPSEY. Although in every case, those provisions have law enforcement and intelligence exceptions.

Ms. WATERS. Oh.

Mr. SCOTT. What do you mean by an exception?

Mr. DEMPSEY. That basically it doesn't matter what the privacy policy says. When the Government comes in with whatever compulsory process is permitted, whether it's a warrant, a subpoena or a court order, the privacy policy evaporates.

Ms. WATERS. But if I got disclosure, if I understand what it is you are storing, and, you know, how you do this, how much information you hold on to for what periods of time, I may have some options about whether or not I want to deal with you or I may want to handle my business in a different way. For example, let me just tell you here in the Congress of the United States, you know, people keep in their computers, you know, all of the daily calls. They keep telephone numbers. They keep everything. Well, you know, some people may want to decide I don't want that in the computer for whatever reasons. I want to use some old systems. And I knew and understood, which I'm going to ask now, what is being stored for how long in the systems that we use, then I may, you know, make some different decisions.

Mr. COBLE. The Gentlelady's time has expired. We have the Lady from Texas has just joined us. We will include, professor, your questions in our post-hearing letter. And that can be addressed then.

The Gentlelady from Texas is recognized for 5 minutes.

Ms. JACKSON LEE OF TEXAS. Thank you very much, Mr. Chairman. To the panelists, thank you. We are at the same time in a Homeland Security mark up and so I thank you for your testimony and apologize for my tardiness in this hearing.

But let me just take the opportunity. This hearing deals with certain sections of the PATRIOT Act for reauthorization that are not necessarily that controversial. But I am going to take this opportunity to press some points that may be somewhat more global.

And that is that the idea of the PATRIOT Act, of course, was to ensure safety or to correct some of the ailments that many thought could cure the tragedy that we faced on 9/11. Some of the weaknesses as we moved into cyber security and technology. We just passed a bill in Homeland Security to establish an Assistant Secretary in the Homeland Security Department for Cyber Security. Again, the whole issue of integration if you will to provide more security for the Nation.

I raise the question, however, as an opponent of the PATRIOT Act and a huge skeptic of the reauthorization of any of the sections,

meaning that I want close scrutiny is where we are in 2005. Some will say that the aviation industry is not that much safer. Questions are being raised about our security personnel as we—our screeners. It's certainly out of the jurisdiction of this Committee, but I think the main question is whether we have been made safer by downsizing on some of our civil liberties and the ability, of course, for unreasonable search and seizure.

I think my colleague from California made the point that now vastness is a vast wasteland dealing with e-mail and I believe that we have lost the touch of writing the written letter, if you will. And so cyber security has become our means of communication. I am concerned with even the minimal, if you will elimination or impacting on the use of e-mails and the privacy of individuals and the intrusion by law enforcement entities on the basis of homeland security or national security.

So I'm going to start with Mr. Swire in terms of putting you on the immediate hot seat for this global question that I've asked and that is are we safer and is the—are we necessarily having to do this—having to reenact these provisions on the PATRIOT Act to ensure that safety?

Mr. SWIRE. That feels pretty hot. Are we overall safer? There was certainly some provisions of the PATRIOT Act that I supported when I was in the Clinton Administration and that were sensible updating to take account of new technology.

I think that when I think of safer and downsizing civil liberties, the one point I stress is that the current law seems to be once the record is stored, once it's held at the ISP or the bank or something like that, you've lost all your constitutional protections of reasonable expectation to privacy. I think that hasn't been fully understood by a lot of people; that those stored records that we've heard so much about today, once they're out there, the constitutional protections are gone. That means Congress is the only place that writes those privacy rules.

And so this Committee and the rest of the Congress has to think about if the courts aren't going to do it, what's the Congress going to do to right the law so that we have safety and civil liberties going forward.

Mr. DEMPSEY. Congresswoman, we are safer, but not safe. Progress has been made, but still a lot more needs to be done.

On the question of cyber security, I think that clearly the PATRIOT Act focuses almost exclusively on after the fact prosecutorial efforts. Clearly, a lot more needs to be done on building secure systems.

