Protect America Act of 2007 and FISA Amendments Act of 2008: More Hastily Passed Statutes

a history of attempts to modify the Foreign Intelligence Surveillance Act after July 2007 and how Americans lost some of their privacy.

Table of Contents

Introduction

My initial interest in the Foreign Intelligence Surveillance Act (FISA) was sparked by President Bush's urgent demand for amendments to FISA on 28 July 2007, as a result of a secret court ruling. I began this document to collect quotations from news sources after 27 July 2007, as a resource for students of legal history.

For information on the FISA statute, including a bibliography of law review articles and list of links to websites, see my separate essay at http://www.rbs0.com/FISA.pdf .

News During July/August 2007

On 27 April 2007, the executive branch proposed a number of amendments to FISA.[1] After secret discussions between Mike McConnell, the Director of National Intelligence, and senators and representatives in Congress, the list of amendments was shortened. McConnell submitted a final draft to Congress on 27 July 2007.[2] These amendments are called the Protect America Act of 2007. The following day, President Bush mentioned the subject in his Saturday morning radio address. Here is the President's entire address, with my comments in footnotes.

> Good morning. This week I visited with troops at Charleston Air Force Base. These fine men and women are serving courageously to protect our country against dangerous enemies. The terrorist network that struck America on September the 11th wants to strike our country again. To stop them, our military, law enforcement, and intelligence professionals need the best possible information about who the terrorists are, where they are, and what they are planning.
>
> One of the most important ways we can gather that information is by monitoring terrorist communications. The Foreign Intelligence Surveillance Act — also known as FISA — provides a critical legal foundation that allows our intelligence community to collect this information while protecting the civil liberties of Americans. But this important law was written in 1978, and it addressed the technologies of that era. This law is badly out of date — and Congress must act to modernize it.[3]
>
> Today we face sophisticated terrorists who use disposable cell phones and the Internet to communicate with each other, recruit operatives, and plan attacks on our country. Technologies like these were not available when FISA was passed nearly 30 years ago, and FISA has not kept up with new technological developments. As a result, our Nation is hampered in its ability to gain the vital intelligence we need to keep the American people safe. In his testimony to Congress in May, Mike McConnell, the Director of National Intelligence, put it this way: We are "significantly burdened in capturing overseas communications of foreign terrorists planning to conduct attacks inside the United States."
>
> To fix this problem, my Administration has proposed a bill that would modernize the FISA statute. This legislation is the product of months of discussion with members of both parties in the House and the Senate — and it includes four key reforms: First, it brings FISA

---

[1] Joby Warrick and Walter Pincus, "How the Fight for Vast New Spying Powers Was Won," *The Washington Post,* (12 Aug 2007).

[2] Ellen Nakashima and Spencer S. Hsu, "Democrats Offer Compromise Plan on Surveillance," *The Washington Post,* (2 Aug 2007).

[3] The President neglected to say that FISA, 50 U.S.C. §§ 1801-1808, had been amended *six* times since 11 Sep 2001. See 115 Stat. 282-283, 291, 295, 364, 392 (26 Oct 2001); 115 Stat. 1402-1403 (28 Dec 2001); 116 Stat. 1812 (2 Nov 2002); 116 Stat. 2258 (25 Nov 2002); 118 Stat. 3691, 3742 (17 Dec 2004); 120 Stat. 195, 197, 203-205, 248 (9 Mar 2006). There is no good reason why FISA should be "badly out of date".

> up to date with the changes in communications technology that have taken place over the past three decades.[4] Second, it seeks to restore FISA to its original focus on protecting the privacy interests of people inside the United States, so we don't have to obtain court orders to effectively collect foreign intelligence about foreign targets located in foreign locations. Third, it allows the government to work more efficiently with private-sector entities like communications providers, whose help is essential. And fourth, it will streamline administrative processes so our intelligence community can gather foreign intelligence more quickly and more effectively, while protecting civil liberties.
>
> Our intelligence community warns that under the current statute, we are missing a significant amount of foreign intelligence that we should be collecting to protect our country. Congress needs to act immediately to pass this bill, so that our national security professionals can close intelligence gaps and provide critical warning time for our country.
>
> As the recent National Intelligence Estimate reported, America is in a heightened threat environment. Reforming FISA will help our intelligence professionals address those threats — and they should not have to wait any longer.[5] Congress will soon be leaving for its August recess. I ask Republicans and Democrats to work together to pass FISA modernization now, before they leave town.[6] Our national security depends on it.

President George W. Bush, Saturday morning radio address, http://www.whitehouse.gov/news/releases/2007/07/20070728.html (28 July 2007).

The true motivation for these amendments is murky, but *The Los Angeles Times* reported on Thursday, 2 Aug 2007:

> A special court that has routinely approved eavesdropping operations has put new restrictions on the ability of U.S. spy agencies to intercept e-mails and telephone calls of suspected terrorists overseas, U.S. officials said Wednesday.
>
> The previously undisclosed ruling by the Foreign Intelligence Surveillance Court has prompted concern among senior intelligence officials and lawmakers that the efforts of U.S. spy agencies to track terrorism suspects might be impaired at a time when analysts have warned that the United States is under heightened risk of attack.
>
> It also has triggered a push in Congress this week to pass temporary legislation that would protect parts of a controversial eavesdropping program launched by the Bush administration after the Sept. 11 attacks.
>
> The administration and Democrats are at odds over how to address the issue, leading to concerns that it might not be resolved before Congress starts its August recess Monday.

---

[4] Despite what President Bush said, the final text of the Protect America Act says *nothing* about any communications technology. And yet this Act was satisfactory, according to President Bush.

[5] Remember, these changes were first proposed yesterday. This is *not* a situation where Congress has been tardy. The proposed bill, S. 1927, was first introduced in the U.S. Senate on 1 Aug 2007, by Senator Mitch McConnell, four days *after* President Bush's speech.

[6] If these changes to FISA are *really* important to our national security, why did the executive branch propose them on 27 July 2007, one week before the scheduled beginning of Congress's vacation? The President did not hint at an answer to this obvious question, but in his previous paragraph, the President did say "Congress needs to act immediately".

> This week, congressional leaders have alluded to the recent decision by the court, which was created in 1978 as part of the Foreign Intelligence Surveillance Act.
>
> House Minority Leader John A. Boehner (R-Ohio) said in a television interview Tuesday evening: "There's been a ruling, over the last four or five months, that prohibits the ability of our intelligence services and our counterintelligence people from listening in to two terrorists in other parts of the world where the communication could come through the United States."
>
> Senate Intelligence Committee Chairman John D. Rockefeller IV (D-W.Va.) said Wednesday that "recent technical developments" had convinced him that "we must take some immediate but interim step to improve collection of foreign intelligence in a manner that doesn't compromise civil liberties of U.S. citizens."
>
> Neither Rockefeller nor Boehner would elaborate, but U.S. intelligence and congressional officials familiar with the matter said they were referring to the FISA court ruling.

Greg Miller, "Court puts limits on surveillance abroad," *The Los Angeles Times,* 2 Aug 2007.

The Washington Post confirmed the decision of the secret court:

> A federal intelligence court judge earlier this year secretly declared a key element of the Bush administration's wiretapping efforts illegal, according to a lawmaker and government sources, providing a previously unstated rationale for fevered efforts by congressional lawmakers this week to expand the president's spying powers.
>
> House Minority Leader John A. Boehner (R-Ohio) disclosed elements of the court's decision in remarks Tuesday to Fox News as he was promoting the administration-backed wiretapping legislation. Boehner has denied revealing classified information, but two government officials privy to the details confirmed that his remarks concerned classified information.
>
> The judge, whose name could not be learned, concluded early this year that the government had overstepped its authority in attempting to broadly surveil communications between two locations overseas that are passed through routing stations in the United States, according to two other government sources familiar with the decision.
>
> The decision was both a political and practical blow to the administration, which had long held that all of the National Security Agency's enhanced surveillance efforts since 2001 were legal. The administration for years had declined to subject those efforts to the jurisdiction of the Foreign Intelligence Surveillance Court, and after it finally did so in January the court ruled that the administration's legal judgment was at least partly wrong.

Carol D. Leonnig and Ellen Nakashima, "Ruling Limited Spying Efforts — Move to Amend FISA Sparked by Judge's Decision," *The Washington Post,* (3 Aug 2007).

The following day, *The Washington Post* repeated the information about the secret decision by the secret FISA Court:

> Adding to the urgency for the administration is a secret ruling by a FISA judge earlier this year that declared surveillance of purely foreign communications that pass through a U.S. communications node illegal without a court-approved warrant — a requirement that intelligence officials have described as unacceptably burdensome.

Joby Warrick and Ellen Nakashima, "Senate Votes To Expand Warrantless Surveillance," *The Washington Post,* (4 Aug 2007).

after the approval on 5 Aug 2007

After Congress voted to approve the amendments, *The Boston Globe* newspaper reported:

> The debate over surveillance dates back to the weeks after the Sept. 11 attacks, when Bush signed a secret order authorizing the NSA to wiretap Americans' international e-mails and phone calls without a court order — even though the 1978 warrant law prohibited it. Bush asserted that his wartime powers gave him an unwritten right to bypass such a law.
>
> In January 2007, [Attorney General] Gonzales announced that the program had been brought under the oversight of the national security court. A judge on the court had issued an unusual classified order allowing some form of the surveillance to continue.
>
> But several months ago another judge on the court ruled that the order was unlawful, shutting down some part of the program and leading to the White House push to get Congress to amend the surveillance law.

Charlie Savage, "New law expands power to wiretap, Diminishes oversight of NSA spy program," *The Boston Globe,* 6 August 2007.

Although Democrats were then the majority party in both the House of Representatives and Senate, they offered little opposition — except to include a six-month sunset provision.[7] The reason for the lack of opposition is that the Bush administration made vague remarks about an increase in communications amongst terrorists, as if an attack on the USA were imminent. Only 32% of senators who voted, and only 45% of representatives who voted, had the courage to risk protecting civil liberties when there was a *possibility* of an attack on the USA. If a terrorist attack occurred, those who voted against the Protect America Act would be portrayed as "soft on terrorism" in the 2008 elections,[8] which could end their political career.

More than one week after Congress approved the Protect America Act, *The Washington Post* revealed a little more about the motivation for these amendments to FISA:

> But in a secret ruling in March [2007], a judge on a special court empowered to review the government's electronic snooping challenged for the first time the government's ability to collect data from such wires even when they came from foreign terrorist targets.
>
> In May [2007], a judge on the same court went further, telling the administration flatly that the law's wording required the government to get a warrant whenever a fixed wire is involved.

---

[7] On 14 August 2007, I predicted that Congress will *not* be ready to enact reasonable legislation in six months. During the four years of the first enactment of the PATRIOT Act, Congress did not find the will to include civil liberties protections during the renewal of the PATRIOT Act. Furthermore, the technical legal concerns about FISA are not important to most citizens, who are more concerned about the war in Iraq, immigration reform, affordable health care, energy policy, and Social Security reform.

[8] See, e.g., the following editorials in newspapers: anonymous, "The Politics of Fear," *The Los Angeles Times,* (7 Aug 2007); Helen Thomas, "Yet again, the Democrats roll over," *Seattle Post-Intelligencer* (9 Aug 2007); Bill Press, "Cowardly Democrats Give In To President On NSA wiretapping," *Baltimore Sun,* (13 Aug 2007).

> "All of a sudden, the world flipped upside down," said a senior administration official familiar with the rulings. The official declined to be identified by name, citing the confidentiality of court decisions involving the Foreign Intelligence Surveillance Act.
>
> The decisions had the immediate practical effect of forcing the NSA to laboriously ask judges on the Foreign Intelligence Surveillance Court each time it wanted to capture such foreign communications from a wire or fiber on U.S. soil, a task so time-consuming that a backlog developed. "We shoved a lot of warrants at the court" but still could not keep up, the official said. "We needed thousands of warrants, but the most we could do was hundreds." The official depicted it as an especially "big problem" by the end of May, in which the NSA was "losing capability."
>
> McConnell even appealed directly to the FISA court, meeting with judges to describe the impact the decisions were having. The judges were sympathetic but said they believed that the law was clear. "They said, 'We don't make legislation — we interpret the law,' " the senior administration official said.
>
> The rulings — which were not disclosed publicly until the congressional debate this month — represented an unusual rift between the court and the U.S. intelligence community. They led top intelligence officials to conclude, a senior official said, that "you can't tell what this court is going to do" and helped provoke the White House to insist that Congress essentially strip the court of any jurisdiction over U.S. surveillance of communications between foreigners.

Joby Warrick and Walter Pincus, "How the Fight for Vast New Spying Powers Was Won," *The Washington Post,* (12 Aug 2007).

The last two paragraphs of this quotation suggest an inappropriately cozy relationship between the FISA court and the U.S. intelligence agencies. The FISA court was intended to provide oversight and to prevent abuses by the intelligence agencies.

On 22 Aug 2007, the *El Paso Times* published a transcript of their question and answer session with Director of National Intelligence, Mike McConnell. I found the following remarks chilling:

> **Q:** Even if it's perception, how do you deal with that? You have to do public relations, I assume.
>
> **A:** Well, one of the things you do is you talk to reporters. And you give them the facts the best you can. Now part of this is a classified world. The fact we're doing it this way means that some Americans are going to die, because we do this mission unknown to the bad guys because they're using a process that we can exploit and the more we talk about it, the more they will go with an alternative means and when they go to an alternative means, remember what I said, a significant portion of what we do, this is not just threats against the United States, this is war in Afghanistan and Iraq.
>
> **Q.** So you're saying that the reporting and the debate in Congress means that some Americans are going to die?
>
> **A.** That's what I mean. Because we have made it so public. We used to do these things very differently, but for whatever reason, you know, it's a democratic process and sunshine's a good thing. We need to have the debate. The reason that the FISA law was passed in 1978 was an arrangement was worked out between the Congress and the administration, we did not want to allow this community to conduct surveillance, electronic surveillance, of Americans for foreign intelligence unless you had a warrant, so that was required. So there was no warrant required for a foreign target in a foreign land. And so we are trying to get back to what was the intention of '78. Now because of the claim, counterclaim, mistrust, suspicion, the only way you could make any progress was to have this debate in an open way.

Q. So you don't think there was an alternative way to do this?
A. There may have been an alternative way, but we are where are ....
Q. A better way, I should say.
A. All of my briefs initially were very classified. But it became apparent that we were not going to be able to carry the day if we don't talk to more people.
Q. Some might say that's the price you pay for living in a free society. Do you think that this is necessary that these Americans die?
A. We could have gotten there a different way. We conducted intelligence since World War II and we've maintained a sensitivity as far as sources and methods. It's basically a sources and methods argument. If you don't protect sources and methods then those you target will choose alternative means, different paths. As it is today al-Qaida in Iraq is targeting Americans, specifically the coalition. There are activities supported by other nations to import electronic, or explosively formed projectiles, to do these roadside attacks and what we know about that is often out of very sensitive sources and methods. So the more public it is, then they take it away from us. So that's the tradeoff.

Chris Roberts, "Transcript: Debate on the foreign intelligence surveillance act," *El Paso Times* (22 Aug 2007) http://www.elpasotimes.com/ci_6685679

The executive branch of the government has a long history of making selective disclosures of classified material to provide political justification for military programs, intelligence programs, and foreign policy. I hope the executive branch is *not* going to posture a vigorous public debate about government surveillance as killing Americans. But if the executive branch is going to engage in this kind of propaganda, the response is that some things may be worth dying for, just as President Bush has sent more than 3700 U.S. military personnel to their deaths in Iraq.

How the Protect America Act Was Passed

my comments

That this happened in the USA is simply astounding. First, the president of the USA willfully violates a federal statute for five years.[9] Then a judge on a secret court issues a classified opinion that allows "some form of surveillance to continue." And then another judge on a secret appellate court reverses the classified opinion, making the surveillance illegal again. Citizens are totally in the dark about this possible incursion on their freedom, because of the classified opinions issued by secret courts.

But it gets worse. Mike McConnell presented draft amendments to FISA on 27 July 2007, to make his desired surveillance legal. On Wednesday, 1 Aug 2007, Senator Mitch McConnell introduced the Protect America Act in a proposed bill, S. 1927, in the U.S. Senate. On Friday night, 3 Aug 2007, the U.S. Senate passed the Protect America Act by a vote of 60 to 28. The U.S. House of Representatives passed the Protect America Act on Saturday night, 4 Aug 2007, by a vote of 227 to 183. Congress then went on ~~vacation~~ recess. President Bush signed the Protect America Act on Sunday afternoon. The hasty passage by Congress of the administration's desired

[9] See my separate essay on the Terrorist Surveillance Program at http://www.rbs0.com/TSP.pdf .

amendments is essentially an abdication of the checks and balances inherent in having three equal branches of government: executive, legislative, and judicial. Note that U.S. Congress passed the Protect America Act without any hearings in any of their committees!

Regardless of the true (and secret) motivation of President Bush in asking Congress to enact amendments to FISA approximately one week before Congress was scheduled to go on vacation, this one-week interval was *not* adequate time for democracy to function. Although the FISA amendments were reported in major U.S. newspapers from 30 July 2007 to 6 August 2007, one week is not enough time for citizens to send letters to their representatives and senators, and one week is not enough time for organizations (e.g., ACLU[10]) to mobilize their supporters. And one week is certainly not enough time for Congress to respond in a thoughtful, independent way that preserves the checks-and-balances role of the legislative branch against the executive branch.

As mentioned above on page 6, liberal commentators harshly criticized the Democrats who voted for the Protect America Act. In my opinion, those Democrats deserve criticism. But what about the Republicans who voted for the Protect America Act? The Republican party *used* to be opposed to big government, opposed to socialism and governmental paternalism, and in favor of individual freedom from oppression by the government. While I don't want to stray into politics, I think the Republicans have betrayed their own political principles. In short, I think that *all* of the people in Congress who voted for the Protect America Act deserve criticism.

Text of Protect America Act of 2007

Full text of the Protect America Act is available from two sources:
(1) http://thomas.loc.gov/cgi-bin/bdquery/z?d110:s.01927: (Library of Congress)

Government Printing Office website:
(2) http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:s1927enr.txt.pdf

my comments on the Protect America Act

Amongst other amendments, the Protect America Act adds to FISA a new section 105B, part of which says:

> Notwithstanding any other law, the Director of National Intelligence and the Attorney General, may for periods of up to one year authorize the acquisition of foreign intelligence information concerning persons reasonably believed to be outside the United States if the Director of National Intelligence and the Attorney General determine, based on the information provided to them, that —

---

[10] "ACLU Warns Congress Against Rushing Spy Law Changes," American Civil Liberties Organization press release, http://www.aclu.org/safefree/general/31157prs20070731.html (31 July 2007).

(1) there are reasonable procedures in place for determining that the acquisition of foreign intelligence information under this section concerns persons reasonably believed to be located outside the United States, and such procedures will be subject to review of the Court pursuant to section 105C of this Act;
(2) the acquisition does not constitute electronic surveillance;
(3) the acquisition involves obtaining the foreign intelligence information from or with the assistance of a communications service provider, custodian, or other person (including any officer, employee, agent, or other specified person of such service provider, custodian, or other person) who has access to communications, either as they are transmitted or while they are stored, or equipment that is being or may be used to transmit or store such communications;
(4) a significant purpose of the acquisition is to obtain foreign intelligence information; and
(5) the minimization procedures to be used with respect to such acquisition activity meet the definition of minimization procedures under section 101(h).

This determination shall be in the form of a written certification, under oath, supported as appropriate by affidavit of appropriate officials in the national security field occupying positions appointed by the President, by and with the consent of the Senate, or the Head of any Agency of the Intelligence Community, **....**

Protect America Act, § 105B(a).

I find it confusing that § 105B(a)(2) says that the government is authorized to acquire foreign intelligence information that "does *not* constitute electronic surveillance",[11] while § 105B(a)(3) says the acquired information comes from a "communications service provider ... who has access to communications, either as they are transmitted or while they are stored". I understand the phrase "communications service provider" to mean corporations such as telephone companies and Internet service providers. The term "communications service provider" is *not* defined in either FISA or the Protect America Act, but is defined in other statutes.[12]

If one simply ignores § 105B(a)(2), then subsection (a) allows the government to wiretap for any surveillance "concerning persons reasonably believed to be outside the United States", without the approval of the FISA court. In other words, subsection (a) returns us to the pre-FISA area in 1978, when — according to case law — warrantless wiretaps are acceptable if the primary purpose of the surveillance is to collect foreign intelligence information. However, § 105B(a)(4) continues from the PATRIOT Act "a significant purpose".[13] Because "a significant purpose" is broader than "the primary purpose", § 105B(a) may be unconstitutional.

---

[11] *Electronic surveillance* is defined as "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication ...." 50 U.S.C. § 1801(f)(1). Alternatively, it can mean "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, ..." 50 U.S.C. § 1801(f)(4).

[12] 18 U.S.C. § 2510(15) says: "*electronic communication service* means any service which provides to users thereof the ability to send or receive wire or electronic communications".

[13] See my essay http://www.rbs0.com/FISA.pdf , in the section "Purpose of FISA".

Later in section 105B there are a series of subsections about the ability of the government to get a judicial order compelling communications service providers to provide information from their customers' communications. The "person" in this quoted statute refers to a "communications service provider ... who has access to communications, either as they are transferred or while they are stored".[14] In law, corporations are fictitious persons.

> **(e)** With respect to an authorization of an acquisition under section 105B, the Director of National Intelligence and Attorney General may direct a person to —
>
> (1) immediately provide the Government with all information, facilities, and assistance necessary to accomplish the acquisition in such a manner as will protect the secrecy of the acquisition and produce a minimum of interference with the services that such person is providing to the target; and
>
> (2) maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the acquisition or the aid furnished that such person wishes to maintain.
>
> **(f)** The Government shall compensate, at the prevailing rate, a person for providing information, facilities, or assistance pursuant to subsection (e).
>
> **(g)** In the case of a failure to comply with a directive issued pursuant to subsection (e), the Attorney General may invoke the aid of the court established under section 103(a) to compel compliance with the directive. The court shall issue an order requiring the person to comply with the directive if it finds that the directive was issued in accordance with subsection (e) and is otherwise lawful. Failure to obey an order of the court may be punished by the court as contempt of court. Any process under this section may be served in any judicial district in which the person may be found.

Protect America Act, § 105B.

Is the person in (g) entitled to appear before the court and argue against the judicial order? Does this mean that the person — who might be in Alaska, Hawaii, or California — needs to hire an attorney in Washington, DC to appear before the FISA court (i.e., "the court established under section 103(a)")? The answer to both questions is apparently yes:

> **(h)(1)**
>
> **(A)** A person receiving a directive issued pursuant to subsection (e) may challenge the legality of that directive by filing a petition with the pool established under section 103(e)(1).
>
> **(B)** The presiding judge designated pursuant to section 103(b) shall assign a petition filed under subparagraph (A) to one of the judges serving in the pool established by section 103(e)(1). Not later than 48 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the directive. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the directive or any part of the directive that is the subject of the petition. If the assigned judge determines the petition is not frivolous, the assigned judge shall, within 72 hours, consider the petition in accordance with the

[14] Protect America Act, § 105B(a)(3).

> procedures established under section 103(e)(2) and provide a written statement for the record of the reasons for any determination under this subsection.
>
> **(h)(2)** A judge considering a petition to modify or set aside a directive may grant such petition only if the judge finds that such directive does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the directive, the judge shall immediately affirm such directive, and order the recipient to comply with such directive.
>
> **(h)(3)** Any directive not explicitly modified or set aside under this subsection shall remain in full effect.

Protect America Act, § 105B(h).

In this way, the FISA court no longer approves request for wiretaps, when the targets are outside the USA. Instead, the Director of National Intelligence and the Attorney General, working together, approve all wiretap requests when the targets are outside the USA. The FISA court is only used to grant judicial orders compelling Americans to comply with a directive for wiretaps. Note also that the government does *not* reimburse the legal fees of any communication service provider who successfully protects the privacy of its subscribers by getting a directive modified or set aside.

The Protect America Act also provides complete immunity to communication service providers who comply with directives of the FISA court:

> Notwithstanding any other law, no cause of action shall lie in any court against any person for providing any information, facilities, or assistance in accordance with a directive under this section.

Protect America Act, § 105B(ℓ).

While complying with a judicial order is probably a good defense to any action for breach of contract or tort, this absolute immunity makes it easy for communication service providers to win summary judgment motions that dismiss litigation filed by their customers.[15] The statutory grant of absolute immunity means that most communication service providers will *not* be challenging directives in the FISA court.

---

[15] An example of the kind of litigation that this statute is intended to prevent is *Hepting v. AT & T Corp.,* 439 F.Supp.2d 974 (N.D.Cal. 2006).

News During September 2007

When Congress went on vacation in August, various representatives and senators promised to resume work on the Protect America Act when they returned in September. In September, Congressional committees held at least four hearings on the Protect America Act. Meanwhile, during September 2007, the executive branch continued to publicly call for at least removing the sunset provision in the Protect America Act.

The House Select Committee on Intelligence held a hearing on FISA on 6 Sep 2007.

U.S. Director of National Intelligence Mike McConnell appeared before the Senate Committee on Homeland Security and Government Affairs on 10 Sep 2007 and urged the senators to make the Protect America Act permanent.

U.S. Director of National Intelligence Mike McConnell released a long statement to the House Judiciary Committee on 18 Sep 2007:
http://judiciary.house.gov/media/pdfs/McConnell070918.pdf (2101 Kbytes).

On 25 Sep 2007, the Senate Judiciary Committee held hearings on the Protect America Act. Michael McConnell testified there too.

I was surprised that mainstream news media essentially ignored all of these important hearings. I scan the top Associated Press national news stories and Google News on the Internet several times each day, but I did not see any coverage of these Congressional hearings. The big stories in Congress during September 2007 were:

- report by General Petraeus to Congress on war in Iraq, Democrats attempt to bring troops home
- reaction to President Bush's nomination of a new Attorney General, Michael Mukasey
- reauthorization or reform of No Child Left Behind Act
- expansion of children's health insurance by Democrats in Congress, which Bush threatened to veto
- appropriations for Fiscal Year 2008

14 Sep 2007

Kenneth L. Wainstein, the Assistant Attorney General for National Security, sent a letter[16] to the House Select Committee on Intelligence on 14 Sep 2007 that clarified the executive branch's understanding of the Protect America Act. *The Washington Post* reported:

....

[16] A copy of the letter is posted at: http://www.fas.org/irp/news/2007/09/wainstein091407.pdf .

... Assistant Attorney General Kenneth L. Wainstein said the Protect America Act, passed in August under intense White House pressure, does not authorize physical searches of homes, domestic mail or people's personal effects and computers, and that Justice Department lawyers "do not think" it authorizes the collection of medical or library records.

He said that "to the extent that this provision could be read to authorize the collection of business records of individuals in the United States . . . we wish to make very clear that we will not use this provision to do so."

"To put it plainly," Wainstein said, "the Protect America Act does not authorize so-called domestic wiretapping without a court order, and the executive branch will not use it for that purpose."

But key Democratic lawmakers said their concerns are not allayed.

"The Bush administration admits that the Protect America Act can be read to let them collect Americans' business records," said Rep. John Conyers Jr. (D-Mich.), chairman of the House Judiciary Committee. "They simply ask us to trust them not to. Trust is not good enough — that's why we need to have court oversight."

....

Ellen Nakashima, "Bush Administration Aiming To Ease Surveillance Concerns," *The Washington Post,* p. A03 (15 Sep 2007).
http://www.washingtonpost.com/wp-dyn/content/article/2007/09/14/AR2007091402206.html

19 Sep 2007

On 19 Sep 2007, President Bush visited the National Security Agency headquarters and gave the following public speech, which quoted here in its entirety:

Good morning. I have just received a briefing from Director McConnell and Lieutenant General Alexander, as well as other members of my national security team. I first want to thank the men and women who work out here for their dedication and their hard work. The work they're doing here is necessary to protect our country from an enemy who would like to attack us again. The people who work out here understand that the federal government has no more urgent responsibility than to protect the American people.

Every day, our intelligence, law enforcement and homeland security professionals confront enemies who are smart, who are ruthless, and who are determined to murder innocent people to achieve their objectives. It is the job of Congress to give the professionals the tools they need to do their work as effectively as possible.

You don't have to worry about the motivation of the people out here; what we do have to worry about is to make sure that they have all the tools they need to do their job. One of the most important tools they use is the Foreign Intelligence Surveillance Act, or FISA. The law provides a critical legal foundation that allows our intelligence community to monitor terrorist communications while protecting the freedoms of American people. Unfortunately, the law is dangerously out of date.

When FISA was passed nearly 30 years ago, the legal protections were based on differences in the way that domestic and overseas communications were transmitted. New technologies have come into being since the law was written. Technologies like the disposable cell phone or the Internet eliminated many of those differences. So one of the consequences of the way the law was originally drafted is that when technology changed, legal protections meant only for the people in the United States began applying to terrorists on foreign soil. As

a result, our intelligence professionals reported that they were missing a significant amount of real-time intelligence needed to protect the American people. So earlier this year, Director McConnell sent Congress legislation to fix the problem.

In August, a bipartisan majority in Congress passed the Protect America Act. This law has helped close a critical intelligence gap, allowing us to collect important foreign intelligence and information about terrorist plots. The problem is the law expires on February 1st — that's 135 days from today. The threat from al Qaeda is not going to expire in 135 days.

So I call on Congress to make the Protect America Act permanent. The need for action is clear. Director McConnell has warned that unless the FISA reforms in the Act are made permanent, our national security professionals will lose critical tools they need to protect our country. Without these tools, it'll be harder to figure out what our enemies are doing to train, recruit and infiltrate operatives in our country. Without these tools our country will be much more vulnerable to attack.

Unfortunately, some in Congress now want to restrict the tools. These restrictions would impede the flow of information that helps us protect our people. These restrictions would reopen gaps in our intelligence that we had just closed. As I did in August, in evaluating any FISA bill, I will ask Director McConnell whether the legislation gives him what he needs to protect our nation. The question I'm going to ask is, do our professionals have the tools necessary to do the job to protect the American people from further attack?

In addition to making the Protection [sic] America Act permanent, I urge Congress to take up other critical proposals included in the comprehensive FISA reform my administration submitted last April. It's particularly important for Congress to provide meaningful liability protection to those companies now facing multi-billion dollar lawsuits only because they are believed to have assisted in efforts to defend our nation following the 9/11 attacks. Additionally, without this protection, state secrets could be revealed in connection with those lawsuits — and our ability to protect our people would be weakened.

At stake in this debate is more than a piece of legislation. The decisions Congress makes will directly affect our ability to save American lives. I look forward to working with Congress to enact this legislation as quickly as possible, so that our intelligence officials will continue to have the tools they need to keep the American people safe. Thank you.

President Bush, "President Bush Discusses the Protect America Act of 2007," (19 Sep 2007). http://www.whitehouse.gov/news/releases/2007/09/20070919.html

"Fact Sheet"

On 19 Sep 2007 the White House posted at its website the following "Fact Sheet" about the Protect America Act. As a comment to students: anytime you hear a politician talk about "facts" you should be aware that you are going to get sprayed with propaganda. The boldface and italics in the following quotation are present in the original text at the White House website.

FISA Amendments In The Protect America Act Of 2007 Remain Necessary To Keep Our Nation Safe

The Protect America Act modernized the Foreign Intelligence Surveillance Act (FISA) to provide our intelligence community essential tools to acquire important information about terrorists who want to harm America. The Act, which passed with bipartisan support in the House and Senate and was signed into law by President Bush on August 5, 2007, restores FISA to its original focus of protecting the rights of persons in the United States, while not acting as an obstacle to gathering foreign intelligence on targets

located in foreign countries. By enabling our intelligence community to close a critical intelligence gap that existed before the Act became law, the Protect America Act has already made our Nation safer.

- **The tools provided by the Protect America Act are scheduled to expire in early February 2008 – it is essential that Congress act to make the legislation permanent.** Congress must also pass legislation to provide meaningful liability protection to those alleged to have assisted our Nation following the 9/11 attacks.

The Protect America Act Of 2007 Modernizes FISA In Four Important Ways

1. **The Protect America Act permits our intelligence professionals to more effectively collect foreign intelligence information on targets in foreign lands without first receiving court approval.** The new law accomplishes this by clarifying that FISA's definition of "electronic surveillance" does not apply to activities directed at persons reasonably believed to be outside the United States, thereby restoring the statute to its original focus on appropriate protections for the rights of persons in the United States.

   - **Electronic surveillance targeting a person in the U.S. continues to require a court order under the Protect America Act.** The statute does not change FISA's definition of "electronic surveillance" as it applies to domestic-to-domestic communications and surveillance targeting persons in the United States.

2. **The Protect America Act provides a role for the FISA Court in reviewing the procedures the intelligence community uses to ensure that collection remains directed at persons located overseas.** The Attorney General is required to submit to the FISA court the procedures by which the Federal government determines that the authorized acquisitions of foreign intelligence do not constitute electronic surveillance and thus do no trigger FISA's court approval requirements.

3. **The Protect America Act provides a mechanism for the FISA Court to direct third parties to assist the intelligence community in its collection efforts.** The Act permits the Director of National Intelligence and the Attorney General to direct communications service providers to provide the information, facilities, and assistance necessary to conduct authorized foreign intelligence activities. In the event such a person fails to comply with a directive, the Attorney General may invoke the aid of the FISA Court to compel compliance with the directive. By the same token, the Act allows third parties to challenge a directive in the FISA Court.

4. **The Protect America Act protects third parties from private lawsuits arising from assistance they provide the Government in authorized foreign intelligence activities targeting individuals located outside the United States.** But the Act does not provide retrospective liability protection for those alleged to have assisted our Nation following the 9/11 attacks. Congress needs to act to provide such protection.

The Basics Of FISA: Why The Protect America Act Of 2007 Is Necessary To Bring The Law Up-To-Date

Congress enacted the Foreign Intelligence Surveillance Act (FISA) in 1978 to regulate the Government's efforts to conduct certain foreign intelligence surveillance activities directed at persons *in the United States*. Congress recognized that the Government must be able to effectively collect foreign intelligence about those who wish to harm our country. To allow this collection to proceed while protecting the rights of Americans in the United States, Congress established a process for judicial approval that generally applied when the government targeted persons *located inside the United States* for foreign intelligence surveillance – but which generally did not apply to activities directed at persons *overseas.*

Revolutionary advances in telecomunications technology since 1978 have upset the careful balance established by Congress to distinguish between surveillance governed by FISA and surveillance directed at targets outside the U.S. The mechanism Congress used to identify which activities fell within FISA's scope – and to strike the balance between surveillance directed at persons overseas and persons in the United States – was a careful and complex definition of the term "electronic surveillance." This definition was framed in terms of the specific communications technologies used in 1978.

As a result, prior to the Protect America Act, the Government often needed to obtain a court order before vital intelligence collection could begin against a terrorist or other foreign intelligence target located in a foreign country. These targets *often were communicating with other foreign persons overseas*, but FISA's court order requirement still applied. It made no sense to require the Government to obtain a court order to collect *foreign* intelligence on targets located in *foreign* countries, nor was such a requirement intended when Congress passed FISA nearly 30 years ago.

This requirement resulted in a critical intelligence gap that was making our Nation less safe. Requiring the Government to go to court before the collection of foreign intelligence could begin resulted, as the Director of National Intelligence put it, in our intelligence professionals "missing a significant amount of foreign intelligence that we should be collecting to protect our country."

By changing FISA's definition of electronic surveillance to clarify that the statute does not apply to surveillance directed at overseas targets, the Protect America Act has enabled the intelligence community to close this critical intelligence gap. The Protect America Act makes clear – consistent with the intent of the Congress that enacted FISA in 1978 – that our intelligence community should not have to get bogged down in a court approval process to gather foreign intelligence on targets located in foreign countries. It does not change the strong protections FISA provides to people in the United States. FISA's definition of electronic surveillance remains unchanged for surveillance directed at people in the United States, and continues to require court approval as it did before.

"Fact Sheet: FISA 101: Why FISA Modernization Amendments Must Be Made Permanent," http://www.whitehouse.gov/news/releases/2007/09/20070919-1.html (19 Sep 2007).

New Definition of Privacy

Donald Kerr, the Principal Deputy Director of National Intelligence, gave a speech on 23 Oct 2007 to the United States Geospatial Intelligence Foundation, in which he proposed a new definition of privacy. Historically, in the USA privacy was the "right to be let alone"[17] — including freedom from surveillance by government unless authorized by a judge, and including the freedom to speak and read anonymously.[18]

> ....
>
> And that leads you directly into the concern for privacy. Too often, privacy has been equated with anonymity; and it's an idea that is deeply rooted in American culture. The Lone Ranger wore a mask[,] but Tonto didn't seem to need one even though he did the dirty work for free. You'd think he would probably need one even more. But in our interconnected and wireless world, anonymity — or the appearance of anonymity — is quickly becoming a thing of the past.
>
> ....
>
> Protecting anonymity isn't a fight that can be won. Anyone that's typed in their name on Google understands that.[19] Instead, privacy, I would offer, is a system of laws, rules, and customs with an infrastructure of Inspectors General, oversight committees, and privacy boards on which our intelligence community commitment is based and measured. ....

Dr. Kerr's final paragraph said:

> It's a debate we need to have in the United States. It's not necessarily best carried out in hearing rooms; it's certainly not best carried out in television environments where people just scream at each other. But I think it's going to take serious, long-term debate for us all to get it right. ....

Later, in the question and answer session, Dr. Kerr responded to a question about "the notion that privacy does not equal anonymity":

---

[17] See, e.g., Ronald B. Standler, Privacy Law in the USA, http://www.rbs2.com/privacy.htm (July 1997).

[18] See, e.g., Ronald B. Standler, Disclosure Should Not Always Destroy Privacy, http://www.rbs2.com/priv4.pdf , (Oct 2007).

[19] I am not certain what Dr. Kerr intends to say here. Is his point that search queries on Google are not private? Or is his point that there is much public information about some people available on the Internet? The former is wrong, Google is one of a few search engines to guard the privacy of queries, see *Gonzales v. Google, Inc.,* 234 F.R.D. 674 (N.D.Cal. 17 Mar 2006), discussed in my essay at http://www.rbs2.com/priv4.pdf . The latter is also wrong: I know many professionals (including some attorneys, physicians, and professors) whose names are mentioned in zero (or only a few) webpages.

> It's a really good question, because, in fact, it's a personal question that everyone, in a way, has to answer for themselves. But I think today, you know, I'm willing to call up, pick the vendor of your choice. I'm willing to share my credit card number and expiration date with a person I have never seen, have no idea whether they've been vetted or not. I've certainly been able to get past being anonymous in that transaction. And of course, you multiply that by all of the transaction[s] that you're involved in every day.
>
> I was taken by a thing that happened to me at the FBI, where I also had electronic surveillance as part of my responsibility. And people were very concerned that the ability to intercept emails was coming into play. And they were saying, well, we just can't have federal employees able to touch our message traffic. And the fact that, for that federal employee, it was a felony to misuse the data — it was punishable by five years in jail and a $100,000 fine, which I don't believe has ever happened — but they were perfectly willing for a green-card holder at an ISP who may or may not have been an illegal entrant to the United State to handle their data.[20] It struck me as an anomalous situation.[21]
>
> So this is not something where groupthink works for an answer. I think all of us have to really take stock of what we already are willing to give up, in terms of anonymity, but what safeguards we want in place to be sure that giving that up doesn't empty our bank account or do something equally bad elsewhere.

Donald Kerr, http://www.dni.gov/speeches/20071023_speech.pdf (23 Oct 2007).

What I find most chilling about this speech is *not* the provocative ideas in it, but that a government official is *telling* the American people what they must accept. In a real democracy, the people — through their legislators — tell the government what to do. The Bush administration, including Dr. Kerr, has the whole process backwards.

The 23 Oct speech by Dr. Kerr was reported by the Associated Press on 11 Nov 2007, but even that news report created little public reaction.

> As Congress debates new rules for government eavesdropping, a top intelligence official says it is time that people in the United States changed their definition of privacy.
>
> Privacy no longer can mean anonymity, says Donald Kerr, the principal deputy director of national intelligence. Instead, it should mean that government and businesses properly safeguard people's private communications and financial information.
>
> Kerr's comments come as Congress is taking a second look at the Foreign Intelligence Surveillance Act.
>
> ....

Pamela Hess, "Intel Official: Expect Less Privacy," Associated Press (13:36 ET 11 Nov 2007). http://www.washingtonpost.com/wp-dyn/content/article/2007/11/12/AR2007111200677.html

---

[20] This is a remarkable piece of propaganda. First, it includes a tautology (i.e., "who may or may not have been"). Second, it raises the spectre of illegal immigrants handling confidential information.

[21] Standler's comment: Partly the so-called anomaly comes from the Fourth Amendment that protects Americans against *un*reasonable searches by the government, but there is nothing comparable to protect Americans against abuse by corporations or corporate employees.

RESTORE Act of 2007 (H.R. 3773)

On 9 October 2007, U.S. House of Representatives Judiciary Committee Chairman John Conyers (D-Mich.) introduced H.R. 3773, a bill that would replace the Protect America Act of 2007. The new bill has the pretentious name "Responsible Electronic Surveillance That is Overseen, Reviewed and Effective (RESTORE) Act of 2007". In my opinion, it is self-serving praise for the House to call the proposed bill "responsible", and Congress has failed to exert any significant oversight or review of surveillance since Sep 2001. Who knows if the surveillance will be "effective"? Nonetheless, I believe that the RESTORE Act is an improvement on the Protect America Act.

text of RESTORE Act of 2007 (H.R. 3773):
http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h3773ih.txt.pdf (9 Oct version)

http://frwebgate.access.gpo.gov/cgi-bin/getdoc.cgi?dbname=110_cong_bills&docid=f:h3773rh.txt.pdf (12 Oct version)

http://thomas.loc.gov/cgi-bin/query/D?c110:3:./temp/~c110XNN2da:: (15 Nov final version)

The Associated Press reported on 9 Oct 2007 that Democrats in the U.S. House of Representatives would be willing to grant telecom companies retroactive immunity for cooperating with government surveillance (i.e., illegal wiretapping), but only if the executive branch made a disclosure of the Terrorist Surveillance Program.

> A top Democratic leader opened the door Tuesday to granting U.S. telecomunications companies retroactive legal immunity for helping the government conduct electronic surveillance without court orders, but said the Bush administration must first detail what those companies did.
>
> House Majority Leader Steny Hoyer, D-Md., said providing the immunity will likely be the price of getting President Bush to sign into law new legislation extending the government's surveillance authority. About 40 pending lawsuits name telecomunications companies for alleged violations of wiretapping laws. Democrats introduced a draft version of the new law Tuesday — without the immunity language.
>
> "We have not received documentation as to what in fact was done, for which we've been asked to give immunity," Hoyer said.
>
> ....
>
> The bill would replace a law enacted in August that is due to expire early next year. That bill was hastily adopted under pressure from the Bush administration, which said changes in technology had resulted in dire gaps in its authority to eavesdrop on terrorists.

Pamela Hess, "Dems Opens Door for Immunity in Spy Bill," Associated Press (18:00 EDT 9 Oct 2007), also published in *The Washington Post.*

Because the executive branch has consistently refused to provide Congress with details of this illegal surveillance program,[22] Hoyer's condition is likely to be poison.

On 10 Oct 2007 President Bush declared that he would not sign any legislation, unless it provided retroactive immunity to telecom companies.

> Good morning. In August, Congress passed the Protect America Act, a bill to modernize the Foreign Intelligence Surveillance Act of 1978. This new law strengthened our ability to collect foreign intelligence on terrorists overseas, and it closed a dangerous gap in our intelligence. Since this important measure took effect, our intelligence professionals have been able to gather critical information that would have been missed without this authority. And keeping this authority is essential to keeping America safe.
>
> Unfortunately, when Congress passed the Protect America Act they set its provisions to expire in February. The problem is the threat to America is not going to expire in February. So Congress must make a choice: Will they keep the intelligence gap closed by making this law permanent? Or will they limit our ability to collect this intelligence and keep us safe, staying a step ahead of the terrorists who want to attack us?
>
> My administration will work with members of Congress from both sides of the aisle to reach an agreement on a bill that will allow us to protect our country. The final bill must meet certain criteria: It must give our intelligence professionals the tools and flexibility they need to protect our country. It must keep the intelligence gap firmly closed, and ensure that protections intended for the American people are not extended to terrorists overseas who are plotting to harm us. **And it must grant liability protection to companies who are facing multi-billion-dollar lawsuits only because they are believed to have assisted in the efforts to defend our nation following the 9/11 attacks.**[23]
>
> When Congress presents me with a bill, I will ask the Director of National Intelligence whether it meets these criteria. And if it does, I will sign it into law.
>
> Today, the House Intelligence and Judiciary Committees are considering a proposed bill that instead of making the Protect America Act permanent would take us backward. While the House bill is not final, my administration has serious concerns about some of its provisions, and I am hopeful that the deficiencies in the bill can be fixed.
>
> Congress and the President have no higher responsibility than protecting the American people from enemies who attacked our country — and who want to do so again. Terrorists in faraway lands are plotting and planning new ways to kill Americans. The security of our country and the safety of our citizens depend on learning about their plans. The Protect America Act is a vital tool in stopping the terrorists — and it would be a grave mistake for Congress to weaken this tool.
>
> On another issue before Congress, I urge members to oppose the Armenian genocide resolution now being considered by the House Foreign Affairs Committee. We all deeply regret the tragic suffering of the Armenian people that began in 1915. This resolution is not the right response to these historic mass killings, and its passage would do great harm to our relations[24] with a key ally in NATO and in the global war on terror.

---

[22] See my essay at http://www.rbs0.com/TSP.pdf .

[23] Boldface added by Standler.

[24] Turkey was then threatening to invade northern Iraq.

President Bush, speech on South Lawn of White House (11:10 EDT 10 Oct 2007).
http://www.whitehouse.gov/news/releases/2007/10/20071010.html

On 11 Oct 2007, the U.S. House Judiciary and Intelligence Committees made several amendments to the RESTORE Act of 2007 and then approved the bill.