But I think finally the question of civil liberties is I believe, and I think there should be pretty wide agreement. If you look at the 9/11 Commission Report, if you look at the Gilmore Commission Reports, the Markle Task Force, what we should be seeking here is not a trade-off, not a surrender of some civil liberties in order to purchase some security, not a trade-off, but a balance. But a little bit here I hear the Justice Department saying give us more power to deal with new technology, but don't adjust the privacy protections to deal more—with the new technology. The technology is changing. We need to change the laws in ways that make it easier for the Government, and there's some validity to that. But don't

change the law in ways that would improve the checks and balances. And I think we need those checks and balances. I think they do not hurt us.

Our rights are not what is wrong with our counter terrorism approach. We need these checks and balances. They can be effective with all the authorities we've talked about today.

Ms. JACKSON LEE OF TEXAS. And this is a very strong point that you made, Mr. Chairman. I think—I hope the halls of this—or the walls of this Committee room have heard Mr. Dempsey and Mr. Swire and not to ignore Mr. Martinez and Ms. Parsky. I'm sure that I'll be able to read your testimony, but my point is the importance of privacy and balancing our national security.

I yield back.

Mr. COBLE. I thank the lady. Mr. Martinez, Mr. Dempsey referred to DOJ, either one of you want to respond to that?

Ms. PARSKY. Well, I appreciate the opportunity, and I would like to just respond briefly that the Justice Department's position is that we should be able to bring our law enforcement tools up to speed with modern technology, while preserving all the checks and balances and the constitutional protections and other protections that are built into our criminal procedures. And all we are looking to do is apply those exact same checks and balances protections of privacy to the modern world.

Mr. COBLE. Well, this——

Mr. SCOTT. Mr. Chairman? Can I ask——

Mr. COBLE. Yes.

Mr. SCOTT. —one. There's one point I——

Mr. COBLE. I will. But I say to my friend from Virginia——

Mr. SCOTT. It will be quick.

Mr. COBLE. Well, if you can, 'cause I got 50 constituents who are waiting on me for about 10 minutes now. So, Mr. Scott.

Mr. SCOTT. Well, if AOL doesn't care about my privacy, what—and they give anybody—they give Government permission, where does it say—am I without safeguards, is that what I understand?

Mr. SWIRE. That's section 217. If AOL invites the Government in, and the Government is supposed to only look at the hackers, but they look at everyone else, right now they get to use all that evidence in court and in future investigations.

Mr. SCOTT. Or look at it, because the question, the point was made that if you're in the doctor's office, you can look at the file. You don't know what's going to be in it when you open it up, but you know what file you're looking at. You're not—you didn't have—you're not in the doctor's office looking at all the files.

Thank you, Mr. Chairman.

Mr. COBLE. I thank the Gentleman, and I thank the panelists. This has been a very worthwhile hearing it seems to me. As I said before, the record will remain open for 7 days, and I again thank the witnesses for your testimony. The Subcommittee very much appreciates this.

In order to ensure full record and adequate consideration of this important issue, the record will be left open for additional submissions for 7 days. Also any written questions that a Member wants to submit should be submitted within that same 7-day timeframe.

This concludes the oversight hearing on the "Implementation of the USA PATRIOT Act: Crime, Terrorism and the Age of Technology."

Thank you for your cooperation and your attendance, and as well as those in the audience and the Subcommittee stands adjourned.

[Whereupon, at 11:49 a.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 scheduling this hearing on USA PATRIOT Act provisions to investigate and prosecute crimes through the use of electronic evidence. Section 209 of he Act references "Seizure of Voice Mail Messages Pursuant to Warrant." However, that section authorizes access to much more than voice mail and authorizes access through ways other warrants, such as by administrative, grand jury and court issued subpoenas, under the appropriate circumstances. And they can be "sneak and peek," whether warrants, court subpoenas or administrative subpoenas. So we are talking about a section that is not only misleading relative to the breadth of the police powers it authorizes, but a title that is also deceptive as to the extraordinary nature of the powers.