On 12 Oct, *The San Francisco Chronicle* published an editorial by legal director of the Electronic Freedom Foundation:

> When Congress rushed to pass the so-called "Protect America Act" on its way out the door for its August recess, San Francisco's Nancy Pelosi, speaker of the House of Representatives, expressed great regret, telling the New York Times on Aug. 5 that the new law "does violence to the Constitution of the United States." She vowed to take steps to correct the temporary measure long before it expires in February 2008.
>
> Now is the time for Speaker Pelosi to make good on that promise, or at least prevent any further harm. In the last couple of weeks, the Bush administration has stepped up the pressure on Congress to surrender even more of individual citizens' privacy and civil liberties. At the top of the Bush administration's list: granting retroactive immunity to the telecomunications companies that have been participating with the National Security Agency in the widespread and incontrovertibly illegal warrantless surveillance of ordinary Americans since 2001. Granting this immunity would prevent the courts from ever ruling on the legality of the "dragnet" surveillance and from imposing needed restraints. Not content with the sweeping new powers granted to it by Congress in August, the Bush administration is essentially demanding that the now Democratic-led Congress cave in to a cover-up.
>
> San Franciscans have a special reason to be concerned about the Bush administration's retroactive immunity push. The best evidence of the dragnet surveillance comes from AT&T's building at 611 Folsom St. in San Francisco. AT&T's own documents show an NSA-controlled room on the sixth floor of that building where millions of e-mail messages to and from ordinary San Franciscans are being indiscriminately copied for the NSA. The 40 or so lawsuits challenging this warrantless surveillance are all being heard here in San Francisco. The U.S. Ninth Circuit Court of Appeals — just a few blocks from the AT&T spy room — heard the leading case in mid-August and is expected to rule soon. The courts appear to be handling the litigation with extreme care: doing their job to ensure that the law is followed without endangering national security.
>
> So what could make Speaker Pelosi, along with Sen. Dianne Feinstein, D-San Francisco, who is a member of the key Senate Intelligence Committee, consider bending to this latest administration effort to muscle the courts out of their role in enforcing the law? Some say the Democrats are so afraid of looking soft on terrorism that they would rubber-stamp anything the administration labels "terrorism-related" — even handing over millions of innocent communications between ordinary Americans. Others fear that most Democrats in Congress don't really know the details of what's actually going on. The administration has only publicly admitted "targeting" individuals located abroad whose messages happen to pass through the United States.
>
> Maybe Speaker Pelosi and Sen. Feinstein don't realize that there is hard evidence that the NSA is engaging in the wholesale interception of everyone's communications with the help of the telecomunications companies like AT&T. Or maybe the phone companies are arguing that, if they are not let off the hook scot free this time, they might refuse the next time the NSA asks for wholesale access to the communications of Americans. But isn't that exactly what we want them to do? Shouldn't a polite "come back with a warrant and we'll jump right

> on it," be the telecomunication carriers' response to government requests that violate customer privacy and the law?
>
> Given recent struggles with the Republican minority, it may be that Speaker Pelosi cannot fix all of the problems with the temporary Protect America Act now. But she cannot and should not make things worse. Granting blanket, no-questions-asked immunity for the telephone companies — particularly retroactive immunity with the aim of ending critical ongoing cases now before federal courts — is a bad idea that must be taken off the table.
>
> The courts must be allowed to determine whether the NSA's wiretapping is illegal and, if so, to put a stop to it. Ordinary San Franciscans have a personal stake in this and, with it, a unique opportunity and responsibility to tell the speaker and senior senator from California — their hometown representatives — what they think. The most fundamental of American freedoms is at stake, and there's no time to lose. Speaker Pelosi's San Francisco office number is (415) 556-4862. Sen. Feinstein's is (415) 393-0707. The local carrier for those calls? AT&T.

Cindy Cohn, "Congress should not assist in a cover-up of NSA spying," *The San Francisco Chronicle* p. B11 (12 Oct 2007)
http://www.sfgate.com/cgi-bin/article.cgi?file=/c/a/2007/10/12/ED9GSOGRP.DTL .

I agree with Ms. Cohn — the telecom companies should be legally responsible for any invasions of privacy (including violations of wiretap statutes) arising from their cooperation with unlawful demands by the U.S. government. The telecom companies should consistently be very careful of their legal obligations to protect the privacy of their customers' communications. Moreover, the telecom companies have large legal departments that could easily challenge in court any unlawful subpoenas and other demands by the government.

On 17 Oct 2007, President Bush held a press conference at which he criticized Congress on a number of issues. Here is what he said about surveillance legislation at the beginning of the event:

> Congress has work to do to keep our people safe. One of the things Congress did manage to get done this year is pass legislation that began modernizing the Foreign Intelligence Surveillance Act. FISA is a law that our intelligence professionals use to monitor the communications of terrorists who want to do harm to our people. The problem is that Congress arranged for the measure they passed to expire this coming February. In addition, the House is now considering another FISA bill that would weaken the reforms they approved just two months ago. When it comes to improving FISA, Congress needs to move forward, not backward, so we can ensure our intelligence professionals have the tools they need to protect us.

President Bush, press conference (10:45 17 Oct 2007)
http://www.whitehouse.gov/news/releases/2007/10/20071017.html

A vote in the entire House of Representatives was scheduled for 17 Oct 2007, but the vote was canceled on 17 Oct. The Associated Press explained:

> Republicans successfully maneuvered to derail a Democratic government eavesdropping bill Wednesday, delaying a House vote until next week at the earliest.
>
> ....

> The House's Democratic leaders pulled the bill after discovering that Republicans planned to offer a motion that politically vulnerable Democrats would have a hard time voting against.
>
> The amendment would have said that nothing in the bill could limit surveillance of Osama bin Laden and terrorist organizations. While Democrats say their bill already provides that authority, voting against the amendment could make it seem as though a member of Congress were against spying on al-Qaida.
>
> Republicans sought to play down the amendment's role in causing the bill to be pulled. Michigan Rep. Pete Hoekstra, the top Republican on the House Intelligence Committee, said the bill was losing moderate Democratic votes because it was fundamentally flawed.
>
> Passage of the Republican amendment would have sent the bill immediately back to committee, effectively killing it. Key Democrats believed they were short of the votes needed to defeat the move.
>
> "Our proposal gives Democrats a very simple choice: They can allow our intelligence officials to conduct surveillance on the likes of Osama bin Laden and al-Qaida or prohibit them from doing so and jeopardize our national security," said Republican leader Rep. John Boehner of Ohio in a statement.
>
> ....

Pamela Hess, "House Surveillance Bill Pulled," Associated Press (20:59 EDT 17 Oct 2007).

On 15 Nov 2007, after making small changes in the bill, the Democratic party leadership in the U.S. House of Representatives again attempted to pass the RESTORE Act of 2007, H.R. 3773. This time the bill passed the entire House on a 227 to 187 vote.[25] The bill contained *no* immunity for telecom companies.

Because the final bill contained *no* immunity for telecom companies, amongst other alleged defects, the bill faced a veto by President Bush:

> In August, Congress took an important step toward modernizing the Foreign Intelligence Surveillance Act of 1978 by enacting the Protect America Act of 2007 (PAA). While only in effect for less than four months, the PAA has allowed us temporarily to close an intelligence gap by enabling our intelligence professionals to collect, without a court order, foreign intelligence on targets located overseas. The intelligence community has implemented the Protect America Act in a responsible way, subject to extensive congressional oversight, to meet the country's foreign intelligence needs while protecting civil liberties. Unless reauthorized by Congress, however, the authority provided in the Protect America Act will expire in February 2008. In the face of the continued and grave terrorist risks to our Nation, Congress must act to make the PAA permanent. Congress also must provide protection from private lawsuits against companies alleged to have assisted the Government in the aftermath of the September 11 terrorist attacks on America.
>
> While the Administration appreciates Congress's recognition of the need to modernize our foreign intelligence surveillance laws, H.R. 3773 accomplishes neither of these twin objectives. This bill does not result in permanent FISA modernization and it contains no retroactive liability provision. H.R. 3773 therefore falls far short of providing the Intelligence Community with the tools it needs effectively to collect foreign intelligence information vital for the security of the Nation. Accordingly, if H.R. 3773 is presented in its current form to

---

[25] http://thomas.loc.gov/cgi-bin/bdquery/z?d110:h.r.03773:

the President, the Director of National Intelligence and the President's other senior advisers will recommend that he veto the bill.

....

H.R. 3773 is deficient in several particular aspects:

....

Fails to Provide Retroactive Liability Protection for Companies Alleged to Have Assisted the Government in the Wake of the September 11 Terrorist Attacks. The Administration strongly opposes H.R. 3773 because it fails to grant liability protection to companies alleged to have assisted the Government's counterterrorism efforts in the aftermath of the September 11th attacks. It is a matter of basic fairness that providers who are alleged to have provided assistance to the Government in the wake of these terrorist attacks should not face liability claims. It also is critical to our national security that such companies be protected from litigation, since companies that face lawsuits for allegedly assisting the Government may be unwilling to provide assistance if and when it is needed to prevent future terrorist attacks.

....

Statement of Administration Policy (15 Nov 2007)
http://www.whitehouse.gov/omb/legislative/sap/110-1/hr3773sap-h.pdf

Senate Bill (S.2248)

Senate Intelligence Committee: Oct 2007

On 18 Oct 2007, the U.S. Senate Intelligence Committee began debating a draft bill that included retroactive immunity for telecom companies.

The draft bill would direct civil courts to dismiss lawsuits against telecomunications companies if the attorney general certifies that the company rendered assistance between Sept. 11, 2001 and Jan. 17, 2007, in response to a written request authorized by the president, to help detect or prevent an attack on the United States.

Suits also would be dismissed if the attorney general certifies that a company named in the case provided no assistance to the government. The public record would not reflect which certification was given to the court, according to Democratic and Republican aides who spoke on condition of anonymity because the committee had not yet acted.

Committee member Sen. Russell Feingold, D-Wis., said he would not support any immunity provision because the documents the panel reviewed proved to him the wiretapping activities were illegal.

Pamela Hess, "Intel bill includes telecom immunity," Associated Press (14:57 EDT 18 Oct 2007).

In a joint press release by U.S. Senators Jay Rockefeller (D-WV) and Kit Bond (R-Missouri) — Chairman and Vice-Chairman of the Senate Intelligence Committee — they described their draft bill:

Key features of the bill are:

- Authority for the intelligence community to conduct the intelligence collection needed to protect our country.

- Strong FISA Court review and approval of the procedures used to accomplish that collection.
- FISA Court review of the minimization procedures used to protect U.S. person information.
- Individual court review for targeting US persons overseas.
- Improved oversight by the FISA Court, the Congress, and the agencies' Inspectors General.
- Targeted immunity for companies who assisted the government after the 9/11 attacks.
- A six-year sunset to allow Congress to evaluate how the new authorities in the legislation are being carried out.

> FISA was carefully crafted in 1978 to balance the need to collect intelligence with the requirement to protect Americans' civil liberties. It was drafted to deal specifically with the technology in use at the time. Over the last 30 years, the world has experienced a technology revolution, yet the FISA statute has not kept pace. This bill brings FISA up to date with today's technology.

Jay Rockefeller and Kit Bond, Press Release (18 Oct 2007)
http://intelligence.senate.gov/press/record.cfm?id=285708

The draft bill passed the Senate Intelligence Committee after one day of consideration by the Committee:

> The Senate Intelligence Committee voted Thursday [18 Oct] to strengthen court oversight of government surveillance while protecting telecomunications companies from civil lawsuits for tapping Americans' phones and computers without court approval.
>
> The panel's approval of the bill, 13-2, doesn't guarantee smooth sailing for the legislation. It still must get the blessing of the Senate Judiciary Committee, whose top Republican and Democratic members have expressed skepticism about the immunity provision.
>
> ....
>
> Exactly what electronic surveillance the Bush administration has conducted inside the United States is classified.
>
> Bush administration officials could face criminal charges if they broke wiretapping and privacy laws, Rockefeller said.
>
> "There is no immunity for government officials," Rockefeller said. "It is the administration who must be accountable for warrantless wiretapping."
>
> ....

Pamela Hess, "Intel Panel OKs Surveillance Bill," Associated Press (09:00 EDT 19 Oct 2007).

On 26 Oct 2007, the Rockefeller-Bond draft became S. 2248, The FISA Amendments Act of 2007.

Senate Judiciary Committee: 31 Oct to 15 Nov 2007

On 31 Oct 2007, Senator Leahy, Chairman of the Senate Judiciary Committee, made the following opening statement at his committee's hearings on S.2248:

> The Foreign Intelligence Surveillance Act (FISA) is intended to protect both our national security and the privacy and civil liberties of Americans.
>
> Changes to that law must be considered carefully and openly — not eviscerated in secret Administration interpretations or compromised through fear or intimidation. The so-called Protect America Act, passed just before the summer recess, was an example of the worst way to consider changes to FISA. It was hurriedly passed under intense, partisan pressure from the Administration. It provides sweeping new powers to the government to engage in surveillance — without warrants — of international calls to and from the United States involving Americans, and it provided no meaningful protection for the privacy and civil liberties of the Americans who are on those calls.
>
> Fortunately, the Protect America Act will expire early next year. This is the Committee's second hearing to inform our consideration of possible legislation to take the place of that flawed Act. Of course we must accommodate legitimate national security concerns and the need for flexibility in surveillance of overseas targets, but Congress should do that in a way that protects the civil liberties of Americans.
>
> I commend the House Committees and the Senate Select Committees on Intelligence for seeking to incorporate the better ideas from our work this summer into their current legislative proposals. The House of Representatives is considering the RESTORE Act, which appears to take a fair and balanced approach — allowing flexibility for the Intelligence Community while providing oversight and protection for Americans' privacy. The Senate Select Committee on Intelligence has also reported a bill that makes improvements to the current temporary law. Increasing the role of the FISA Court and oversight by the Inspector General and the Congress are matters we should have incorporated this summer.
>
> At the outset I should acknowledge the grave concern I have with one aspect of S.2248. It seeks to grant immunity — or, as Senator Dodd has called it, "amnesty" — for telecomunications carriers for their warrantless surveillance activities from 2001 through this summer, which would seem to be contrary to FISA and in violation of the privacy rights of Americans.
>
> Before even considering such a proposal, Senator Specter and I have always been clear with the Administration that we would need the legal justifications, authorizations, and other documents that show the basis for the actions of the government and the carriers. Since the existence of the President's secret wiretapping program became public in December 2005, this Committee has sought that relevant information through oral and written requests and by conducting oversight hearings. After our repeated requests did not yield the information the Committee requested, we authorized and issued subpoenas for documents related to the legal justification for the President's program.
>
> Finally, this week, the Administration has belatedly responded. Senators on the Committee and designated staff have begun to receive access to legal opinions and documents concerning authorization and reauthorization of the program. This is a significant step, though long overdue.
>
> I am considering carefully what we are learning from these materials. **The Congress should be careful not to provide an incentive for future unlawful corporate activity by giving the impression that if corporations violate the law and disregard the rights of Americans, they will be given an after-the-fact free pass. If Americans' privacy is to**

mean anything, and if the rule of law is to be respected, that would be the wrong result.[26]

A retroactive grant of immunity or preemption of state regulators does more than let the carriers off the hook. Immunity is designed to shield this Administration from any accountability for conducting surveillance outside the law. It could make it impossible for Americans whose privacy has been violated illegally to seek meaningful redress.

The lawsuits that would be dismissed as a result of such a grant of immunity are perhaps the only avenue that exists for an outside review of the government's program and honest assessment of its legal arguments. That kind of assessment is critical if our government is to be held accountable. One of my chief inquiries before deciding to support any legislation on this subject is whether it will foster government accountability. Anyone who proposes letting the telecomunications carriers off the hook or preempting state authorities has a responsibility to propose a manner to test the legality of the government's program and to determine whether it did harm to the rights of Americans.

Safeguarding the new powers we are giving to our government is far more than just an academic exercise. The FISA law itself is testament to the fact that unchecked government power leads to abuse. The FISA was enacted in the wake of earlier scandals, when the rights and privacy of Americans were trampled while no one was watching. We in the Senate, and on this Committee, have a solemn responsibility to hundreds of millions of our fellow citizens. Because the American people's rights, freedom and privacy are easily lost; but once lost, they are difficult to win back.

I look forward to the testimony of our witnesses and thank them for appearing.

Patrick Leahy, http://judiciary.senate.gov/member_statement.cfm?id=3009&wit_id=2629 (31 Oct 2007).

The U.S. Senate Judiciary Committee was *not* willing to grant retroactive immunity to telecom companies. The Associated Press reported on 31 Oct 2007:

The top members of the Senate Judiciary Committee said Wednesday [31 Oct] that the nation's courts may be the only way to determine if the White House violated wiretapping and privacy laws when it eavesdropped on Americans without court orders.

The senators remain reluctant to grant legal immunity to telecomunications companies that allegedly helped.

Legal protection for the companies is a top priority for President Bush, who has vowed to veto any eavesdropping bill that does not provide it.

Telecomunications companies face about 40 civil lawsuits nationwide for alleged violations of wiretapping and surveillance laws at the Bush administration's request. Another five lawsuits have been filed against the U.S. government.

At issue is the interception of American e-mails and phone calls from 2001 to 2007. The so-called Terrorist Surveillance Program was conducted without the consent of the secret Foreign Intelligence Surveillance Court, which oversees intelligence agencies' eavesdropping inside the United States.

The Senate Intelligence Committee provided immunity in its version of a new eavesdropping bill. It bars civil lawsuits against telecomunication companies if the attorney general and national intelligence director certify that the companies acted on written orders approved by the president. The Judiciary panel still needs to act on the bill before it goes before the full Senate.

---

[26] Boldface added by Standler.

> Judiciary Committee Chairman Sen. Patrick Leahy, D-Vt., said he would agree to immunize telecomunications only if there is an effective way to scrutinize the Bush administration's secret surveillance program.
>
> "The lawsuits ... are perhaps the only avenue that exists for an outside review of the government's program, an honest assessment of its legal arguments, especially as the Congress has for years been stonewalled on this program," Leahy said at a committee hearing Wednesday.
>
> The committee's senior Republican, Pennsylvania Sen. Arlen Specter, said the courts are best equipped to rein in presidential powers. "In the long history of this country, the courts have done a much better job in protecting civil liberties than has the Congress from an overreaching executive branch," he said.
>
> Assistant Attorney General Kenneth Wainstein said the lawsuits could financially cripple the telecomunications industry with billions in fines if they lost. He said even closed court hearings could harm national security by airing classified information. And he warned that terrorists could target companies accused in court.

....

Pamela Hess, "Senate Panel Balks at Telecom Immunity," Associated Press (17:55 ET 31 Oct 2007).

The Washington Post reported on the Senate Judiciary Committee hearings:

> In a blow to the Bush administration, the Senate Judiciary Committee's top Democrat and Republican expressed reluctance yesterday to granting blanket immunity to telecomunications carriers sued for assisting the government's warrantless surveillance program.
>
> Committee Chairman Patrick J. Leahy (D-Vt.) and the ranking Republican, Sen. Arlen Specter (Pa.), had said that before even considering such a proposal, they would need to see the legal documents underpinning the program, which began after Sept. 11, 2001, and were put under court oversight in January.
>
> On Tuesday, the committee was given access to some of the documents. But Leahy said yesterday that he had a "grave concern" about blanket immunity, saying that "it seems to grant . . . amnesty for telecomunications carriers for warrantless surveillance activities."
>
> The activities seem to be "in violation of the privacy rights of Americans" and of federal domestic surveillance law, he said, noting that he is still "carefully considering" what is in the documents.
>
> The immunity provision sought by the White House would wipe out about 40 lawsuits that accuse AT&T, Verizon Communications and Sprint Nextel of invading Americans' privacy and constitutional rights by assisting the government in domestic surveillance without a warrant.
>
> The Senate intelligence committee approved the provision two weeks ago as part of a larger bill to amend the Foreign Intelligence Surveillance Act, which governs some aspects of domestic surveillance. The Judiciary Committee will take up the bill next.
>
> Immunity "is designed to shield this administration from accountability for conducting surveillance outside the law," Leahy said. Dismissing the lawsuits would eliminate "perhaps the only avenue" for "an honest assessment" of the legality of the warrantless surveillance program, he said.
>
> Specter agreed that the "courts ought not to be closed" to such lawsuits. "If, at this late date, the Congress bails out whatever was done before — and we can't even discuss what has been done — that is just an open invitation for this kind of conduct in the future," he said.

> Specter added that he thinks the carriers "have a strong, equitable case" but that his inclination is toward indemnification, where the government would assume any financial penalties.
>
> ....

Ellen Nakashima, "Roadblock for Telecom Immunity: Senate Judiciary Leaders Resist Leniency for Surveillance," *The Washington Post,* p. A06 (1 Nov 2007)
http://www.washingtonpost.com/wp-dyn/content/article/2007/10/31/AR2007103103126.html

However, on 15 Nov 2007, the Senate Judiciary Committee decided by an 11 to 8 vote to accept the telecom immunity that was in the draft bill, S.2248, that had been approved by the Senate Intelligence Committee. Chairman Leahy hoped to remove the immunity in debate on the floor of the Senate in early December, after Congress returns from a two-week Thanksgiving ~~vacation~~ recess.

See my separate essay at http://www.rbs0.com/TSP.pdf for a discussion of negotiations between the White House and Senate Judiciary Committee for access to classified documents on the terrorist surveillance program in exchange for the Judiciary Committee agreeing to provide immunity for telecoms.

President Bush: 1 Dec 2007

On 1 Dec, President Bush again urged Congress to pass legislation to "modernize" FISA:

> Good morning. Next week, Congress returns from its Thanksgiving recess. Members are coming back to a lot of unfinished business. And the clock will be ticking, because they have only a few weeks to get their work done before leaving again for Christmas.
>
> Congress must address four critical priorities. First, Congress needs to pass a bill to fund our troops in combat. Second, Congress needs to make sure our intelligence professionals can continue to monitor terrorist communications so we can prevent attacks against our people. Third, Congress needs to pass a bill to protect middle-class families from higher taxes. And fourth, Congress needs to pass all the remaining appropriations bills to keep the Federal Government running.
>
> ....
>
> Another priority Congress must address is the Foreign Intelligence Surveillance Act, or FISA. FISA provides a critical legal framework that allows our intelligence community to monitor terrorist communications while protecting the freedoms of the American people. Unfortunately, the law is dangerously out of date. In August, Congress passed legislation to help modernize FISA. That bill closed critical intelligence gaps, allowing us to collect important foreign intelligence. The problem is, this new law expires on February 1st — while the threat from our terrorist enemies does not.
>
> Congress must take action now to keep the intelligence gaps closed — and make certain our national security professionals do not lose a critical tool for keeping America safe. As part of these efforts, Congress also needs to provide meaningful liability protection to

> those companies now facing multi-billion dollar lawsuits only because they are believed to have assisted in the efforts to defend our Nation following the 9/11 attacks.
>
> ....

President Bush, Weekly Radio Address,
http://www.whitehouse.gov/news/releases/2007/12/20071201.html (1 Dec 2007).

I am convinced that such appeals are mostly propaganda. We don't need to "modernize" FISA. If anything, we need to revise FISA to make it clearer and easier to understand that the government must get an order from the FISA court *before* conducting surveillance on U.S. citizens inside the USA. And we don't get a better — or safer — nation by having more surveillance. And we need a government that obeys its own laws, instead of having the illegal Terrorist Surveillance Program.

Full Senate: 17 December 2007

The full Senate was scheduled to debate the draft bill, S.2248, and more than one dozen amendments on 17 Dec 2007. First, Senator Christopher Dodd (D-Conn.) spoke for several hours, opposing immunity for telecoms, and he threatened to filibuster the bill. By noon, the Senate defeated Dodd on a 76 to 10 vote. After debate during the afternoon and evening, the Senate Majority Leader, Harry Reid (D-Nev.) pulled the bill from consideration, so that the Senate could focus on critical appropriations bills before adjourning for the Christmas/New Year holiday.[27] Reid issued the following press release:

> The Senate is committed to improving our nation's intelligence laws to fight terrorism while protecting Americans' civil liberties. We need to take the time necessary to debate a bill that does just that, rather than rushing one through the legislative process. While we had hoped to complete the FISA bill this week, it is clear that is not possible. With more than a dozen amendments to this complex and controversial bill, this legislation deserves time for thorough discussion on the floor.
>
> We will consider this bill when we return in January. In the meantime, I again encourage the Director of National Intelligence and the Attorney General to make available to all Senators the relevant documents on retroactive immunity, so that each may reach an informed decision on how to proceed on this provision. I oppose retroactive immunity, but believe every Senator must have access to the information to make this important decision.

Harry Reid, Press Release, http://reid.senate.gov/newsroom/record.cfm?id=289303&
(17 Dec 2007)

---

[27] Pamela Hess, "Senators Debate Immunity for Telecoms," Associated Press (13:53 EST 17 Dec 2007); Pamela Hess, "Senate Takes Up Surveillance Bill," (18:12 EST 17 Dec 2007); Pamela Hess, "Surveillance Bill Delayed Until 2008," Associated Press (22:43 EST 17 Dec 2007); Jonathan Weisman and Paul Kane, "Telecom Immunity Issue Derails Spy Law Overhaul: Reid Pulls Legislation, Citing Insufficient Time Before Recess," *The Washington Post,* p. A02 (18 Dec 2007).

The Washington Post incidentally and tersely remarked on Republican efforts to attack Democrats who vote against surveillance legislation favored by the Bush administration:

> After the House passed surveillance legislation that did not include retroactive immunity, the National Republican Senatorial Committee accused House Democrats running for the Senate of "putting the rights of known terrorists ahead of the safety and security of Americans."

Jonathan Weisman and Paul Kane, "Telecom Immunity Issue Derails Spy Law Overhaul: Reid Pulls Legislation, Citing Insufficient Time Before Recess," *The Washington Post,* p. A02 (18 Dec 2007). This kind of attack on dissenters motivates an orthodoxy in which no professional politician dares oppose the Bush administration.

January 2008

When Congress returned from its Christmas/New Year's holiday, Congress suddenly noticed that the economy was in shambles. The Standard & Poor's index of 500 largest stocks had declined from 1560 in Oct 2007 to 1320 on 22 Jan 2008, a decline of 15% in three months. So the hot topic in Congress was immediately passing some kind of economic stimulus, in an attempt to avoid a recession. The 1 Feb 2008 deadline for the renewal of the Protect America Act was ignored by most politicians.

On 22 Jan 2008, Senate Majority leader Harry Reid asked for unanimous consent to extend the deadline for renewal of the Protect America Act. The leader of the Republicans in the Senate objected.[28]

On 24 Jan 2008, the Senate by a 60 to 36 vote, rejected the Judiciary Committee version of the bill, which contained no immunity for telecom companies.[29] The Intelligence Committee's version of the bill (S.2248), which contains retroactive immunity demanded by President Bush, will be considered by the full Senate on Monday, 28 Jan.[30] *The Washington Post* reported:

> The issue has spilled over into the Democratic presidential race: Sens. Hillary Rodham Clinton (N.Y.) and Barack Obama (Ill.) have said that they oppose legal immunity for the telecoms, but neither was present for yesterday's vote. In a series of e-mails to supporters yesterday, the liberal group `MoveOn.org` urged Clinton and Obama to help lead a filibuster to block the immunity legislation in the Senate.

---

[28] Pamela Hess, "Senate Rejects Surveillance Law Renewal," Associated Press (22 Jan 2008 18:46 EST)

[29] Dan Eggen, "Senate Rejects Expansion of Secret Court's Oversight," *The Washington Post,* (24 Jan 2008 17:07 EST) http://www.washingtonpost.com/wp-dyn/content/article/2008/01/24/AR2008012401098.html

[30] Pamela Hess, "Senate Delays Eavesdropping Vote," Associated Press (24 Jan 2008 19:45 EST).

Dan Eggen and Paul Kane, "Phone Firms' Bid for Immunity in Wiretaps Gains Ground," *The Washington Post,* p. A03 (25 Jan 2008)
http://www.washingtonpost.com/wp-dyn/content/article/2008/01/24/AR2008012403454_pf.html

Bush[31] and Cheney[32] continue to characterize lawsuits against telephone companies as punishing the companies for helping the government fight terrorism. I think a more accurate characterization would be that the telephone companies knew, or should have known, that they were violating the law by intercepting communications of their customers — American citizens, who are legally entitled to privacy in their communications. It is quite proper to hold the telephone companies accountable for their unlawful acts that invaded the privacy of American citizens.

Because the House version of the bill contains no retroactive immunity for telecom companies, President Bush needs to persuade Representatives to include immunity.
On 24 Jan 2008, Bush finally agreed to let members of the House Judiciary Committee and House Intelligence Committee see classified documents on the Terrorist Surveillance Program.[33] With the 1 Feb deadline for a House-Senate conference committee to approve the final legislation, members of the House have little time to review classified documents on the TSP.

On Saturday, 26 Jan 2008, President Bush made his weekly radio address to the nation. He said that there were two issues that "require immediate attention" by Congress: (1) the economic stimulus legislation, and (2) —

> The other urgent issue before Congress is a matter of national security. Congress needs to provide our intelligence professionals with the tools and flexibility they need to protect America from attack. In August, Congress passed a bill that strengthened our ability to monitor terrorist communications. The problem is that Congress set this law to expire on February 1st. That is next Friday. If this law expires, it will become harder to figure out what our enemies are doing to infiltrate our country, harder for us to uncover terrorist plots, and harder to prevent attacks on the American people.
>
> Congress is now considering a bipartisan bill that will allow our professionals to maintain the vital flow of intelligence on terrorist threats. It would protect the freedoms of Americans, while making sure we do not extend those same protections to terrorists overseas. It would provide liability protection to companies now facing billion-dollar lawsuits because they are believed to have assisted in efforts to defend our Nation following the 9/11 attacks. I call on Congress to pass this legislation quickly. We need to know who our enemies are and what they are plotting. And we cannot afford to wait until after an attack to put the pieces together.

George Bush, http://www.whitehouse.gov/news/releases/2008/01/20080126.html (26 Jan 2008).

---

[31] For example, see Bush's radio address on 26 Jan 2008, part of which is quoted below.

[32] Tom Raum, "Cheney Wants Surveillance Law Expanded," Associated Press (23 Jan 2008 15:34 EST), describing Cheney's speech to the Heritage Foundation on 23 Jan 2008.

[33] Pamela Hess, "Bush Opens Wiretap Documents to House," Associated Press, (24 Jan 2008 13:26 EST).

On Monday, 28 Jan, the U.S. Senate voted 48 to 45 for cloture on S.Amend.3911 and 3918, however 60 votes were needed to end debate and have a vote.[34] S.Amend.3918 would have extended by 30 days the 1 Feb expiration of the Protect America Act of 2007.

In his State of the Union speech on Monday night, 28 Jan 2008, President Bush urged Congress to extend the Protect America Act:

> We are grateful that there has not been another attack on our soil since 9/11. This is not for the lack of desire or effort on the part of the enemy. In the past six years, we've stopped numerous attacks, including a plot to fly a plane into the tallest building in Los Angeles and another to blow up passenger jets bound for America over the Atlantic. Dedicated men and women in our government toil day and night to stop the terrorists from carrying out their plans. These good citizens are saving American lives, and everyone in this chamber owes them our thanks. (Applause.)
>
> And we owe them something more: We owe them the tools they need to keep our people safe. And one of the most important tools we can give them is the ability to monitor terrorist communications. To protect America, we need to know who the terrorists are talking to, what they are saying, and what they are planning. Last year, the Congress passed legislation to help us do that. Unfortunately, the Congress set the legislation to expire on February 1. This means that if you do not act by Friday, our ability to track terrorist threats would be weakened and our citizens will be in greater danger. The Congress must ensure the flow of vital intelligence is not disrupted. The Congress must pass liability protection for companies believed to have assisted in the efforts to defend America. We have had ample time for debate. The time to act is now.

George Bush, http://www.whitehouse.gov/news/releases/2008/01/20080128-13.html (28 Jan 2008). There are at least four errors in Bush's second paragraph about surveillance, which was quoted above:

1. Bush's concept that missing the 1 Feb deadline will weaken our ability to monitor terrorists and place Americans "in greater danger" is wrong. After approval by the Foreign Intelligence Surveillance Court, a surveillance order can continue for one year. So the wiretaps issued under the Protect America Act do *not* expire on 1 Feb.
2. Note that Bush invokes the word "terrorist" repeatedly to justify wiretaps, but the controversy amongst civil libertarians is that innocent Americans inside the USA will have their communications monitored if those innocent Americans talk to someone who a low-level government bureaucrat has labeled a "terrorist".
3. Moreover, Bush continues to insist on retroactive immunity for telecom companies who illegally wiretapped communications of Americans. Bush simply violates the principle that the law must apply equally to everyone (i.e., no one is above the law), including telecom companies. Innocent Americans who were injured by illegal activities by the government or corporations must have the opportunity to sue in court.

---

[34] Paul Kane, "GOP Unable to Force Vote on Bush Surveillance Bill," *The Washington Post,* p. A03 (29 Jan 2008).

4. Finally, Bush asserts that "we have had ample time for debate." That is *not* true. There were a few brief hearings in the Intelligence and Judiciary Committees of Congress. But there was little debate open to all members of Congress. In the Senate, open debate was shut down by procedural votes in both December and January.

On 29 Jan 2008, the House of Representatives voted during the day to extend the Protect America Act for 15 days, and the U.S. Senate voted at night for the same extension.[35] And then the House took a one-week vacation. In an earlier version of this essay, I predicted on 14 Aug 2007 that Congress will *not* be ready to enact legislation before the six-month expiration of the Protect America Act. It was an easy prediction, given that few people in Congress really care about surveillance law, few people (both in and out of Congress) understand surveillance law, and the lack of public attention to this issue. Furthermore, the polarizing propaganda that more surveillance will make the USA safer from attack by terrorists has impeded rational discussion of this issue.

On 30 Jan 2008, there were 66 amendments to S.2248 pending in the U.S. Senate. The Senate considered S.2248 on 31 Jan, and unanimously agreed to consider only 12 amendments during 14 hours of scheduled debate.[36] Then, the Senate postponed further discussion until 14:00 on 4 Feb 2008, and took a three-day vacation.[37] The Associated Press ignored these proceedings on S.2248, but did cover Senator Specter's threat to withdraw the National Football League's antitrust exemption because the NFL destroyed evidence of a cheating scandal.[38]

---

[35] Pamela Hess, "Congress Extends Eavesdropping Law," Associated Press (29 Jan 2008 23:52 EST). Paul Kane, "Congress Passes Extension of Surveillance Law," *The Washington Post,* p. A04, http://www.washingtonpost.com/wp-dyn/content/article/2008/01/29/AR2008012902909.html (30 Jan 2008).

[36] CONGRESSIONAL RECORD, pp. S536-S537 (31 Jan 2008).

[37] CONGRESSIONAL RECORD, p. S559 (31 Jan 2008).

[38] Anonymous, "Senator Asks Why NFL Destroyed Tapes," Associated Press (1 Feb 2008 14:26 EST) quotes Sen. Specter: "I do believe that it is a matter of importance. It's not going to displace the stimulus package or the Iraq war, but I think the integrity of football is very important, and I think the National Football League has a special duty to the American people — and further the Congress — because they have an antitrust exemption."

4-11 February 2008

During 4-8 Feb 2008, the big event in the U.S. Senate was the debate and passage of an economic stimulus bill, including rebate checks to taxpayers. However, the Senate did spend some time each day in debate on the surveillance amendments.[39] On 8 Feb 2008, Amendment Nr. 3907, to strike from S.2248 retroactive immunity for telecoms, was scheduled for a vote on 12 Feb . Because of the procrastination by the Senate during the past six months, the Senate Majority Leader, Harry Reid, introduced S.2615 on 8 Feb, which would extend the expiration of the Protect America Act a *second* time, from 15 Feb to 1 March 2008.

Attorney General Michael Mukasey and National Intelligence Director Mike McConnell sent a 12-page letter to leaders in the U.S. Senate, again saying that President Bush would veto any bill that did not include retroactive immunity for telecom companies.[40] To the best of my knowledge, this is the only news story by the Associated Press on the surveillance legislation during 4-9 Feb 2008. On Sunday, 10 Feb, *The New York Times* published a blistering editorial about S.2248 and retroactive immunity for telecoms, in which they noted: "Even by the dismal standards of what passes for a national debate on intelligence and civil liberties, last week was a really bad week."[41]

On Monday, 11 Feb 2008, the Senate finished its debate on amendments to S.2248.[42] Senator Dodd spoke for 150 minutes in favor of Amendment Nr. 3907, to strike from S.2248 retroactive immunity for telecoms.[43]

---

[39] CONGRESSIONAL RECORD, S564-580 (4 Feb 2008), S639-655 (5 Feb 2008), S686-714 (6 Feb 08), S775-778 (7 Feb 2008), S805-813 (8 Feb 2008).

[40] Lara Lakes Jordan, "Bush Threatens Veto in Surveillance Laws," Associated Press (5 Feb 2008 17:39 EST).

[41] anonymous editorial, "Because They Said So," *The New York Times,* http://www.nytimes.com/2008/02/10/opinion/10sun1.html (10 Feb 2008).

[42] CONGRESSIONAL RECORD, S827-845, S862-863 (11 Feb 2008).

[43] CONGRESSIONAL RECORD, S864-878 (11 Feb 2008).

12 Feb 2008 votes in Senate

Senate Amendment 3907, sponsored by Senators Dodd and Feingold, to strike from S.2248 retroactive immunity for telecoms, was defeated[44] by a vote of 67 to 31. Here is an alphabetical list of the courageous senators who voted to hold the telecoms responsible for their unlawful acts:[45]

Akaka (D-HI), **Yea**
Baucus (D-MT), **Yea**
Biden (D-DE), **Yea**
Bingaman (D-NM), **Yea**
Boxer (D-CA), **Yea**
Brown (D-OH), **Yea**
Byrd (D-WV), **Yea**
Cantwell (D-WA), **Yea**
Cardin (D-MD), **Yea**
Casey (D-PA), **Yea**
Dodd (D-CT), **Yea**
Dorgan (D-ND), **Yea**
Durbin (D-IL), **Yea**
Feingold (D-WI), **Yea**
Harkin (D-IA), **Yea**
Kennedy (D-MA), **Yea**
Kerry (D-MA), **Yea**
Klobuchar (D-MN), **Yea**
Lautenberg (D-NJ), **Yea**
Leahy (D-VT), **Yea**
Levin (D-MI), **Yea**
Menendez (D-NJ), **Yea**
Murray (D-WA), **Yea**
Obama (D-IL), **Yea**
Reed (D-RI), **Yea**
Reid (D-NV), **Yea**
Sanders (I-VT), **Yea**
Schumer (D-NY), **Yea**
Tester (D-MT), **Yea**

---

[44] Pamela Hess, "Senate OKs Immunity for Telecoms," Associated Press (12 Feb 2008, approx. 13:00 EST); William Branigin and Paul Kane, "Senate Protects Telecom Immunity in Spy Bill," *The Washington Post,* (12 Feb 2008 ,14:53 EST).

[45] Roll Call Vote Nr. 15 in U.S. Senate for year 2008. Copied from http://senate.gov/legislative/LIS/roll_call_lists/roll_call_vote_cfm.cfm?congress=110&session=2&vote=00015

Whitehouse (D-RI), **Yea**
Wyden (D-OR), **Yea**
All of the Republicans voted for immunity for telecoms. Hillary Clinton (D-NY) did not vote, her opponent in the presidential primary elections, Obama, voted against immunity. Diane Feinstein (D-CA), Kohl (D-WI), Landrieu (D-LA), Lieberman (I-CT), Mikulski (D-MD), Rockefeller (D-WV), Salazar (D-CO), and Stabenow (D-MI) were among prominent Democrats who voted for immunity. Altogether, 17 Democrats voted with the Republicans on granting retroactive immunity to telecoms.

After all eight amendments were rejected, the Senate then voted 69 to 29 for cloture, and then approved S.2248 by a vote of 68 to 29 on 12 Feb 2008. Neither Obama nor Clinton voted on the approval of S.2248.

13 Feb to 10 Mar 2008

13-14 Feb 2008

The issue of immunity for telecoms will be resolved by a conference committee composed of members of the House of Representatives and Senate. However, President Bush refused to approve a second extension of the expiration of the Protect America Act, which artificially forced the House and Senate to reach a consensus in three days or less, or to allow the Protect America Act to expire. *The Washington Post* reported on Wednesday morning, 13 Feb:

> The Senate's action, days before a temporary surveillance law expires Friday [15 Feb], sets up a clash with House Democrats, who have previously approved legislation that does not contain immunity for the telecommunications industry. The chambers have been locked in a standoff over the immunity provision since the House vote Nov. 15, with President Bush demanding the protection for the industry.
>
> White House spokesman Tony Fratto said the president "will not sign another extension" of the temporary law, a decision that could force congressional leaders to reconcile their differences this week.
>
> "The House is risking national security by delaying action," Fratto said. "It's increasingly clear Congress will not act until it has to, and a second extension will only lead to a third."
>
> But House leaders vowed again yesterday to oppose the telecom immunity provision until the White House releases more information about the controversial warrantless surveillance program it initiated shortly after the terrorist attacks.

Paul Kane, "Senate Authorizes Broad Expansion Of Surveillance Act," *The Washington Post,* http://www.washingtonpost.com/wp-dyn/content/article/2008/02/12/AR2008021201202_pf.html (13 Feb 2008).

Actually, the so-called 15 Feb deadline — when the Protect America Act expires — is contrived. If new legislation is not approved by Congress and the President before 16 Feb, existing surveillance orders from the FISA court continue to be valid for one year from the date of issue. In other words, the first surveillance orders issued under the Protect America Act will expire in August 2008, approximately six months from mid-February. Any new surveillance orders would need to be approved under the FISA statute in effect before the Protect America Act

was enacted. Therefore, any mention of surveillance stopping is not only false, but also purely hyperbole and propaganda.

On Tuesday, 12 Feb, the same day as the final votes on S.2248 in the U.S. Senate, the Chairman of the House Judiciary Committee issued a public statement saying that the secret documents provided by the White House did *not* justify retroactive immunity for telecoms. I have posted at http://www.rbs0.com/Conyers080212.pdf a copy of his six-page letter to the White House counsel. That letter must have really irked President Bush, given Bush's reaction in the next paragraph of this essay.

On Wednesday morning, 13 Feb, President Bush made the following statement from the Oval Office, with Director of National Intelligence, Mike McConnell at his side:

> Director, thank you for joining me. Good morning. At this moment, somewhere in the world, terrorists are planning new attacks on our country. Their goal is to bring destruction to our shores that will make September the 11th pale by comparison.[46] To carry out their plans, they must communicate with each other, they must recruit operatives, and they must share information.
>
> The lives of countless Americans depend on our ability to monitor these communications. Our intelligence professionals must be able to find out who the terrorists are talking to, what they are saying, and what they're planning.
>
> To help our intelligence agencies do this, Congress passed the Protect America Act last year. Unfortunately, Congress set the law to expire on February 1st — and then failed to pass new legislation that would keep these tools in effect over the long run. And so at the 11th hour, Congress passed a temporary 15-day extension of the current law which will expire at midnight this Saturday. I signed that extension. I did so to give members of the House and Senate more time to work out their differences.
>
> Well, the Senate has used this time wisely.[47] I am pleased that last night, Senators approved new legislation that will ensure our intelligence professionals have the tools they need to make us safer — and they did so by a wide, bipartisan majority. The Senate bill also provides fair and just liability protections for companies that did the right thing and assisted in defending America after the attacks of September the 11th.
>
> In order to be able to discover enemy — the enemy's plans, we need the cooperation of telecommunication companies. If these companies are subjected to lawsuits that could cost them billions of dollars, they won't participate; they won't help us; they won't help protect America.[48] Liability protection is critical to securing the private sector's cooperation with our

---

[46] This is pure propaganda, intended to scare Congress into enacting legislation. If the government really knows about terrorists, why doesn't the government arrest the suspected terrorists and try them in open court on conspiracy charges?

[47] No, the Senate did *not* use the time wisely. Not only did the Senate fail to approve a bill during the original six months, but they finally approved a bill just *three days* before a second deadline.

[48] Bush fails to mention that the telecom companies that cooperated with the government violated the statutory law and infringed constitutionally protected liberties of citizens of the USA. Now Bush demands retroactive immunity to protect these criminal telecom companies.

> intelligence efforts. The Senate has passed a good bill, and has shown that protecting our nation is not a partisan issue. And I congratulate the senators.
>
> Unfortunately, the House has failed to pass a good bill. And now House leaders say they want still more time to reach agreement with the Senate on a final bill. They make this claim even though it is clear that the Senate bill, the bill passed last night, has significant bipartisan support in the House.
>
> Congress has had over six months to discuss and deliberate. The time for debate is over. I will not accept any temporary extension. House members have had plenty of time to pass a good bill. They have already been given a two-week extension beyond the deadline they set for themselves. If Republicans and Democrats in the Senate can come together on a good piece of legislation, there is no reason why Republicans and Democrats in the House cannot pass the Senate bill immediately.[49]
>
> The House's failure to pass the bipartisan Senate bill would jeopardize the security of our citizens. As Director McConnell has told me, without this law, our ability to prevent new attacks will be weakened. And it will become harder for us to uncover terrorist plots. We must not allow this to happen. It is time for Congress to ensure the flow of vital intelligence is not disrupted. It is time for Congress to pass a law that provides a long-term foundation to protect our country. And they must do so immediately.
>
> Thank you very much.

President Bush, "President Bush Discusses Protect America Act," http://www.whitehouse.gov/news/releases/2008/02/20080213.html (13 Feb 2008 09:01 EST).

Commentators suggested that President Bush demanded the retroactive immunity for telecoms, *not only* to protect the telecoms from burdensomely expensive judgments, but also to prevent courts from publicly exposing Bush's illegal (and still secret) Terrorist Surveillance Program.[50]

On Wednesday afternoon, 13 Feb, the House rejected, by a vote of 229 to 191, to extend the Protect America Act for 21 days. *The Washington Post* said:

> The House and Senate versions of the new FISA provisions differ slightly, but leaders on both sides acknowledged that the major stumbling block is immunity for the telecommunications industry, which faces dozens of lawsuits for providing personal information to intelligence agencies without warrants.

Paul Kane, "House Rejects Extension of Surveillance Act," *The Washington Post,* http://www.washingtonpost.com/wp-dyn/content/article/2008/02/13/AR2008021300959.html (13 Feb 2008, 17:25 EST).

---

[49] Well, one reason is that the Senate bill contains retroactive immunity for unlawful wiretapping by telecoms, which immunity subverts the rule of law and denies justice to grieved citizens whose privacy was violated.

[50] See my separate essay on the Terrorist Surveillance Program at http://www.rbs0.com/TSP.pdf .