Quite frankly, Mr. Chairman, the more I review the extent of the powers we have extended to law enforcement through provisions such section 209, the more I am pleased with our decision to provide for a sunset on some of these powers in order that we may review in earnest what we have done, and so that the law enforcement authorities who get access to our private information pursuant to these powers, is aware we will be reviewing them. This is a section whose original purpose was to protect our electronic data against intrusion. When I see the "mack truck" hole we carved out of that purpose for law enforcement access, and the limitations on traditional methods of holding law enforcement accountability such as prior notice with right to quash, and oversight of a court through return reports to the court within a certain number of days, the more I am convinced that sunset review in this area is absolutely essential to our oversight responsibilities to the public. And this is especially true in the areas of electronics and general technology, given the growing impact of technology on our society. I have the same concerns about Section 217, which allows an ISP to give law enforcement wide latitude to look at private electronic communications without court oversight or review. Its one thing to call law enforcement to look at a trespass that is occurring; its another thing to call in law enforcement to look o see if there is anything suspicious going on, prior to a trespass occurring. And while I can understand the efficiency and exigency arguments for a nationwide search warrant authority in the arena of electronic communications, I am also concerned with the sufficiency of the notice and, right to challenge and oversight of such warrants.

For law enforcement, the good news in what I am saying is that I think these powers should be available in appropriate circumstances, so I am not calling for sunsetting them. However, for the public's protection of their privacy as well as their safety, I am saying that we need to look more precisely our notice, oversight and reporting requirements for these powers, and make appropriate adjustments. We should also continue this kind of oversight through sunsets, where we have to periodically look at the use of these powers in an arena of evolving technologies, and where law enforcement is aware that the use of these powers will need to be scrutinized and justified. So, Mr. Chairman, I look forward to the testimony of our witnesses on how we might best do that, and to working with you on implementing their recommendations. Thank you.

PREPARED STATEMENT OF THE HONORABLE MAXINE WATERS, A REPRESENTATIVE IN CONGRESS FROM THE STATE OF CALIFORNIA

Mr. Chairman, sections 209, 217, and 220 of the Patriot Act, violate Americans' privacy rights and civil liberties and should not be renewed. None of these sections are limited in their application—they can be used for any kind of criminal investigation that the DOJ sees fit, and are not limited to terrorism.

Mr. Chairman, section 209, the "Seizure of Voicemail Messages Pursuant to Warrants" of the Patriot Act allows law enforcement agencies, in some circumstances, depending on the amount of time the messages have been stored, to seize American citizens' stored voicemail messages without a search warrant or subpoena. Section 209 also is not subject to the exclusionary rule. Therefore, if law enforcement illegally seizes an American citizen's voicemail messages, the illegally seized voicemails still can be used as evidence against a person in court. Since section 209 has no notice requirement, the citizen would not even know she was the subject of surveillance, until she is brought to court.

Mr. Chairman, even if law enforcement gains access to an American citizen's voicemail in adherence to section 209, there are no limitations as to how the information will be used or publicized. This power far overreaches into the constitutionally guaranteed right to privacy.

Mr. Chairman, section 217, or the "Interception of Computer Trespasser Communications" section, is just as harmful as section 209. Under section 217, if a computer service provider claims that an individual is "trespassing" on its network, law enforcement is free to intercept that individual's private communications without permission from a judge. This section fails to address the question of, who qualifies as a "trespasser."

Mr. Chairman, the DOJ would like Americans to believe this section is limited to computer hackers. However, section 217 never specifically describes a "computer trespasser" as a computer hacker. The definition given is "a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy, in any communication transmitted to...the protected computer." This definition leaves open several definitions as to what constitutes a "computer trespasser."

Mr. Chairman, this vague definition is dangerous because there is no judicial oversight or notice requirement in section 217. Therefore, this section, like many other Patriot Act provisions, allows law enforcement to freely and secretly spy on Americans, with no checks or supervision from a judge to make sure this power is not abused. Section 217 places all power within the hands of law enforcement and the system owner or operator.

Mr. Chairman, section 220, or the "Nationwide Service of Search Warrants for Electronic Evidence" section, amends the Federal Rules of Criminal Procedure to expand the jurisdictional authority of a court to authorize search warrants outside of the court's judicial district in a criminal investigation. This section allows law enforcement to pick and choose which court it can ask for a search warrant. This leaves open the possibility that law enforcement agents can "shop" for judges that have demonstrated a strong bias toward law enforcement with regard to search warrants, using only those judges least likely to say no—even if the warrant does not satisfy the strict requirements of the Fourth Amendment of the Constitution. This section also has no notice requirement.

Mr. Chairman, only local judges and courts should be allowed to grant warrants for investigations falling within their jurisdictions. Judicial oversight is only effective if the presiding judge is within the jurisdiction where the search and/or investigations are taking place. Local judicial oversight is a key check against unreasonable searches and seizures. Also, Americans have the right to due process and should be notified if they, or their property, are the subject of a search warrant or criminal investigation, even if the notice is issued after the search or investigation has commenced.