At 13:00 EST on Thursday, 14 Feb, the President gave a ten-minute public speech on the South Lawn of the White House about the surveillance legislation:

> Good afternoon. This Saturday at midnight, legislation authorizing intelligence professionals to quickly and effectively monitor terrorist communications will expire. If Congress does not act by that time, our ability to find out who the terrorists are talking to, what they are saying, and what they are planning will be compromised. It would be a mistake if the Congress were to allow this to happen.
>
> Members of Congress knew all along that this deadline was approaching. They said it themselves. They've had more than six months to discuss and deliberate. And now they must act, and pass legislation that will ensure our intelligence professionals have the tools they need to keep us safe.
>
> Earlier this week the Senate did act, and passed a strong bill, and did so with a bipartisan majority. The Senate bill will ensure that we can effectively monitor those seeking to harm our people. The Senate bill will provide fair and just liability protection for companies that assisted in the efforts to protect America after the attacks of September the 11th.[51] Without this protection, without this liability shield, we may not be able to secure the private sector's cooperation with our intelligence efforts. And that, of course, would put the American people at risk.
>
> Now it's the House's turn to act. It is clear that the Senate bill would pass the House with bipartisan support. Republicans and Democrats in the Senate can put partisanship aside, and pass a good bill. There's no reason why the House cannot do the same, and pass the Senate bill immediately.
>
> Our government has no greater responsibility than getting this work done, and there really is no excuse for letting this critical legislation expire. I urge congressional leaders to let the will of the House and the American people prevail,[52] and vote on the Senate bill before adjourning for their recess. Failure to act would harm our ability to monitor new terrorist activities, and could reopen dangerous gaps in our intelligence. Failure to act would also make the private sector less willing to help us protect the country, and this is unacceptable. The House should not leave Washington without passing the Senate bill.
>
> I am scheduled to leave tomorrow for a long-planned trip to five African nations. Moments ago, my staff informed the House leadership that I'm prepared to delay my departure, and stay in Washington with them, if it will help them complete their work on this critical bill.

---

[51] What about the American citizens who were illegally wiretapped during 2001-2006? Where is the fairness and justice for them? What about prosecuting government officials who approved or supervised illegal wiretaps during the Terrorist Surveillance Program?

[52] Who knows what the will of the American people is? If one asked them, “Do you favor wiretapping of evil terrorists who are planning to murder thousands of Americans?”, the American people would probably say yes. But if one asked them, “Do you favor allowing some low-level government bureaucrat to wiretap communications of innocent Americans, without a court order and in violation of Constitutional privacy rights?”, the American people would probably say no. And if one asked American people, “Do you believe that giant telephone companies should be able to illegally wiretap American citiizens — violate Constitutional privacy rights of individual American citizens — and then have Congress give the telephone companies immunity from lawsuits by victimized individuals?”, I hope people would say no.

The lives of countless Americans depend on our ability to monitor terrorist communications. Our intelligence professionals are working day and night to keep us safe, and they're waiting to see whether Congress will give them the tools they need to succeed or tie their hands by failing to act. The American people are watching this debate, as well.[53] They expect Congress to meet its responsibilities before they leave town on a recess.

I'll answer a few questions. Ben, if you've got a question, I'll be prepared to answer.

Question: Thank you, Mr. President. It appears with that deadline approaching, that the House and the White House might be seen as being engaged in a game of chicken here, playing politics with an important intelligence law. If the law expires, and something happens, wouldn't you be at least partly to blame? And on your Africa trip, if you have to delay, do you think that you would be shortening your trip at all?

THE PRESIDENT:

As to the latter, the delay depends on whether the House acts, of course, and they got plenty of time to get this done. But if we have to delay, we'll delay. But I'm going to go to the countries that I said I'd go to.

And to the first case, whether or not this is politics, I certainly hope not. I can assure you al Qaeda in their planning isn't thinking about politics. They're thinking about hurting the American people again.

Who's to blame? Look, these folks in Congress passed a good bill last — late last summer. In other words, they analyzed the situation, they said there's a threat, and they agreed to give our professionals the tools they needed to do the job. The problem is they let the bill expire.

My attitude is, if the bill was good enough then, why not pass the bill again? I mean, the threat hasn't gone away. Secondly, they've had plenty of time to think about how to address the issue. Thirdly, the Senate led the way; the Senate showed how to pass a good bill, with a bipartisan majority. And the truth of the matter is, if there was a willingness to get this problem solved, all the leadership would have to do is submit the Senate bill for a vote.

So we'll see what happens. My attitude is, now is the time to get the job done. There's been plenty of time to think about it, plenty of time to debate it, and there's a good way forward. And hopefully the House leadership will put this bill for a vote and let the members vote as they so desire.

Mike.

Question: Mr. President, I realize this is a sensitive matter, but I'm wondering if there's a way you can spell out for the American public what the practical impact may be, if this law expires, on our intelligence professionals, say, next week.

THE PRESIDENT:

Well, I hope it doesn't. But clearly, there will be a gap. And of course, we won't be able to assess that gap until the time. Step one is, I guess you got to come to the conclusion that there's a threat to America, or not a threat. And evidently some people just don't feel that sense of urgency. I do. And the reason I do is I firmly believe that there's still people out there who would do us harm.

---

[53] The American people are probably not understanding this debate, given the sporatic coverage and superficial reporting by journalists.

Secondly, I know that the tools that I've just described are necessary to protect us. Why? Because we need to know what people are saying, what they're planning and what they're thinking. And the tool that I have just described has been very effective.

Thirdly, people are wondering why companies need liability protection. Well, if you cooperate with the government and then get sued for billions of dollars because of the cooperation, you're less likely to cooperate.[54] And obviously we're going to need people working with us to find out what the enemy is saying and thinking and plotting and planning.[55]

And so it's a — to me it's a — I guess one way to look at it is, some may not feel that same sense of urgency I do. I heard somebody say, well, this is just pure politics. No, this is what is necessary to protect the American people from harm.[56] And I recognize there hasn't been an attack on our country, but that does not mean that there's not still an enemy that lurks, plans and plots.

And one of the reason we've been effective is because we put new tools in place that give our professionals that which is necessary to protect us. This is a different kind of threat than we've ever faced before, it's a different kind of war that we're fighting, and it requires a different approach.

Again, I'll repeat to you that the Congress took a look at this issue and decided that the tools were necessary to give to our professionals last — late last summer. And if it was necessary late last summer, why is it not necessary today? What has changed? Well, the threat hasn't gone away. It's still there, it's still real, and we better be worried about it as a nation. And the House has now got time to go out and get the deal done.

Yesterday — a couple of days — votes ago in the Senate made it abundantly clear that Republicans and Democrats can come together and put a good piece of legislation together and get it passed. And the House leadership has an opportunity to do that now.

Listen, thank you all very much.

President Bush, "President Bush Discusses Protect America Act," (14 Feb 2008, 13:00 EST) http://www.whitehouse.gov/news/releases/2008/02/20080214-1.html

Later on Thursday, 14 Feb, President Bush released a written statement about the surveillance law:

Democratic leaders said today that if the Protect America Act expires, there will be no impact on our intelligence gathering capabilities, and no cost to our national security. They are wrong.

Although PAA authorizations permitting *current* intelligence activities will not immediately expire with expiration of the Act, Senator Reid is wrong and irresponsibly misleading to say that we will be just as safe if the PAA expires as we are with the PAA in effect. The House's willingness to permit the PAA to expire without passing the bipartisan

---

[54] The telecoms were *not* sued because they cooperated with the government. The telecoms were sued because they violated the statutory law in the USA that protects citizens from wiretapping without a court order.

[55] The end does *not* justify the means. Just because we need intelligence does not mean government can trample on U.S. citizens' constitutional rights of privacy for telephone calls and e-mails.

[56] There is also a need to protect America from an overzealous government who wants wiretaps of citizens without a court order.

> Senate bill will harm our ability to conduct surveillance to detect new threats to our security, including the locations, intentions, and capabilities of terrorists and other foreign intelligence targets abroad. The Attorney General and the Director of National Intelligence would be stripped of the power to authorize new certifications against foreign intelligence targets, including international terrorists, abroad. And they could be stripped of their power to compel the assistance of a private company not already helping us. This means that surveilling new terrorist threats will require the Intelligence Community to go back to the old pre-PAA process of seeking court approvals that created the dangerous intelligence gap that we temporarily closed with passage of the PAA last August. The Intelligence Community will be stuck with the authorities it currently has and would be hampered in its ability to protect us from new terrorist threats that emerge. This risks creating new intelligence gaps, which damages our national security and makes no sense if the first priority is making sure our citizens are safe.
>
> The House's failure to act will also raise risks with respect to current intelligence activities. This is because the PAA provides liability protection for our private sector partners assisting in current activities, but those partners are likely to raise questions about whether the liability protection they currently enjoy expires with the PAA. Similar questions could arise regarding whether the PAA's provisions authorizing courts to compel cooperation by the private sector also expire with the Act. At a minimum, the private sector would become less willing to help our efforts to defend the country because of this uncertainty; at worst, they would cease helping us at all.[57] And if we don't have their cooperation, we don't have a program.
>
> The terrorist threats to our nation are very real and grave, and inaction by the House in the face of these risks is unacceptable.
>
> Democrat leaders know that if they put the Senate bill on the House floor today, it would pass with bipartisan support. Make no mistake — letting the PAA expire without replacing it with the bipartisan Senate bill results in greater risk to our national security, and it is irresponsible and false for Democrats to suggest otherwise.
>
> ....

President Bush, "Statement on Protect America Act" (14 Feb 2008)
http://www.whitehouse.gov/news/releases/2008/02/20080214-4.html

Calling Democrats who oppose retroactive immunity for telecoms "irresponsible" is not likely to advance a bipartisan consensus. If the Protect America Act is *really* essential for national security, then Bush should have agreed to extend it, rather than let it expire.

---

[57] Bush's assertion is ridiculous. If the telecoms do not cooperate with the government in surveillance ordered by the FISA court, the government could ask the FISA court to compel the telecoms to cooperate.

On Thursday, 14 Feb 2008, the House of Representatives voted 223 to 32 to hold presidential chief of staff Josh Bolten and former White House counsel Harriet Miers in contempt[58] for failure to supply documents about the alleged partisan firings of U.S. Attorneys in Dec 2006. The vote was lopsided because angry Republicans walked out prior to the vote. This development is irrelevant to the discussion of surveillance and retroactive immunity for telecoms, but it set the stage for what happened next.

conference committee appointed

President Bush demanded that the House of Representatives pass S.2248, so that he could sign the bill and avoid the expiration of the Protect America Act. Instead, the Speaker of the House — Nancy Pelosi (D-CA) — "instructed the chairmen of the House intelligence and judiciary committees to meet with their Senate counterparts by Friday to start reconciling the House and Senate eavesdropping legislation — something she predicted could be done within 21 days."[59] It is important to recognize that such conference committees are the *usual* way to reconcile differences between bills passed by the House and Senate. After instructing the conference committee to meet, the House took a ten-day recess, to meet again on Monday, 25 Feb 2008.

Bush's Weekly Radio Address, 16 Feb

Director of National Intelligence Mike McConnell began saying that, without immunity, the telecom companies would refuse to cooperate with the government in surveillance of suspected terrorists.[60] Such a statement is false. The government is always able to get an order from the FISA court to compel the telecoms to implement any surveillance order issued by that court. It is distressing to see senior government officials misrepresent the law to the American people, in order to mislead people into supporting the government's desired legislation.

President Bush departed on Friday afternoon, 15 Feb, for a six-day tour of Africa. Given the President's public pronouncements of imminent terrorist attacks on the USA if the Protect America Act expired, it was not only inconsistent but also irresponsible for Bush to depart on a routine trip to foreign countries during a time that Bush alleges that the USA faces an imminent

---

[58] Julie Davis, "House Holds Bush Confidants in Contempt," Associated Press (14 Feb 2008, 15:24 EST).

[59] Deb Riechmann, "Bush Criticizes Congress on Terror Bill," Associated Press (15 Feb 2008, 03:11 EST).

[60] Pamela Hess, "Bush, Congress in Spy Bill Standoff," Associated Press (15 Feb 2008, 05:39 EST).

threat. I think the fact that Bush departed as scheduled on a routine six-day trip shows that Bush did not believe his own propaganda about the expiration of the Protect America Act.

Bush's recorded Saturday morning radio address said the following about the surveillance legislation:

> Good morning. At the stroke of midnight tonight, a vital intelligence law that is helping protect our nation will expire. Congress had the power to prevent this from happening, but chose not to.[61]
>
> The Senate passed a good bill that would have given our intelligence professionals the tools they need to keep us safe. But leaders in the House of Representatives blocked a House vote on the Senate bill, and then left on a 10-day recess.
>
> Some congressional leaders claim that this will not affect our security. They are wrong. Because Congress failed to act, it will be harder for our government to keep you safe from terrorist attack. At midnight, the Attorney General and the Director of National Intelligence will be stripped of their power to authorize new surveillance against terrorist threats abroad.[62] This means that as terrorists change their tactics to avoid our surveillance, we may not have the tools we need to continue tracking them — and we may lose a vital lead that could prevent an attack on America.
>
> In addition, Congress has put intelligence activities at risk even when the terrorists don't change tactics. By failing to act, Congress has created a question about whether private sector companies who assist in our efforts to defend you from the terrorists could be sued for doing the right thing. Now, these companies will be increasingly reluctant to provide this vital cooperation, because of their uncertainty about the law and fear of being sued by class-action trial lawyers.
>
> For six months, I urged Congress to take action to ensure this dangerous situation did not come to pass. I even signed a two-week extension of the existing law, because members of Congress said they would use that time to work out their differences. The Senate used this time productively[63] — and passed a good bill with a strong, bipartisan super-majority of 68 votes. Republicans and Democrats came together on legislation to ensure that we could effectively monitor those seeking to harm our people. And they voted to provide fair and just liability protection for companies that assisted in efforts to protect America after the attacks of 9/11.
>
> The Senate sent this bill to the House for its approval. It was clear that if given a vote, the bill would have passed the House with a bipartisan majority. I made every effort to work with the House to secure passage of this law. I even offered to delay my trip to Africa if we could come together and enact a good bill. But House leaders refused to let the bill come to a vote. Instead, the House held partisan votes that do nothing to keep our country safer. House

---

[61] Actually, Bush — and Republicans in the House of Representatives — refused to allow a 21-day extension of the deadline in the Protect America Act. The expiration of the Protect America Act is an artificial crisis created by Republicans.

[62] Instead, the government will actually need to follow Fourth Amendment protections in the U.S. Constitution, and get a judicial order before the government can legally wiretap.

[63] Bush said this before, on 13 Feb. No, the Senate did *not* use the time wisely. Not only did the Senate fail to approve a bill during the original six months, but they finally approved a bill just *three days* before a second deadline.

leaders chose politics over protecting the country — and our country is at greater risk as a result.

House leaders have no excuse for this failure. They knew all along that this deadline was approaching, because they set it themselves. My administration will take every step within our power to minimize the damage caused by the House's irresponsible behavior. Yet it is still urgent that Congress act. The Senate has shown the way by approving a good, bipartisan bill. The House must pass that bill as soon as they return to Washington from their latest recess.

At this moment, somewhere in the world, terrorists are planning a new attack on America. And Congress has no higher responsibility than ensuring we have the tools to stop them.

Thank you for listening.

President Bush, Weekly Radio Address, 16 Feb 2008
http://www.whitehouse.gov/news/releases/2008/02/20080216.html

This kind of inflammatory rhetoric can give children nightmares and does nothing to reach a rational consensus.

Democrat's Response to Bush, 16 Feb 2008

The Democrats were swift to react to Bush's address — the Speaker of the House and the Senate Majority Leader issued the following joint statement:

The Protect America Act will expire only because the President and congressional Republicans refused to approve an extension of that law. Their true concern here is not national security. Rather, they want to protect the financial interests of telecommunications companies and avoid judicial scrutiny of their warrantless wiretapping program.

Congressional Democrats will continue to work on a bipartisan basis to finalize a strong law. As we do, there should be no question in anyone's mind that U.S. intelligence agencies have the legal ability to take all actions necessary to protect the security of the American people. For anyone to suggest otherwise is irresponsible and totally inaccurate.

In particular, the law protects telecommunication carriers, and we will ensure that no lawfully cooperating carrier is disadvantaged by the President's decision to block a brief extension of the Protect America Act.

Nancy Pelosi and Harry Reid, "Joint Statement on FISA" (16 Feb 2008, 15:49 EST)
http://www.speaker.gov/blog/?p=1145

Senator Sheldon Whitehouse (D-RI), the co-author of some Senate amendments to S.2248, gave the Democrat's response to the President's Weekly Radio Address:

Hello, I'm Sen. Sheldon Whitehouse, Democrat from Rhode Island. I'm a former U.S. attorney and Rhode Island attorney general, and I serve on the Senate Intelligence and Judiciary Committees.

This week, instead of working with Congress in a calm, constructive way, the president, unfortunately, has chosen to manufacture a sudden and unnecessary confrontation over reauthorization of our foreign surveillance laws. We Democrats urge the president to work with Congress to provide our intelligence professionals needed authorities while protecting the privacy of law-abiding Americans.

Both the House and the Senate worked hard to pass bills to improve the Protect America Act, an ill-advised law Congress passed in a stampede last August. These bills strengthen the Protect America Act: For example, both, for the first time, protect Americans from being wiretapped without a court order outside the United States.

But the House and Senate bills are not identical, and in the American legislative process, the next step is a negotiation to resolve differences between the two bills. And Democrats stand ready to do that now. That is how our system has always worked. But the president doesn't want the legislative process to work — instead, he has made an unrealistic demand that the House simply adopt the Senate version, and at his request congressional Republicans are preventing negotiations from moving forward.

America's bicameral system of government is designed to bring broad, bipartisan consensus to important laws. We're at the finish line. Letting the House and the Senate complete the process would strengthen support in Congress and among the American people and give the intelligence community greater legal certainty for surveillance activities.

Negotiation should take place immediately. In the meantime, Democrats are willing to extend the current Protect America Act. But the president has threatened to veto any extension, and Senate Republicans have blocked such a bill. Every House Republican voted against extension of the law.

We know this president dislikes compromise, but this time he has taken his stubborn approach too far. He is whipping up false fears and creating artificial confrontation. As the president, himself, said in the Rose Garden, there is really no excuse for letting this critical legislation expire. So let's get it done.

But the president instead chose political gamesmanship, rejecting a short extension of the Protect America Act that would allow Congress to complete its work. Make no mistake: If the surveillance law expires, if any intelligence loss results, it is President Bush's choice. Period.

Fortunately, the president's decision to allow the Protect America Act to expire does not, in reality, threaten the safety of Americans. As the president is well-aware, existing surveillance orders under that law remain in effect for a year, and the 1978 FISA law remains available for new surveillance orders.

I urge the president to come to his senses. Democrats have taken significant and important steps to strengthen the laws governing surveillance and to make sure that privacy protections for Americans aren't left in the dust. The president should work with us to enshrine these new protections in the law of the land. He should also sign into law the torture ban passed by both houses of Congress that would make crystal clear that America condemns torture and will not stoop to the techniques of the Spanish Inquisition.

Our values, and our American process of government, are what make America strong.

Sheldon Whitehouse, "Democratic Radio Address," (16 Feb 2008)
http://www.foxnews.com/story/0,2933,330904,00.html
http://www.democrats.org/a/2008/02/senator_sheldon.php

After Bush's wailing about a strong bipartisan majority in the U.S. Senate in support of retroactive immunity for telecoms, it is interesting to note that a conference committee composed of the chairmen of the judiciary and intelligence committees in both the House and Senate would have only 1 vote in 4 for retroactive immunity. John Conyers (D-Mich.) and Patrick Leahy (D-VT), chairmen of the House and Senate Judiciary Committees, both oppose retroactive immunity for telecoms. Silvestre Reyes (D-TX), chairman of the House Intelligence Committee, also opposes retroactive immunity.

Bush on 21 Feb

On 21 Feb 2008, President Bush spoke to journalists aboard Air Force One, as the airplane was returning from his trip to Africa. The Associated Press reported:

> President Bush on Thursday [21 Feb] stood by his demand for legal protection for phone companies that help the government eavesdrop on suspected terrorists, saying he sees no prospect of a compromise with congressional Democrats.
>
> ....
>
> Asked about a potential deal with Democrats, Bush said, "I would just tell you there's no compromise on whether these phone companies get liability protection." The administration says it needs the help of the phone companies for its post-Sept. 11, 2001, surveillance.
>
> Bush said his strategy for breaking the deadlock on the surveillance bill will be to keep talking about why it should be passed on his terms. "The American people understand we need to be listening to the enemy," he said.
>
> ....
>
> Democratic staff members from the House and Senate Intelligence and Judiciary committees were meeting informally this week to work on compromise language, the committees said. Republicans are not attending the meetings because they want the Senate version of the bill, which passed 68-29, and believe that any changes to the Senate bill would make it unacceptable to the White House.

Ben Feller, "Bush: Surveillance Compromise Unlikely," Associated Press (21 Feb 2008 19:52 EST)

It is stupid for President Bush to be intransigent and absolutely refuse to compromise. The Democratic party leadership in the House of Representatives could refuse to vote on any surveillance legislation, thus creating a stalemate. Bush would look weak and defeated if he eventually accepts no retroactive immunity for telecoms, given his many public statements demanding immunity.

Bush's Weekly Radio Address, 23 Feb

Bush's recorded Saturday morning radio address said the following about the surveillance legislation:

> Members of Congress will soon be returning to Washington, as well, and they have urgent business to attend to. They left town on a 10-day recess without passing vital legislation giving our intelligence professionals the tools they need to quickly and effectively monitor foreign terrorist communications. Congress' failure to pass this legislation was irresponsible. It will leave our Nation increasingly vulnerable to attack. And Congress must fix this damage to our national security immediately.

The way ahead is clear. The Senate has already passed a good bill by an overwhelming bipartisan majority. This bill has strong bipartisan support in the House of Representatives, and would pass if given an up or down vote. But House leaders are blocking this legislation, and the reason can be summed up in three words: class action lawsuits.

The Senate bill would prevent plaintiffs' attorneys[64] from suing companies believed to have helped defend America after the 9/11 attacks. More than 40 of these lawsuits have been filed, seeking hundreds of billions of dollars in damages from these companies. It is unfair and unjust to threaten these companies with financial ruin only because they are believed to have done the right thing and helped their country.[65]

But the highest cost of all is to our national security. Without protection from lawsuits, private companies will be increasingly unwilling to take the risk of helping us with vital intelligence activities. After the Congress failed to act last week, one telecommunications company executive was asked by the *Wall Street Journal* how his company would respond to a request for help. He answered that because of the threat of lawsuits, quote, "I'm not doing it ... I'm not going to do something voluntarily." In other words, the House's refusal to act is undermining our ability to get cooperation from private companies. And that undermines our efforts to protect us from terrorist attack.

Director of National Intelligence Mike McConnell recently explained that the vast majority of the communications infrastructure we rely on in the United States is owned and operated by the private sector. Because of the failure to provide liability protection, he says private companies who have "willingly helped us in the past, are now saying, 'You can't protect me. Why should I help you?'" Senator Jay Rockefeller, the Democratic Chairman of the Senate Intelligence Committee, puts it this way: "The fact is, if we lose cooperation from these or other private companies, our national security will suffer."

When Congress reconvenes on Monday, Members of the House have a choice to make: They can empower the trial bar[66] — or they can empower the intelligence community. They can help class action trial lawyers[67] sue for billions of dollars — or they can help our intelligence officials protect millions of lives. They can put our national security in the hands of plaintiffs' lawyers[68] — or they can entrust it to the men and women of our government who work day and night to keep us safe. As they make their choice, Members of Congress must never forget: Somewhere in the world, at this very moment, terrorists are planning the next attack on America. And to protect America from such attacks, we must protect our telecommunications companies from abusive lawsuits.

---

64 This is a propaganda tactic to attack “plaintiffs’ attorneys” who are following the law and trying to get justice for their clients who were illegally wiretapped.

65 These telecoms are megacorporations who employ many lawyers to tell them that wiretapping without a court order is illegal. These megacorporations do not deserve to protected. Where is Bush’s sympathy for individual people whose constitutional rights to privacy were violated by overzealous government and cooperative megacorporations?

66 More propaganda against the “trial bar”.

67 More propaganda against “class-action trial lawyers”. Note that the “intelligence community” and “intelligence officials” violated statutory law in the USA by illegally wiretapping people, hardly the type of government program that people should endorse.

68 Three consecutive sentences of pure propaganda!

> Thank you for listening.

President Bush, Weekly Radio Address, 23 Feb 2008
http://www.whitehouse.gov/news/releases/2008/02/20080223.html

It is important to remember that the so-called "trial lawyers" (who are mostly nonprofit organizations such as the American Civil Liberties Union and the Electronic Frontier Foundation) are insisting that telecoms pay damages to people whose constitutional right of privacy was violated, as a way of holding telecoms accountable for their unlawful acts. These lawyers are upholding the rule of law, and protecting individual people from an overzealous government and megacorporations like telecoms. On the other hand, Bush continues to assert that security is the only thing that matters, and that more surveillance will somehow make us more secure.

President Bush repeated his diatribe against trial lawyers at a press conference on 28 Feb:

> And now, all of a sudden, plaintiffs attorneys, class-action plaintiffs attorneys, you know — I don't want to try to get inside their head; I suspect they see, you know, a financial gravy train — are trying to sue these companies. First, it's unfair. It is patently unfair. And secondly, these lawsuits create doubts amongst those who will — whose help we need.

President Bush, press conference 28 Feb 2008 10:05 EST
http://www.whitehouse.gov/news/releases/2008/02/20080228-2.html

Despite what Bush said, his Terrorist Surveillance Program was illegal. It is *not* unfair to hold telecoms accountable for violating federal statutes. And the plaintiffs' attorneys are *not* motivated by money, they are staff attorneys at nonprofit organizations.

alleged "lost information"

On Friday, 22 Feb, the Bush administration alleged that the government had lost intelligence information, because telecom companies were no longer cooperating with the government. However, the following day, the Bush administration backed away from its allegation.
The Washington Post reported:

> The Bush administration said yesterday [22 Feb] that the government "lost intelligence information" because House Democrats allowed a surveillance law to expire last week, causing some telecommunications companies to refuse to cooperate with terrorism-related wiretapping orders.
>
> But hours later, administration officials told lawmakers that the final holdout among the companies had relented and agreed to fully participate in the surveillance program, according to an official familiar with the issue.
>
> ....
>
> The standoff has led to almost daily attacks from the White House and GOP lawmakers, who accuse Democrats of endangering national security to appease civil-liberties advocates and other liberal groups.
>
> Director of National Intelligence Mike McConnell and Attorney General Michael B. Mukasey said in a letter sent yesterday afternoon to Capitol Hill that the companies were refusing to cooperate because they were uncertain about what legal liability they might face.

"We have lost intelligence information this past week as a direct result of the uncertainty created by Congress' failure to act," McConnell and Mukasey wrote to Rep. Silvestre Reyes (D-Tex.), chairman of the House intelligence committee. "Because of this uncertainty, some partners have reduced cooperation."

The two officials noted that some companies have "delayed or refused compliance" with requests to add surveillance targets to general orders that were approved before the law expired. They did not provide further details.

Reyes and other Democrats have countered by accusing Republicans of fear-mongering, noting that long-standing surveillance laws remain in effect and that all surveillance under the expired law is authorized until at least August.

Reyes and three other Democrats — Sens. John D. Rockefeller IV (W.Va.) and Patrick J. Leahy (Vt.) and Rep. John Conyers Jr. (Mich.) — said in a joint response that Republicans are "politicizing the debate" and have refused to participate in negotiations over the legislation.

....

Dan Eggen and Ellen Nakashima, "Spy Law Lapse Blamed for Lost Information Some Telecom Firms Not Cooperating for Fear of Liability, U.S. Says," *The Washington Post,* p. A03 (23 Feb 2008) http://www.washingtonpost.com/wp-dyn/content/article/2008/02/22/AR2008022202859.html

On Monday, 25 Feb, *The Washington Post* published a letter by the four leading Democrats in the conference committee:

Nothing is more important to the American people than our safety and our freedom. As the chairmen of the House and Senate intelligence and judiciary committees, we have an enormous responsibility to protect both.

Unfortunately, instead of working with Congress to achieve the best policies to keep our country safe, once again President Bush has resorted to scare tactics and political games.

In November, the House passed legislation to give U.S. intelligence agencies strong tools to intercept terrorist communications that transit the United States, while ensuring that Americans' private communications are not swept up by the government in violation of the Fourth Amendment.

Almost two weeks ago, the Senate passed similar legislation. The Senate bill also contains a provision to grant retroactive legal immunity to telecommunications companies that assisted the executive branch in conducting surveillance programs after the Sept. 11, 2001, attacks.

While the four of us may have our differences on what language a final bill should contain, we agree on several points.

First, our country did not "go dark" on Feb. 16 when the Protect America Act (PAA) expired. Despite President Bush's overheated rhetoric on this issue, the government's orders under that act will last until at least August. These orders could cover every known terrorist group and foreign target. No surveillance stopped. If a new member of a known group, a new phone number or a new e-mail address is identified, U.S. intelligence can add it to the existing orders, and surveillance can begin immediately.

As Assistant Attorney General Kenneth Wainstein acknowledged while speaking to reporters on Feb. 14, "the directives are in force for a year, and with the expiration of the PAA, the directives that are in force remain in force until the end of that year. . . . [W]e'll be able to continue doing surveillance based on those directives."

If President Bush truly believed that the expiration of the Protect America Act caused a danger, he would not have refused our offer of an extension.

> In the remote possibility that a terrorist organization that we have never previously identified emerges, the National Security Agency could use existing authority under the Foreign Intelligence Surveillance Act (FISA) to track its communications. Since Congress passed FISA in 1978, the court governing the law's use has approved nearly 23,000 warrant applications and rejected only five. In an emergency, the NSA or FBI can begin surveillance immediately and a FISA court order does not have to be obtained for three days.
>
> When U.S. agencies provided critical intelligence to our German allies to disrupt a terrorist plot last summer, we relied on FISA authorities.
>
> Those who say that FISA is outdated do not appreciate the strength of this powerful tool.
>
> So what's behind the president's "sky is falling" rhetoric?
>
> It is clear that he and his Republican allies, desperate to distract attention from the economy and other policy failures, are trying to use this issue to scare the American people into believing that congressional Democrats have left America vulnerable to terrorist attack.
>
> But if our nation were to suddenly become vulnerable, it would not be because we don't have sufficient domestic surveillance powers. It would be because the Bush administration has done too little to defeat al-Qaeda, which has reconstituted itself in Pakistan and gained strength throughout the world. Many of our intelligence assets are being used to fight in Iraq instead of taking on Osama bin Laden and the al-Qaeda organization that attacked us on Sept. 11 and that wants to attack us again.
>
> The president may try to change the topic by talking about surveillance laws, but we aren't buying it.
>
> We are motivated to pass legislation governing surveillance because we believe this activity must be carefully regulated to protect Americans' constitutional rights. Companies that provide lawful assistance to the government in surveillance activities should be legally protected for doing so.
>
> We are already working to reconcile the House and Senate bills and hope that our Republican colleagues will join us in the coming weeks to craft final, bipartisan legislation. A key objective of our effort is to build support for a law that gives our intelligence professionals not only the tools they need but also confidence that the legislation they will be implementing has the broad support of Congress and the American public.
>
> If the president thinks he can use this as a wedge issue to divide Democrats, he is wrong. We are united in our determination to produce responsible legislation that will protect America and protect our Constitution.

Jay Rockefeller, Patrick Leahy, Silvestre Reyes and John Conyers, "Scare Tactics and Our Surveillance Bill," *The Washington Post,* p. A15 (25 Feb 2008)
http://www.washingtonpost.com/wp-dyn/content/article/2008/02/24/AR2008022401668.html
Note that Senator Rockefeller, who supported retroactive immunity for illegal wiretapping by telecoms, joins his three colleagues who oppose retroactive immunity for telecoms.

The Associated Press reported President Bush's response:

> President Bush on Monday [25 Feb] lobbied again for an intelligence law allowing government eavesdropping on phone calls and e-mails, as the tone of the dispute between the White House and Congress over terrorist surveillance grew increasingly sharp.
>
> "To put it bluntly, if the enemy is calling into America, we really need to know what they're saying, and we need to know what they're thinking, and we need to know who they're talking to," Bush said at the start of his annual meeting with the nation's governors at the White House.

> "This is a different kind of struggle than we've ever faced before. It's essential that we understand the mentality of these killers," Bush said.
>
> ....
>
> The president's pitch was the latest installment in a long and increasingly sharply-worded debate between Bush and congressional Democrats.

Ben Feller, "Bush Lobbies Again for Surveillance Law," Associated Press (25 Feb 2008 17:46 EST).

Note that Bush mischaracterized the debate: no one is opposing interception of enemy communications. The debate is about whether to give telecoms retroactive immunity for illegal wiretaps of American citizens.

The Associated Press wrote a "fact check" article in response to President Bush's claims at a press conference on 28 Feb 2008:

> **BUSH:** Lawmakers should act "to pass legislation our intelligence officials need to quickly — quickly and effectively monitor terrorist communications."
> **THE FACTS:** Both the House and Senate have passed surveillance legislation. The House finished its bill in October; the Senate this month. The Senate's provides telecommunications companies full legal immunity from civil suits for their alleged involvement in the wiretapping program between Sept. 11, 2001, and January 2007. The House is silent on the matter of legal protection.
>
> The companies allegedly placed wiretaps inside the United States and aimed at suspected terrorists, at the request of either the president, the attorney general or their designees for nearly six years without the knowledge or permission of a special court, the Foreign Intelligence Surveillance Court. The White House brought the Terrorist Surveillance Program under that court in January 2007. The program's existence was revealed in December 2005 by *The New York Times.*
>
> **BUSH:** "Allowing these lawsuits to proceed would be unfair. If any of these companies helped us, they did so after being told by our government that their assistance was legal and vital to our national security."
> **THE FACTS:** House Democrats agree the suits could be considered unfair, but only if the companies believed what they were doing was legal and necessary in the wake of Sept. 11. To verify that, the Democrats say they need to see secret documents underpinning the program. The White House has only allowed the House Intelligence and Judiciary committees to see the documents, limiting distribution because of the documents' sensitivity.
>
> But some lawmakers, including Sen. Ted Kennedy, D-Mass., say that not allowing the suits to go forward would be unfair to people on whom the government may have eavesdropped illegally. "If they broke the law, the American people deserve to know the size and scope of their lawbreaking," he said Thursday.
>
> **BUSH:** "Allowing the lawsuits to proceed could aid our enemies because the litigation process could lead to the disclosure of information about how we conduct surveillance and it would give al-Qaida and others a road map as to how to avoid the surveillance."

THE FACTS: About 40 suits have been filed in U.S. courts against telecommunications companies. Intelligence officials are concerned that a trial may expose records detailing how, when and against whom the wiretaps were carried out. That could cause terrorists to take more steps to cover their tracks.

Democrats say the courts have a proven record of being able to keep information secret. Sometimes domestic criminal cases use evidence gathered by the government under FISA wiretaps. The government must inform defendants of the wiretaps and what information was gathered. Democrats say that in none of those cases has that disclosure revealed sources or methods.

BUSH: "Allowing these lawsuits to proceed could make it harder to track the terrorists because private companies besieged by and fearful of lawsuits would be less willing to help us quickly get the information we need. Without the cooperation of the private sector, we cannot protect our country from terrorist attack."

THE FACTS: Companies cannot refuse to conduct a wiretap if they are presented with a FISA court order. They can delay their compliance by challenging the orders or slowing implementation of the wiretaps because company employees are responsible for placing them.

Intelligence officials say immunity is needed to maintain the cooperation of the private sector in ways unrelated to electronic surveillance. Company executives sometimes agree to allow intelligence agents to work in their companies, giving them what is known as nonofficial cover to do their intelligence business. That is a voluntary program; companies may see the immunity issue as an indication that the government will not help them if the agent is exposed.

BUSH: "Republicans and Democrats in the House stand ready to pass the Senate bill if House leaders would only stop blocking an up-or-down vote and let the majority in the House prevail."

THE FACTS: On Feb. 13, House Republicans and 34 Democrats blocked a 21-day extension of the expired law with encouragement from the White House, which wants the Senate bill to become law. House Democratic leaders say they want to vote on a compromise bill.

BUSH: "The bipartisan bill (the Senate passed) provides those tools our intelligence professionals need, yet the House's failure to pass this law raises the risk of reopening a gap in our intelligence gathering, and that is dangerous."

THE FACTS: The Senate bill passed with 68 votes, including 19 from Democrats. Both the House and Senate bills would close the intelligence gaps in similar, though not identical, ways.

Surveillance that began under the law that expired Feb. 16 may continue for up to a year. As of Saturday, intelligence officials said all telecommunications companies that have been asked to continue them are doing so. They said there was a delay in getting their cooperation because of the law's expiration, however, and therefore potentially important intercepts were not conducted.

The old procedures, which the White House says ties intelligence agents up in red tape, are now in effect. They generally require FISA court orders for all intelligence wiretaps on U.S. soil.

Pamela Hess, "Fact Check on Wiretapping Law Claims," Associated Press (27 Feb 2008 16:56 EST).

The issue of amendments to the Foreign Intelligence Surveillance Act (FISA) is not only a dispute about how government should conduct surveillance on its citizens, but also a hot political issue in an election year. For example, *The Washington Post* summarized the political attacks by Republicans:

> Republicans are convinced that highlighting their counterterrorism policies will be a political winner in this presidential election year, and they have focused this week on Democratic opposition to their version of a new surveillance bill as a way to paint Democrats as soft on national security, according to GOP lawmakers and their aides.
>
> Democrats respond that they are unfazed by the attacks, arguing that most Americans doubt the credibility of President Bush and Republicans when it comes to warning about security threats.
>
> Bush and GOP lawmakers have been releasing a blizzard of public statements and organizing multiple news conferences to pressure the House to adopt a Senate bill renewing and expanding a temporary surveillance law called the Protect America Act. The measure would grant legal immunity to telecommunications companies over their cooperation in warrantless wiretapping done after the Sept. 11, 2001, attacks.

Dan Eggen, "GOP Uses Surveillance Bill to Bash Democrats," *The Washington Post,* p. A08 (28 Feb 2008)
http://www.washingtonpost.com/wp-dyn/content/article/2008/02/27/AR2008022703316.html

conference committee

While President Bush continued to demand that the House pass the S.2248, the conference committee was privately meeting to reach a compromise between the House and Senate versions of the surveillance legislation. The House Intelligence Committee chairman, Rep. Silvestre Reyes, said in an interview on 2 Mar: "We think we're very close, probably within the next week we'll be able to hopefully bring it to a vote."[69] The second-ranking Republican in the House of Representatives was less optimistic than Reyes.[70]

The Washington Post reported on 4 March 2008:

> House and Senate Democratic leaders are headed into talks today that they say could lead to a breakthrough on legislation to revamp domestic surveillance powers and grant phone companies some form of immunity for their role in the administration's warrantless wiretapping program after the Sept. 11, 2001, terrorist attacks.
>
> A senior House Democratic aide said a bill could be sent to President Bush as early as next week. But significant issues remain, including those surrounding immunity, said Wyndee R. Parker, general counsel of the House Permanent Select Committee on Intelligence.

---

[69] anonymous, "Reyes: Deal Soon on Eavesdropping Law," Associated Press (2 Mar 2008 13:37 EST). See transcript of CNN Late Edition program at http://transcripts.cnn.com/TRANSCRIPTS/0803/02/le.01.html .

[70] *Ibid.*

> Parker, who said she hopes the House can take up the compromise legislation as early as this week, said a resolution has been delayed partly by the need for all members of the House Judiciary Committee to gain access to the letters and other relevant documents sent to the phone companies by the administration requesting their assistance.
>
> House Democratic leaders demanded such access before they would contemplate immunity, and the administration granted full access last week. Parker spoke at a breakfast meeting sponsored by the American Bar Association yesterday.
>
> ....
>
> Aides said House Majority Leader Steny H. Hoyer (D-Md.) has been polling his party's divided caucus the past few days about the immunity issue, with the liberal camp pushing to do nothing and the moderate wing supporting a provision in Senate-passed legislation granting immunity for the telecommunications industry.

Ellen Nakashima and Paul Kane, "Wiretap Compromise in Works," *The Washington Post,* p. A03 (4 Mar 2008)
http://www.washingtonpost.com/wp-dyn/content/article/2008/03/03/AR2008030302814.html

House 11-14 Mar 2008

On 11 March 2008, Representative Conyers introduced an amended H.R.3773 to the House. The night of 13 March, the House held a rare secret session to hear classified information on surveillance programs.[71] On Friday, 14 March, the House voted 213 to 197 to approve the amended H.R.3773. The House then adjourned for a two-week recess, leaving President Bush and the Senate without their desired legislation. There are three features of amended H.R.3773 that I find remarkable:

- no retroactive immunity for telecoms who cooperated with the government in illegal wiretaps (i.e., deletes § 202 of the Senate version)
- § 301 would create a National Commission to investigate Bush's secret Terrorist Surveillance Program
- § 802(b) would allow a judge in a civil action involving alleged unlawful surveillance to review classified information and "make any appropriate determination of fact or law."

This *in camera* review of classified information in § 802(b) permits the telecoms to offer a defense that involves what the government considers classified information. The Bush administration has been invoking the "state secrets" defense, to prevent public disclosure of Bush's Terrorist Surveillance Program, but which incidentally crippled any defense that the telecoms might offer.

---

[71] Pamela Hess, "House Closes Its Door for Spying Bill," Associated Press (14 Mar 2008 08:05 EDT).

The Washington Post reported on 15 March:

> A deeply divided House approved its latest version of terrorist surveillance legislation yesterday, rebuffing President Bush's demand for a bill that would grant telecommunications firms retroactive immunity for their cooperation in past warrantless wiretapping and deepening an impasse on a fundamental national security issue.
>
> Congress then defiantly left Washington for a two-week spring break.
>
> The legislation, approved 213 to 197, would update the Foreign Intelligence Surveillance Act of 1978 to expand the powers of intelligence agencies to eavesdrop on terrorism and spying suspects and keep pace with ever-changing communications technologies.
>
> ....
>
> The House's action ensures that Bush will not receive any surveillance legislation for weeks — if ever. White House spokesman Tony Fratto called the vote "a significant step backward in defending our country against terrorism."
>
> Senate Majority Leader Harry M. Reid (D-Nev.) tried to put the ball in Bush's court, however, saying: "Now is the time for Republicans to come to the negotiating table."

Jonathan Weisman, "House Passes a Surveillance Bill Not to Bush's Liking," *The Washington Post,* p. A02 (15 Mar 2008)

http://www.washingtonpost.com/wp-dyn/content/article/2008/03/14/AR2008031400803.html

Bush 13 Mar 2008

President Bush denounced the amended House bill at a speech on the South Lawn of the White House on 13 March:

> Last month House leaders declared that they needed 21 additional days to pass legislation giving our intelligence professionals the tools they need to protect America. That deadline passed last Saturday without any action from the House.
>
> This week House leaders are finally bringing legislation to the floor. Unfortunately, instead of holding a vote on the good bipartisan bill that passed the United States Senate, they introduced a partisan bill that would undermine America's security. This bill is unwise. The House leaders know that the Senate will not pass it. And even if the Senate did pass it, they know I will veto it.
>
> Yesterday the Attorney General and the Director of National Intelligence sent a leader [sic] to the Speaker explaining why the bill is dangerous to our national security. They cited a number of serious flaws in the bill, including the following:
>
> First, the House bill could reopen dangerous intelligence gaps by putting in place a cumbersome court approval process that would make it harder to collect intelligence on foreign terrorists. This is an approach that Congress explicitly rejected last August when bipartisan majorities in both houses passed the Protect America Act. And it is an approach the Senate rejected last month when it passed a new — new legislation to extend and strengthen the Protect America Act by an overwhelming vote of 68 to 29.
>
> Now House leaders are proposing to undermine this consensus. Their partisan legislation would extend protections we enjoy as Americans to foreign terrorists overseas. It would cause us to lose vital intelligence on terrorist threats, and it is a risk that our country cannot afford to take.

> Second, the House bill fails to provide liability protection to companies believed to have assisted in protecting our nation after the 9/11 attacks. Instead, the House bill would make matters even worse by allowing litigation to continue for years. In fact, House leaders simply adopted the position that class action trial lawyers are taking in the multi-billion-dollar lawsuits they have filed. This litigation would undermine the private sector's willingness to cooperate with the intelligence community, cooperation that is absolutely essential to protecting our country from harm. This litigation would require the disclosure of state secrets that could lead to the public release of highly classified information that our enemies could use against us. And this litigation would be unfair, because any companies that assisted us after 9/11 were assured by our government that their cooperation was legal and necessary.
>
> Companies that may have helped us save lives should be thanked for their patriotic service, not subjected to billion-dollar lawsuits that will make them less willing to help in the future. The House bill may be good for class action trial lawyers, but it would be terrible for the United States.
>
> Third, the House bill would establish yet another commission to examine past intelligence activities. This would be a redundant and partisan exercise that would waste our intelligence officials' time and taxpayers' money.
>
> The bipartisan House and Senate intelligence and judiciary committees have already held numerous oversight hearings on the government's intelligence activities. It seems that House leaders are more interested in investigating our intelligence professionals than in giving them the tools they need to protect us. Congress should stop playing politics with the past and focus on helping us prevent terrorist attacks in the future.
>
> Members of the House should not be deceived into thinking that voting for this unacceptable legislation would somehow move the process along. Voting for this bill does not move the process along. Instead, voting for this bill would make our country less safe because it would move us further away from passing the good bipartisan Senate bill that is needed to protect America.
>
> The American people understand the stakes in this struggle. They want their children to be safe from terror. Congress has done little in the three weeks since the last recess, and they should not leave for their Easter recess without getting the Senate bill to my desk.

President Bush, “President Bush Discusses FISA,” (13 March 2008 09:20 EDT).

The following day, after the House passed their amended bill, Bush’s deputy press secretary made the following statement:

> Today, the House of Representatives took a significant step backward in defending our country against terrorism and passed a partisan bill that will please class-action trial lawyers at the expense of our national security. Their bill would make it easier for class-action trial lawyers to sue companies whose only "offense" is that they are alleged to have assisted in efforts to protect the country after the attacks of September 11. These companies already face multibillion-dollar lawsuits, but even the status quo — which our intelligence professionals have said is undermining our ability to get cooperation from the private sector — is better than the alternative proposed in the House bill, which would preserve these lawsuits and give trial lawyers more weapons to attack companies for doing their patriotic service. The good news is that the House bill will be dead on arrival in the Senate and, in any event, would be vetoed by the President if it ever got to his desk.
>
> The House bill is not a serious effort to move the legislative process forward, nor is it a serious effort to protect our national security. It is a partisan bill designed to give the House Democratic leadership cover for their failure to act responsibly and vote on the bipartisan Senate bill. The President trusts that Senate leaders, who have acted in a far more bipartisan

> and responsible way than their colleagues in the House, will see the House bill for the political ploy that it is, reject it, and send back to the House the strong bill the Senate has already passed.