Mr. Chairman, absent a clear demonstration from law enforcement that these new surveillance powers are necessary, sections 209, 217, and 220 should be allowed to expire. These sections of the Patriot Act threaten the basic constitutional rights of millions of Americans.

I yield back the balance of my time.

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

				Page
I.	National Security Surveillance Before 1978			3
	A.	The Fourth Amendment and Law Enforcement Wiretaps		7
	B.	The Law and Logic of National Security Wiretaps		10
	C.	National Security Wiretaps and "The Lawless State"		15
		1.	Routine Violations of Law	
		2.	Expansion of Surveillance, for Prevention and Other Purposes	18
		3.	Secrecy	19
		4.	Use Against Political Opponents	19
		5.	Targeting and Disruption of Unpopular Groups, Including the Civil Rights Movement	20
		6.	Chilling of First Amendment Rights	20
		7.	Harm to Individuals	21
		8.	Distortion of Data to Influence Government Policy and Public Perceptions	21
		9.	Cost and Ineffectiveness	22
II.	The 1978 Compromise – The Foreign Intelligence Surveillance Act			22
III.	FISA from 1978 to 2001			30
IV.	The Patriot Act, The New Guidelines, and New Court Decisions			37
	A.	The USA-PATRIOT Act		37
		1.	From "Primary Purpose" to "A Significant Purpose"	38
		2.	FISA Orders for Any "Tangible Object"	39

* This document is copyright Peter Swire, under a Creative Commons by-nc license, *see* http://creativecommons.org/license/meet-the-licenses. 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.

		3. Expansion of "National Security Letters"	41
		4. Other Changes in the Patriot Act	42
	B.	New Guidelines in the Department of Justice	43
	C.	Decisions by the FISA Courts	46
V.	The System of Foreign Intelligence Surveillance Law		51
	A.	Foreign Intelligence Law as a System for Both National Security and the Rule of Law	52
	B.	The Special Status of the 1978 Compromise	54
	C.	To What Extent Did "Everything Change" After September 11?	56
		1. Magnitude of the Threat	57
		2. Threat from Terrorists Rather than Nation States	57
		3. Sleeper Cells and Other Domestic Threats	57
		4. The Failure of the Previous Intelligence System	58
		5. The Need to Respond in "Real Time"	58
	D.	Some Responses to the Claim that "Everything Has Changed"	58
		1. The Magnitude and Non-Nation State Nature of the Threat	60
		2. The Threat Domestically	61
		3. The Failure of the Previous Intelligence System	62
		4. The Need to Respond in "Real Time"	63
	E.	Considerations Suggesting Caution in Expanding Surveillance Powers	64
VI.	Proposals for Reform		68
	A.	The Practical Expansion of FISA Since 1978	70
		1. Expand Reporting on FISA Surveillance	72
		2. Defining "Agent of a Foreign Power"	75
	B.	Section 215 and National Security Letter Powers to Get Records and Other Tangible Objects	77
		1. Expanding the Use of National Security Letters	78
		2. Using FISA to Get Records and Other Tangible Objects	78
		3. The Unjustified Expansion of the "Gag Rule"	82
	C.	What To Do About "The Wall"	85
		1. The Logic of the Conflicting Positions	85
		2. One Way to Rebuild "The Wall"	87
		3. Resolving the Dilemma By Focusing on the Foreign Intelligence Value of the Surveillance	89
	D.	Improved Procedures for the Foreign Intelligence Surveillance Court System	92
		1. More of an Adversarial System in the FISC	92
		2. Adversary Counsel in FISCR Appeals	93
		3. Possible Certification to the FISC in Criminal Cases	93
		4. Create a Statutory Basis for Minimization and Other Rulemaking by the FISC	94
	E.	Additional Oversight Mechanisms	95
		1. Reporting on Uses of FISA for Criminal Investigations	

	and Prosecutions	96
2.	Disclosure of Legal Theories	96
3.	Judiciary Committee Oversight	96
5.	Consider Greater Use of Inspector General Oversight After the Fact	97
6.	Consider Providing Notice of FISA Surveillance Significantly After the Fact	97
Conclusion		98

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.