Tony Fratto, "Partisan House Bill," (14 Mar 2008)
http://www.whitehouse.gov/news/releases/2008/03/20080314-7.html

June/July 2008

Despite President Bush's rhetoric during February 2008 and ending on 14 March 2008 about the urgent need to extend the Protect America Act and to give telecoms retroactive immunity for their unlawful acts, there was mostly silence about amendments to FISA during the three months from mid-March 2008 to mid-June 2008. Apparently, during these three months, members of the U.S. House of Representatives and U.S. Senate were negotiating compromise amendments to FISA. The public silence allowed compromise, since the public would forget about prior positions of key legislators. The public silence also showed that Bush's rhetoric about urgent need was hyperbole, because the legislative delay apparently caused no problems. The real deadline was always the 5 August 2008 expiration of the Protect America Act.

In one of the few news stories during the three months of silence, the Associated Press on 22 May 2008 reported that a compromise had been reached between the House and Senate. On the critical issue of retroactive immunity for telecoms, the Associated Press reported:

> The new Republican proposal — which Sen. Kit Bond of Missouri said is backed by the White House and intelligence agencies — would allow the FISA court to decide. It would require the attorney general to certify that the companies acted lawfully and at the request of the president.
>
> The court would be allowed to read the requests to telecom companies for the wiretaps to be placed, and the plaintiffs could file their complaints with the court. The court could dismiss the lawsuits if it finds that supported by "a preponderance of the evidence."

Pamela Hess, "Republicans shift, a little, on surveillance rules," Associated Press (22 May 2008 23:38 ET).

H.R. 6304

On 19 June 2008, a final compromise was publicly announced, and a vote was scheduled in the U.S. House of Representatives for the following day on H.R. 6304, with the short title of "FISA Amendments Act of 2008". The Associated Press reported:

> House and Senate leaders have agreed to a new compromise surveillance bill that would effectively shield from potentially costly civil lawsuits telecommunications companies that helped the government wiretap citizens' phone and computer lines after the September 11 terrorist attacks without court permission.
>
> The House will debate the bill on Friday [20 June], potentially ending a months-long standoff about the rules for government wiretapping inside the United States.
>
> House Majority Leader Steny Hoyer of Maryland said the new bill "balances the needs of our intelligence community with Americans' civil liberties, and provides critical new oversight and accountability requirements."

> The issue of legal protection for telecommunications companies that participated in "warrantless wiretapping" has been the single largest sticking point. The Senate passed a bill that immunized them from lawsuits. The House bill was silent on the matter. The White House threatened to veto any bill that did not shield the companies, which tapped lines at the behest of the president and attorney general — but without permission from a special court established for this very purpose — the Foreign Intelligence Surveillance Court.
>
> "Warrantless wiretapping" went on for almost six years until it was revealed by the New York Times. Some 40 lawsuits have been filed against the companies by people and groups who think they were illegally eavesdropped on by the government.
>
> The compromise bill would have a federal district court determine whether the telecommunications companies received signed orders authorized by the president asking them to place wiretaps to detect or prevent a terrorist attack. If so, the lawsuits would be dismissed.
>
> But not all Democrats are falling in line. Senate Judiciary Committee Chairman Patrick Leahy of Vermont said he does not support the immunity deal because it prevents a court from reviewing the legality of the warrantless wiretapping program.

Pamela Hess, "Dems, GOP agree to telecom immunity deal," Associated Press (19 June 2008, 12:58 ET).

key features of H.R. 6304

The exact language of H.R. 6304 giving telecoms immunity from civil litigation is:

> (a) Notwithstanding any other provision of law, a civil action may not lie or be maintained in a Federal or State court against any person for providing assistance to an element of the intelligence community, and shall be promptly dismissed, if the Attorney General certifies to the district court of the United States in which such action is pending that —
>
> ....
>
> (4) in the case of a covered civil action, the assistance alleged to have been provided by the electronic communication service provider was —
>
> (A) in connection with an intelligence activity involving communications that was —
>
> (i) authorized by the President during the period beginning on September 11, 2001, and ending on January 17, 2007; and
>
> (ii) designed to detect or prevent a terrorist attack, or activities in preparation for a terrorist attack, against the United States; and

(B) the subject of a written request or directive, or a series of written requests or directives, from the Attorney General or the head of an element of the intelligence community (or the deputy of such person) to the electronic communication service provider indicating that the activity was —

(i) authorized by the President; and

(ii) determined to be lawful, or

(5) the person did not provide the alleged assistance.
H.R. 6304, Title II, § 802(a)(4) (as passed by the House on 20 June 2008).

The amended H.R. 3773, which was approved on 14 Mar 2008, created a national commission to investigate the TSP and issue a written report due in one year. Section 301(b) of H.R. 6304 would require "the Inspectors General of the Department of Justice, the Office of the Director of National Intelligence, the National Security Agency, the Department of Defense, and any other element of the intelligence community that participated in the President's Surveillance Program, shall complete a comprehensive review of" the TSP.

While prior statutes were *not* ambiguous, H.R. 6304 adds to federal statutes an explicit command that the domestic wiretap statutes and the FISA statute are the "exclusive means" for conducting surveillance, which would make it more difficult for a future president to violate federal statutes in the way President George W. Bush did with his TSP.

§ 112. (a) Except as provided in subsection (b), the procedures of chapters 119, 121, and 206 of title 18, United States Code, and this Act shall be the exclusive means by which electronic surveillance and the interception of domestic wire, oral, or electronic communications may be conducted.

"(b) Only an express statutory authorization for electronic surveillance or the interception of domestic wire, oral, or electronic communications, other than as an amendment to this Act or chapters 119, 121, or 206 of title 18, United States Code, shall constitute an additional exclusive means for the purpose of subsection (a)."

(b) Offense — Section 109(a) of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1809(a)) is amended by striking "authorized by statute" each place it appears and inserting "authorized by this Act, chapter 119, 121, or 206 of title 18, United States Code, or any express statutory authorization that is an additional exclusive means for conducting electronic surveillance under section 112."; and

(c) Conforming Amendments —

(1) TITLE 18, UNITED STATES CODE — Section 2511(2)(a) of title 18, United States Code, is amended by adding at the end the following:

> "(iii) If a certification under subparagraph (ii)(B) for assistance to obtain foreign intelligence information is based on statutory authority, the certification shall identify the specific statutory provision and shall certify that the statutory requirements have been met."; and

(2) TABLE OF CONTENTS — The table of contents in the first section of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. § 1801 et seq.) is amended by inserting after the item relating to section 111, the following new item:

> "Sec. 112. Statement of exclusive means by which electronic surveillance and interception of certain communications may be conducted.".

H.R. 6304, Title VII, § 112 (as passed by the House on 20 June 2008).

Chapter 119 of Title 18 of the U.S. Code corresponds to 18 U.S.C. § 2510-2522, which covers interception of communications. Chapter 121 of Title 18 of the U.S. Code corresponds to 18 U.S.C. § 2701-2712, which covers access of stored communications, such as e-mail. Chapter 206 of Title 18 of the U.S. Code corresponds to 18 U.S.C. § 3121-3127, which covers tracing telephone numbers.

more news

The Washington Post reported on how the compromise was finally obtained and some consequences of H.R. 6304:

> House and Senate leaders agreed yesterday [19 June] on surveillance legislation that could shield telecommunications companies from privacy lawsuits, handing President Bush one of the last major legislative victories he is likely to achieve.
>
> The agreement extends the government's ability to eavesdrop on espionage and terrorism suspects while effectively providing a legal escape hatch for AT&T, Verizon Communications and other telecom firms. They face more than 40 lawsuits that allege they violated customers' privacy rights by helping the government conduct a warrantless spying program after the Sept. 11, 2001, attacks.
>
> The breakthrough on the legislation came hours after the White House agreed to Democratic demands for domestic spending additions to an emergency war funding bill. Taken together, the bills — two of the last major pieces of legislation to be approved by Congress this year — suggest that Bush still wields considerable clout on national security issues but now must acquiesce to Democratic demands on favored domestic priorities to secure victory.

The war spending bill, for example, includes $162 billion for the conflicts in Iraq and Afghanistan and an additional $95 billion worth of domestic spending on programs such as unemployment insurance and higher-education benefits for veterans. Bush, who had threatened for months to veto the legislation, said he will sign it.

Leading Democrats acknowledged that the surveillance legislation is not their preferred approach, but they said their refusal in February to pass a version supported by the Bush administration paved the way for victories on other legislation, such as the war funding bill.

"When they saw that we were unified in sending that bill rather than falling for their scare tactics, I think it sent them a message," said House Speaker Nancy Pelosi (D-Calif.). "So our leverage was increased because of our Democratic unity in both cases."

Under the surveillance agreement, which is expected to be approved today by the House and next week by the Senate, telecoms could have privacy lawsuits thrown out if they show a federal judge that they received written assurance from the Bush administration that the spying was legal.

The proposal marks a compromise by Republicans and the Bush administration, which had opposed giving federal judges any significant role in granting legal immunity to the phone companies.

The legislation also would require court approval of procedures for intercepting telephone calls and e-mails that pass through U.S.-based servers — another step that the White House and GOP lawmakers previously resisted.

"It is the result of compromise, and like any compromise it is not perfect, but I believe it strikes a sound balance," said House Majority Leader Steny H. Hoyer (Md.), the lead Democratic negotiator in talks between lawmakers and the White House.

But overall, the deal appears to give Bush and his aides, including Attorney General Michael B. Mukasey and Director of National Intelligence Mike McConnell, much of what they sought in a new surveillance law.

....

The sharpest critics of the administration's surveillance policies were not mollified. Sen. Russell Feingold (D-Wis.) said the legislation "is not a compromise; it is a capitulation." "Allowing courts to review the question of immunity is meaningless when the same legislation essentially requires the court to grant immunity," he said.

Caroline Frederickson, a lobbyist for the American Civil Liberties Union, said, "The telecom companies simply have to produce a piece of paper we already know exists, resulting in immediate dismissal."

Dan Eggen and Paul Kane, "Surveillance Bill Offers Protection To Telecom Firms, Deal Would Extend U.S. Wiretap Power, Shield Providers Facing Privacy Lawsuits," *The Washington Post,* p. A01 (20 June 2008). http://www.washingtonpost.com/wp-dyn/content/article/2008/06/19/AR2008061901545.html

President Bush made a terse speech at the White House, which is quoted here in its entirety:

Good morning. This week Congress moved forward on two important issues affecting the national security of our country.

Yesterday the House passed a responsible war funding bill that will provide vital resources to our men and women on the front lines in the war on terror. This legislation gives our troops the funds they need to prevail without tying the hands of our commanders in the field or imposing artificial timetables for withdrawal.

The bill also supports our military families by passing an expansion of the GI Bill that makes it easier for our troops to transfer unused education benefits to their spouses and their

children. I want to thank the members of Congress for their action on this legislation, and I urge the Senate to pass it as soon as possible.

Members of the House and Senate also reached a bipartisan agreement yesterday [19 June] on legislation to allow our intelligence professionals to quickly and effectively monitor the plans of terrorists abroad, while protecting the liberties of Americans here at home.

My Director of National Intelligence and the Attorney General tells me that this is a good bill. It will help our intelligence professionals learn our enemies' plans for new attacks. It ensures that those companies whose assistance is necessary to protect the country will themselves be protected from liability for past or future cooperation with the government.

The enemy who attacked us on September the 11th is determined to strike this country again. It's vital that our intelligence community has the ability to learn who the terrorists are talking to, what they're saying, and what they are planning.

I encourage the House of Representatives to pass this bill today, and I ask the Senate to take it up quickly so our intelligence professionals can better protect Americans from harm.

I'm pleased with the bipartisan cooperation on both these bills, and I thank the members for their efforts. Thank you.

President Bush, "President Bush Discusses the Foreign Intelligence Surveillance Act and Funding For Troops," (20 June 2008, 09:11 ET)
http://www.whitehouse.gov/news/releases/2008/06/20080620-1.html

Senator Arlen Specter, a Republican and former chairman of the Senate Judiciary Committee, issued the following press release:

I am opposed to the proposed legislation because it does not require a judicial determination that what the telephone companies have done in the past is constitutional. It is totally insufficient to grant immunity for the telephone companies' prior conduct based merely on the written assurance from the administration that the spying was legal.

The provision that the bill will be the exclusive means for the government to wiretap is meaningless because that specific limitation is now in the 1978 Act and it didn't stop the government from the warrantless terrorist surveillance program and what the telephone companies have done. That statutory limitation leaves the president with his position that his Article II powers as commander in chief cannot be limited by statute, which is a sound constitutional doctrine unless the courts decide otherwise. Only the courts can decide that issue and this proposal dodges it.

Arlen Specter, "Specter Reaction to FISA Agreement" (20 June 2008)
http://specter.senate.gov/public/index.cfm?FuseAction=NewsRoom.NewsReleases&ContentRecord_id=a64d90e3-f406-72b5-56ed-fa0512b90a3c .

Senator Patrick Leahy, a Democrat and current chairman of the Senate Judiciary Committee, also opposed H.R. 6304:

After months of negotiations, the legislation unveiled today to replace the so-called Protect America Act, which Republicans refused to extend, is not a bill I can support. I have said since the beginning of this debate that I would oppose a bill that did not provide accountability for this administration's six years of illegal, warrantless wiretapping. This bill would dismiss ongoing cases against the telecommunications carriers that participated in that program without allowing a judicial review of the legality of the program. Therefore, it lacks accountability measures that I believe are crucial. My interest is not in harming telecommunications carriers. I would have supported indemnification by the government or

substitution of the government for them in these lawsuits. But for me, there must be accountability.

With respect to the surveillance authorities, I believe the bill represents an improvement over the flawed legislation passed the Senate earlier this year. I applaud Representative Hoyer and Senator Rockefeller for their diligent work in negotiating this package. They added protections to the surveillance authorities that bring it closer to the bill the Senate Judiciary Committee reported last year. If the bill passes, I will work with the next administration to make additional improvements.

I will continue to work to protect all Americans from the Bush-Cheney administration's roll back of civil liberties of Americans and disregard for the rule of law. As the Supreme Court noted last week, "security subsists, too, in fidelity to freedom's first principles."

We can protect our security while honoring American values and respecting our freedoms.

Patrick Leahy, "Comment Of Senator Patrick Leahy (D-Vt.), ..., On FISA Amendments Act Of 2008," (19 June 2008) http://leahy.senate.gov/press/200806/061908a.html .

After three hours of speeches and proceedings on the floor of the U.S. House of Representatives, H.R. 6304 was approved by a vote of 293 to 129.[72] The Associated Press reported:

"This bill, though imperfect, protects both," said Rep. Jane Harman, D-Calif., and a former member of the intelligence committee.

President Bush praised the bill Friday [20 June]. "It will help our intelligence professionals learn enemies' plans for new attacks," he said in a statement before television cameras a few hours before the vote.

The House's passage of the FISA Amendment bill marks the beginning of the end to a monthslong standoff between Democrats and Republicans about the rules for government wiretapping inside the United States. The Senate was expected to pass the bill with a large margin, perhaps as soon as next week, before Congress takes a break during the week of the Fourth of July.

....

The compromise bill directs a federal district court to review certifications from the attorney general saying the telecommunications companies received presidential orders telling them wiretaps were needed to detect or prevent a terrorist attack. If the paperwork were deemed in order, the judge would dismiss the lawsuit.

It would also require the inspectors general of the Justice Department, Pentagon and intelligence agencies to investigate the wiretapping program, with a report due in a year.

Critics of the bill say dismissal [of civil litigation on the TSP] is a foregone conclusion. "These provisions turn the judiciary into the administration's rubber stamp," said Rep. Zoe Lofgren, D-Calif. She opposes the bill.

Opponents of immunity believe civil lawsuits are the only way the full extent of the wiretapping program will ever be revealed.

---

[72] Roll call vote Nr. 437 in House of Representatives, 20 June 2008.

> Key senators voiced strong opposition to the compromise, although they're unlikely to have the votes to either defeat or filibuster the bill. Sen. Arlen Specter of Pennsylvania, the top Republican on the Senate Judiciary Committee, condemned the immunity deal. He said that nothing in the new bill would prevent the government from once again wiretapping domestic phone and computer lines without court permission.
>
> Specter said the problem is constitutional: The White House may still assert that the president's Article II powers as commander in chief supersede statutes that would limit him actions. "Only the courts can decide that issue and this proposal dodges it," Specter said.
>
> Speaker of the House Nancy Pelosi of California disputed that, saying FISA would from now on be the authority for the government to conduct electronic surveillance. "There is no inherent authority of the president to do whatever he wants. This is a democracy, not a monarchy," she said.

Pamela Hess, "House easily passes compromise surveillance law," Associated Press (20 June 2008, 14:31 ET).

U.S. Senate

Five days after the House passed H.R. 6304, the U.S. Senate began to consider the same bill. On Wednesday, 25 June 2008, the Senate held a procedural vote on a motion to invoke cloture, which motion was passed by a vote of 80 to 15.[73] The 15 nay votes — who wanted to continue debate or filibuster — were by 14 Democrats and 1 Independent:

Biden (D-DE)	Boxer (D-CA)	Brown (D-OH)	Cantwell (D-WA)
Dodd (D-CT)	Durbin (D-IL)	Feingold (D-WI)	Harkin (D-IA)
Kerry (D-MA)	Lautenberg (D-NJ)	Leahy (D-VT)	Menendez (D-NJ)
Sanders (I-VT)	Schumer (D-NY)	Wyden (D-OR)	

The following day, a vote on the bill in the Senate was unexpectedly postponed. According to the Associated Press:

> The Senate on Thursday [26 June] put off voting on controversial electronic surveillance legislation, in spite of what appeared to be overwhelming support for the bill.
>
> Sen. Russ Feingold, D-Wis., and more than a dozen other senators who oppose telecom immunity threw up procedural delays that threatened to force the Senate into a midnight or weekend session. The prospect of further delays was enough to cause Senate Majority Leader Harry Reid, D-Nev., to postpone the vote until after the weeklong July 4 vacation.
>
> ....
>
> Feingold and other critics of the legislation say civil lawsuits are the only way the country will learn the extent of the Bush administration's nearly six years of warrantless wiretapping. The surveillance took place without the permission or knowledge of the secret court Congress created 30 years ago to handle such activities.

---

[73] U.S. Senate Roll Call Vote Nr. 158 (25 June 2008); CONGRESSIONAL RECORD at S6141.

"I hope that over the July 4th holiday, senators will take a closer look at this deeply flawed legislation and understand how it threatens the civil liberties of the American people," Feingold said in a statement. "It is possible to defend this country from terrorists while also protecting the rights and freedoms that define our nation."

The bill amending the Foreign Intelligence Surveillance Act represents a compromise. In exchange for telecom immunity, the inspectors general of the Pentagon, Justice Department and intelligence agencies will investigate the wiretapping program.

The attorney general and national intelligence director on Thursday said President Bush would veto the bill if the immunity provisions were stripped from it.

Pamela Hess, "Senate delays vote on surveillance bill," Associated Press (26 June 2008, 20:22 ET).

On 26 June 2008, the White House press secretary issued the following "fact sheet". The italics, underlining, and bold face in the original are all preserved in this quotation.

Senate Should Not Pass Any Amendment That Would Deny Retroactive Liability Protection Or Unnecessarily Delay Dismissal Of Costly Lawsuits For Companies That Are Believed To Have Assisted The Government Following 9/11

Today, the Senate could consider amendments that would strip or weaken the retroactive liability protection provided by the bipartisan FISA modernization bill that passed the House by an overwhelming vote of 293 to 129. Failure to pass the liability protection contained in the House bill for companies that assisted our intelligence professionals after the 9/11 attacks will undermine our partnership with the private sector. Such cooperation is essential to protecting the country from another terrorist attack. The Senate should pass the bipartisan House legislation so our intelligence professionals can better protect Americans from foreign threats.

Without This Protection, Private Sector Companies Will Become Less Willing To Cooperate With Our Intelligence Community's Efforts To Protect The Country

Failure to provide retroactive liability protection would undermine the private sector's willingness to cooperate with the Intelligence Community – cooperation that is essential to protecting America. Companies may also be less willing to assist the government in the future if they face a threat of private lawsuits each time they are alleged to have provided assistance.

- **Providing retroactive liability protection is critical to providing our intelligence officials the tools they need to carry out their mission of protecting our homeland.** The Attorney General and Director of National Intelligence have reported that "even prior to the expiration of the Protect America Act, we experienced significant difficulties in working with the private sector because of the continued failure to provide liability protection for such companies."

- **The Senate should not pass any amendment that would unnecessarily complicate and prolong lawsuits against companies.** A major purpose of the retroactive liability protections in the bipartisan House bill is to provide for the expeditious dismissal of lawsuits once the Attorney General certifies, and the district court confirms, that companies provided assistance in response to a request from the Government. The Senate Intelligence Committee, in a bipartisan report, concluded that any companies

that provided assistance acted in good faith and that permitting the lawsuits to continue could deter the private sector from providing lawful assistance to the intelligence community in the future.

It is unfair and unjust to threaten companies with financial ruin because they are believed to have helped their country. Allowing these lawsuits to continue would be unfair because any companies that assisted us after 9/11 were assured by our government that their cooperation was legal and necessary. More than 40 such lawsuits have been filed, seeking hundreds of billions of dollars in damages from these companies. These lawsuits are good for class action trial lawyers, but they are terrible for the United States.

- **Companies that assisted with the clear intention of helping to protect their fellow citizens should be thanked for their patriotic service, not subjected to multibillion-dollar lawsuits that will make them less willing to help in the future.**

Allowing These Lawsuits To Proceed Risks Disclosure Of Highly Classified Information Regarding The Methods Used By Our Intelligence Community To Protect The Country From Terrorist Attack

This litigation could lead to the disclosure of state secrets and possibly the public release of highly classified information that our enemies could use against us. It makes no sense to give the enemy critical knowledge about what the United States is doing to protect the American people. But this is what could happen if the Senate allows massive and costly class-action lawsuits to proceed, which would increase the risk of revealing the methods used by our Intelligence Community to monitor foreign terrorist communications.

Fact Sheet: Retroactive Liability Protection: Providing Our Intelligence Officials the Tools They Need to Keep Our Nation Safe (26 June 2008)
http://www.whitehouse.gov/news/releases/2008/06/20080626-10.html
The bashing of "class-action trial lawyers" by the White House is a familiar theme, which was introduced by President Bush on 16 Feb 2008 and quoted above.

Public discussion of this bill was diverted by the U.S. Supreme Court's 26 June 2008 decision in *District of Columbia v. Heller,* a decision holding that the Second Amendment permits citizens who are not members of a militia to own firearms, and thus a city's ban on pistols was unconstitutional. Also on 26 June, David Addington and John Yoo[74] testified publicly before a subcommittee of the House Judiciary Committee about "harsh interrogation methods" (i.e., torture) of terrorist suspects. The right to own firearms and torture of suspects are easier to understand than the technical content of the amendments to FISA.

The San Francisco Chronicle reported on 6 July:

> Obama has been an outspoken critic of the surveillance program for more than two years, and voted against the confirmation of its director, Michael Hayden, to head the CIA in 2006.
>
> "No more illegal wiretapping of American citizens. ... No more ignoring the law when it is inconvenient," the Illinois senator declared in August 2007.

---

[74] Addington is chief of staff to Vice-President Cheney; Yoo was a staff attorney at the Justice Department.

> Obama has been particularly adamant against Bush's insistence on protecting phone companies from lawsuits.
>
> "No one should get a free pass to violate the basic civil liberties of the American people - not the president of the United States, and not the telecommunications companies that fell in line with his warrantless surveillance program," Obama said in January. He backed legislation that would have barred immunity for the companies, and says he will support an immunity-stripping amendment to the bill this week.
>
> But after wrapping up the Democratic nomination a month ago with support from the party's liberal base, Obama — now facing daily criticism from Republicans on national security — has moved right on several issues, including surveillance.
>
> He announced two weeks ago that he would support the wiretap bill as compromise legislation. **....** Many of Obama's supporters were dismayed.
>
> The legislation "is not a compromise; it is a capitulation," said Sen. Russ Feingold, D-Wis., an Obama backer and author of the amendment to deny immunity to the phone companies. On Obama's campaign Web site, BarackObama.com, more than 10,000 fans of the candidate have implored him to reverse course again and oppose the bill.

Bob Egelko, "The politics behind Senate wiretap bill," *The San Francisco Chronicle,* (6 July 2008) http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/07/05/MNFJ11IQ46.DTL

This news article foreshadowed that the eventual approval of the FISA Amendments Act of 2008, H.R. 6304, would be reported along with Senator Obama's change in position on that issue. When Obama defeated Hillary Clinton in early June 2008, Obama no longer needed to take liberal positions because *all* of the liberals would presumedly vote for him in the presidential election in November 2008. Instead, it was natural that Obama would shift toward the center, in the hopes of attracting votes from moderates.

On 8 July, the White House released another "fact sheet" urging that the Senate approve immunity for telecoms. The italics, underlining, and boldface are all present in the original.

> *Congress Should Not Pass Any Amendments To Delay Or Eliminate Retroactive Liability Protection For Companies Believed To Have Assisted Our Government In The Aftermath Of 9/11*
>
> **As Congress returns from its Fourth of July recess, it should act quickly to pass the crucial long-term FISA modernization bill to keep our Nation safe.** The strong bipartisan legislation passed in the House provides the Intelligence Community with the tools it needs to secure our Nation while protecting the liberties of Americans. This bill also provides the necessary legal protections for those companies sued in the aftermath of 9/11. Both Houses of Congress, by wide bipartisan margins, have made the judgment that retroactive liability protection is the appropriate and fair result. If Congress were to include any amendment that eliminates or delays liability protection for those that assisted the Government in the aftermath of 9/11, the President would veto this legislation.
>
> **Three Senate Amendments Threaten The Important Liability Protection Provided In The Bipartisan House Bill**

1. The Dodd/Feingold/Leahy amendment proposes to entirely eliminate retroactive liability protection from the bipartisan House intelligence legislation. The Administration opposes any amendment to strike liability protection because any companies that may have assisted the Government after 9/11 were assured that their cooperation was legal and necessary. The liability protection in the bipartisan House legislation does not extend to the Government or Government officials, and it does not immunize any criminal conduct. The liability protection provision applies only in a narrow set of circumstances. An action must be dismissed if:

- The electronic communications service provider did not provide the assistance; or

- The assistance was provided in the wake of the 9/11 attacks and was the subject of a written request or series of requests from a senior Government official indicating that the activity was authorized by the President and determined to be lawful.

2. The Specter Amendment would continue to leave companies vulnerable to unwarranted and unfair lawsuits. Congress should not allow companies to be subjected to billion-dollar claims because they are believed to have answered the Government's request for assistance and were assured of the legality of any actions.

- **This amendment would unnecessarily prolong and delay litigation, and the companies being sued would continue to be subjected to burdens of litigation such as attorneys' fees and disruption of their businesses.** This could deter private sector cooperation with the intelligence community.

- **The amendment would also risk the disclosure of highly sensitive classified information concerning intelligence sources and methods.** Extending this litigation could lead to the disclosure of highly sensitive national security information and would be contrary to the well-established state secrets privilege doctrine.

3. The Bingaman amendment would unnecessarily postpone a decision on whether to provide liability protection to telecommunications companies. The amendment would prevent providers from receiving retroactive liability protection until 90 days after the Inspectors General of various departments complete and submit a review of prior activities.

- **Providing prompt liability protection is critical to our national security.** These cases have already been pending for years, and delaying implementation of the liability protections means that the companies would remain subjected to the prospect of defending against multi-billion-dollar claims and continue to suffer from the uncertainty caused by pending litigation.

Retroactive Liability Protection Is The Appropriate And Fair Result

Liability protection is a fair and just result and is necessary to ensure the continued assistance of the private sector. The Senate Intelligence Committee already conducted an extensive study of the issue and determined that providers had acted in response to written requests or directives stating that the activities had been authorized by the President and had been determined to be lawful. This Committee, chaired by Sen. Rockefeller (D-WV), carefully studied the issue and found that "without retroactive immunity, the private sector

might be unwilling to cooperate with lawful Government requests in the future without unnecessary court involvement and protracted litigation."

- **The assistance of private-sector telecommunications companies is vital to protecting our Nation from attack.** Most of the communications infrastructure the Intelligence Community relies on is owned and operated by the private sector, meaning private-sector assistance is essential to gaining intelligence on the plans of those who wish to attack us.

- **Without this protection, companies will be increasingly reluctant to provide vital cooperation because of their uncertainty about the law and fear of being sued by class-action trial lawyers.**

White House Press Secretary, "Fact Sheet: Retroactive Liability Protection Is Critical to Our National Security,"
http://www.whitehouse.gov/news/releases/2008/07/20080708-7.html (8 July 2008)

On the morning that the U.S. Senate voted on H.R. 6304, *The San Francisco Chronicle* published the following editorial:

> Warrantless wiretapping of Americans should outrage Congress into banning the practice. But, in a display of political expediency, the Senate is about to bless it, following a similar cave-in by the House last month.
>
> Making matters worse, both likely presidential candidates — Sens. Barack Obama and John McCain — plan to reverse their opposition and vote for the White House-backed rewrite of the Foreign Intelligence Surveillance Act. The bigger of the two reversals is Obama, who earlier this year had promised a filibuster to defeat the bill.
>
> Giving in on wiretapping — along with earlier remarks favoring a Supreme Court ruling barring a gun ban — are part of Obama's noticeable shift to the center and away from prior principles. His decision to reverse direction and back the wiretap law has touched off a storm among his bedrock backers and civil liberties groups.
>
> At issue is an attempt to rein in President Bush's post-9/11 usurpation of wiretap law. Until 2005, he gave intelligence gatherers wide powers to eavesdrop on domestic calls to overseas phones in the name of tracking terrorists. But he largely dodged using a special intelligence court that federal law established to oversee the work. He also enlisted major phone companies in the operation and kept it secret.
>
> The new rewrite falls short in serious ways. It allows judges to dismiss about 40 lawsuits that claim the phone companies illegally cooperated. If these suits end, the public may never know the extent of the Bush wiretapping scheme.
>
> It's time for the Senate, and especially its two presidential aspirants, to halt a serious invasion of personal rights.

Editorial, "Stand up, senators," *San Francisco Chronicle,* (9 July 2008)
http://www.sfgate.com/cgi-bin/article.cgi?f=/c/a/2008/07/08/EDJQ11LM1T.DTL

8-9 July 2008

On 8 July 2008, there were a long series of speeches in the U.S. Senate on the FISA Amendments Act of 2008, H.R. 6304.[75] The following day, there were more speeches, then votes on three amendments, followed by a vote on the Act itself.[76] Each of the three amendments were defeated:

1. **Specter amendment**, S.Amndt. 5059. to H.R. 6304 defeated 61 to 37, (Vote Nr. 165, 9 July 2008). The amendment provided that the certification about the TSP from the Attorney General could be rejected by the trial court, if "the court finds that such certification is not supported by substantial evidence provided to the court". In other words, if the court found that the TSP was unconstitutional or illegal, then the telecoms would have no immunity, despite the certification of the Attorney General. Senator Specter was the only Republican to vote for this amendment.

2. **Dodd-Feingold-Leahy amendment**, S.Amndt. 5064 defeated 66 to 32 (Vote Nr. 164, 9 July 2008) would have stricken the immunity for telecoms from H.R. 6304. Voting for Dodd-Feingold-Leahy amendment were 31 Democrats, 1 Independent, and zero Republicans: This was the least popular of the three amendments to H.R. 6304.

3. **Bingaman amendment**, S.Amndt. 5066 defeated by 56 to 42 (Vote Nr. 166, 9 July 2008) purpose: "To stay pending cases against certain telecommunications companies and provide that such companies may not seek retroactive immunity until 90 days after the date the final report of the Inspectors General on the President's Surveillance Program is submitted to Congress."[77] Specifically, the Attorney General may not make the certification to a court until 90 days after the final report is submitted to Congress.

   Senator Specter was the only Republican to vote for the Bingaman amendment. The Bingaman amendment was the most popular of the three amendments to H.R. 6304, but the Bingaman amendment needed an additional 18 votes to pass.

At 14:47 EDT on 9 July, H.R. 6304 passed the Senate on a vote of 69 to 28. (Vote Nr. 168, 9 July 2008). Fifty votes were needed to pass this bill, so there was a margin of 19 additional votes. 27 Democrats, 1 Independent, and zero Republicans voted against H.R. 6304. The following senators voted against H.R. 6304:

---

[75] CONGRESSIONAL RECORD, S. 6379 - S. 6429 (8 July 2008).

[76] CONGRESSIONAL RECORD, S. 6454 - S. 6476 (9 July 2008).

[77] CONGRESSIONAL RECORD, S. 6398 (8 July 2008).

Akaka (D-HI)	Dorgan (D-ND)	Murray (D-WA)
Biden (D-DE)	Durbin (D-IL)	Reed (D-RI)
Bingaman (D-NM)	Feingold (D-WI)	Reid (D-NV)
Boxer (D-CA)	Harkin (D-IA)	Sanders (I-VT)
Brown (D-OH)	Kerry (D-MA)	Schumer (D-NY)
Byrd (D-WV)	Klobuchar (D-MN)	Stabenow (D-MI)
Cantwell (D-WA)	Lautenberg (D-NJ)	Tester (D-MT)
Cardin (D-MD)	Leahy (D-VT)	Wyden (D-OR)
Clinton (D-NY)	Levin (D-MI)	
Dodd (D-CT)	Menendez (D-NJ)	

President Bush made the following terse speech a few hours after the Senate passed the FISA Amendments Act of 2008:

> Today the United States Congress passed a vital piece of legislation that will make it easier for this administration and future administrations to protect the American people. This vital intelligence bill will allow our national security professionals to quickly and effectively monitor the plans of terrorists outside the United States, while respecting the liberties of the American people.
>
> This legislation is critical to America's safety; it is long overdue. Months ago my administration set out key criteria that this intelligence legislation would have to have before I would sign it into law. The Attorney General and Director of National Intelligence report that the bill Congress passed today meets these criteria, and therefore, I will soon sign the bill into law.
>
> This bill will help our intelligence professionals learn who the terrorists are talking to, what they're saying, and what they're planning. It will ensure that those companies whose assistance is necessary to protect the country will, themselves, be protected from lawsuits for past or future cooperation with the government. It will uphold our most solemn obligation as officials of the federal government to protect the American people.
>
> I want to thank the members of my administration who worked hard to get this legislation passed. I thank the Democratic and Republican leadership in the Congress for their efforts, particularly House Majority Leader Hoyer, House Republican Whip Blunt, Senators Bond and Rockefeller, Congressmen Hoekstra, Reyes and Smith.
>
> This legislation shows that even in an election year we can come together and get important pieces of legislation passed.
>
> Thank you.

George W. Bush, "President Bush Pleased by Passage of FISA Reform Legislation," (9 July 2008 16:01 EDT) http://www.whitehouse.gov/news/releases/2008/07/20080709-7.html

A few hours after the Senate voted to approve the FISA Amendments Act of 2008, *The New York Times* published the following editorial.

> The results were so thoroughly precooked that there was no surprise in the Senate's 69-to-28 vote today to gut a law that has protected Americans from spying by their own government for 30 years.
>
> Still, it was distressing — and depressing — to watch Congress wrench Americans' civil liberties back to where they were in the days before Watergate, when the United States government listened to our phone calls whenever it wanted.
>
> We had hoped, at least, that the supporters of this awful bill would make a substantive case for their position. Instead, they offered up the usual thick stew of fear mongering mixed with big chunks of disinformation.
>
> Senator Christopher S. Bond, the Missouri Republican who is vice chairman of the Senate Intelligence Committee, said there was nothing to fear in the bill "unless you have Al Qaeda on your speed dial." Actually, the bill has nothing to do with whether Al Qaeda is on your speed dial.
>
> It dilutes safeguards in the old Foreign Intelligence Surveillance Act that directed government eavesdropping at threats like Al Qaeda. The bill will permit the government to intercept your telephone calls, cell phone calls, letters, faxes and email messages to other countries basically whenever it wants.
>
> The government eavesdroppers won't need a warrant and they won't even have to say they are trying to prevent a terrorist act.
>
> All the government has to do is certify that its target is someone overseas and it can snoop all it wants for an entire year without a warrant.
>
> Does the C.I.A. want to listen in on all the calls to say, Damascus, or Tel Aviv, or London? No problem, just get the Attorney General and the Director of National Intelligence to "certify" that no one in this country is the "target" of that investigation and they can listen to every call made to those cities from the United States, regardless of who is making them.
>
> Proponents of the bill, and much of news coverage, are portraying the vote as a battle between liberals (in the 2008 edition of the Bush GOP Dictionary that means "lily-livered appeasers of terrorism") and conservatives (patriots who understand the threat to America and have "nothing to hide and therefore nothing to fear").
>
> First, there is no position more conservative than fighting to protect the rights and liberties enshrined in the Bill of Rights, and nothing more radical than trying to undermine them.
>
> Second, anyone with an elementary-school understanding of American history can recite cases in which the government spied on, harassed and even imprisoned people who did nothing more than exercise their constitutional right to express their political beliefs.
>
> This bill was not a compromise, as the spinners would have it. It was a bad bill. Period. Democrats who voted for it did so primarily because they were afraid to vote against a "national security bill" in an election year.
>
> [link to roll call vote deleted here]
>
> All of the Republicans voted for the bill — except for John McCain, who was too busy campaigning to cast a vote on a bill that many of his fellow Republicans, including President Bush, claimed was one of the most important national security bills of our time.

> Senator Barack Obama, who had once promised to filibuster against immunity for the telecommunications companies, executed a deeply distressing pivot in recent weeks, hewing to the "best we could do" line that was adopted by many Democrats. Today, he voted to cut off debate on the bill, and then voted for its final passage.
>
> Fortunately, Mr. Obama seemed to have no influence over Democrats who opposed the bill. None of them joined him in changing their positions.

Editorial Board, "The Wiretapping Bill: President Bush, and Fear, Lead the Senate Off a Cliff," *The New York Times,* (9 July 2008 16:35 EDT)
http://theboard.blogs.nytimes.com/2008/07/09/the-wiretapping-bill-president-bush-and-fear-lead-the-senate-off-a-cliff/

Later in the day, *The New York Times* reported:

> The [FISA Amendments] issue put Senator Barack Obama of Illinois, the presumptive Democratic nominee, in a particularly precarious spot. After long opposing the idea of immunity for the phone companies in the wiretapping operation, he voted for the plan on Wednesday. His reversal last month angered many of his most ardent supporters, who organized an unsuccessful drive to get him to reverse his position once again. And it came to symbolize what civil liberties advocates saw as "capitulation" by Democratic leaders to political pressure from the White House in an election year.
>
> ....
>
> Liberal Democrats in the Senate, led by Senators Feingold and Christopher J. Dodd of Connecticut, sought in vain to pare down the proposal. An amendment sponsored by Mr. Dodd to strip the immunity provision from the bill was defeated, 66 to 32.
>
> Two other amendments were also rejected. One, offered by Senator Arlen Specter, Republican of Pennsylvania, would have required that a district court judge assess the legality of warrantless wiretapping before granting immunity. It lost by 61 to 37. The other, which would have postponed immunity for a year pending a federal investigation, was offered by Senator Jeff Bingaman, Democrat of New Mexico. It was defeated by 56 to 42.
>
> Lawyers involved in the lawsuits against the phone companies promised to challenge the immunity provision in federal court, although their prospects appeared dim.
>
> "The law itself is a massive intrusion into the due process rights of all of the phone subscribers who would be a part of the suit," said Bruce Afran, a New Jersey lawyer who represents several hundred plaintiffs in one lawsuit against Verizon and other companies. "It is a violation of the separation of powers. It's presidential election-year cowardice. The Democrats are afraid of looking weak on national security."

Eric Lichtblau, "Senate Approves Bill to Broaden Wiretap Powers," *The New York Times* (early version posted night of 9 July 2007) http://www.nytimes.com/2008/07/10/washington/10fisa.html

This explanation in the *New York Times* of *why* Democrats "capitulated" to President Bush on the FISA Amendments Act of 2008 (i.e., Democrats did not want to be called weak on national security during an election year) is the same reason that Democrats have offered little resistance to any of Bush's security programs, beginning with the PATRIOT Act in 2001.

Approximately 23 hours after the Senate passed H.R. 6304, President Bush signed the bill at a ceremony at the White House, where he gave the following speech:

> Thank you. Welcome to the Rose Garden. Today I'm pleased to sign landmark legislation that is vital to the security of our people. The bill will allow our intelligence professionals to quickly and effectively monitor the communications of terrorists abroad while respecting the liberties of Americans here at home. The bill I sign today will help us meet our most solemn responsibility: to stop new attacks and to protect our people.
>
> Members of my administration have made a vigorous case for this important law. I want to thank them and I also want to thanks the members of the House and the Senate who've worked incredibly hard to get this legislation done. Mr. Vice President, welcome.
>
> Respect the members of the Senate and the House who've joined us — Senate Republican Whip Jon Kyl; John Boehner, House Republican Leader; Roy Blunt, House Republican Whip. I do want to pay special tribute to Congressman Steny Hoyer, House Majority Leader, for his hard work on this bill. I thank so very much Senator Jay Rockefeller, Chairman of the Senate Select Committee on Intelligence, and Senator Kit Bond, Vice Chairman, for joining us. I appreciate the hard work of Congressman Silvestre Reyes, Chairman of the House Permanent Select Committee on Intelligence, and Congressman Pete Hoekstra, Ranking Member. I also welcome Congressman Lamar Smith, Ranking Member of the House Judiciary. I thank all the other members of the House and Senate who have joined us. I appreciate your very good work.
>
> I welcome Attorney General Michael Mukasey, as well as Admiral Mike McConnell, Director of National Intelligence. I appreciate other members of the administration who have joined us. I want to thank the congressional staff who are here, and all the supporters of this piece of legislation.
>
> Almost seven years have passed since that September morning when nearly 3,000 men, women and children were murdered in our midst. The attack changed our country forever. We realized America was a nation at war against a ruthless and persistent enemy. We realized that these violent extremists would spare no effort to kill again. And in the aftermath of 9/11, few would have imagined that we would be standing here seven years later without another attack on American soil.
>
> The fact that the terrorists have failed to strike our shores again does not mean that our enemies have given up. To the contrary, since 9/11 they've plotted a number of attacks on our homeland. I can remember standing up here — I receive briefings on the very real and very dangerous threats that America continues to face.
>
> One of the important lessons learned after 9/11 was that America's intelligence professionals lacked some of the tools they needed to monitor the communications of terrorists abroad. It is essential that our intelligence community know who our enemies are talking to, what they're saying, and what they're planning. Last year Congress passed temporary legislation that helped our intelligence community monitor these communications.
>
> The legislation I am signing today will ensure that our intelligence community professionals have the tools they need to protect our country in the years to come. The DNI and the Attorney General both report that, once enacted, this law will provide vital assistance to our intelligence officials in their work to thwart terrorist plots. This law will ensure that those companies whose assistance is necessary to protect the country will themselves be protected from lawsuits from past or future cooperation with the government. This law will protect the liberties of our citizens while maintaining the vital flow of intelligence. This law will play a critical role in helping to prevent another attack on our soil.

> Protecting America from another attack is the most important responsibility of the federal government — the most solemn obligation that a President undertakes. When I first addressed the Congress after 9/11, I carried a badge by the mother of a police officer who died in the World Trade Center. I pledged to her, to the families of the victims, and to the American people that I would never forget the wound that was inflicted on our country. I vowed to do everything in my power to prevent another attack on our nation. I believe this legislation is going to help keep that promise. And I thank the members who have joined us. And now it's my honor to sign the bill.

George W. Bush, "President Bush Signs H.R. 6304, FISA Amendments Act of 2008," (10 July 2008, 13:17 EDT) http://www.whitehouse.gov/news/releases/2008/07/20080710-2.html

The passage of the FISA Amendments Act of 2008 by Congress and the signature by the President is *not* the end of this legislation. Litigation has already been filed in federal courts to test the constitutionality of this Act. See my remarks below, beginning at page 79.

My Opinion on H.R. 6304

I do not understand how H.R. 6304 is a compromise on the critical issue of immunity for telecoms. The executive branch will certainly issue letters to each of the telecom companies that participated in the illegal Terrorist Surveillance Program, and — under the so-called compromise bill — the judge hearing the civil cases would be retroactively forced to dismiss the litigation. This is effectively absolute immunity for the telecoms and thus *not* a compromise on immunity.

I find it ironic for two reasons that the U.S. Congress would write and approve a statute that gives legal significance to the attorney general's certification that George Bush asked the telecoms to engage in the Terrorist Surveillance Program (TSP). First, Bush never attended law school, so he is *not* a credible authority on the legality of surveillance. Second, Bush's attorney general at the time the TSP was begun, Dan Ashcroft, believed that the TSP was *not* lawful.[78] Therefore, a letter issued by the current attorney general stating that the TSP was "determined to be lawful" should have no credibility. The ultimate legality of some activity should always be a matter for the courts to decide.

Moreover, the telecom firms being sued are megacorporations that knew, or should have known, that warrantless wiretaps are both *un*constitutional and *un*lawful. These telecom megacorporations should *not* have relied on the legal opinions of the government that Bush's TSP was legal.

If President Bush were really confident that his wartime powers allowed him to ignore federal statutes on wiretapping, then Bush would *not* be demanding immunity for telecom companies who assisted in Bush's Terrorist Surveillance Program.

---

[78] See my separate essay on the Terrorist Surveillance Program at http://www.rbs0.com/TSP.pdf .

President Bush's repeated insistence on retroactive immunity for telecoms, and his concurrent threat to veto any surveillance legislation that lacked retroactive immunity, seems to have pushed Congress into including the retroactive immunity. This is strange, because the Democrats have a majority in both the House of Representatives and the Senate, so the Democrats *could* have simply refused to pass any surveillance legislation. The first surveillance orders approved by the Foreign Intelligence Surveillance Court under the Protect America Act would then expire in August 2008. Sometime thereafter, President Bush would probably decide that a compromise was desirable and drop his demands for retroactive immunity for telecoms, in order to pass legislation that would broaden the ability of the government to conduct surveillance. Alternatively, the next president —sometime after 20 January 2009 — could propose a compromise. Instead of these scenarios that would protect civil liberties, the Democrats in Congress appear to have capitulated to Bush's demands, so that Republicans would not accuse Democrats of being soft on terrorism in the November 2008 election.

The amendments to FISA during July 2007 to July 2008 can be put in a historical context as further weakening of the plain meaning of the Fourth Amendment to the U.S. Constitution, to assist either law enforcement or acquisition of foreign intelligence, and to erode legal rights of private individuals.

Litigation

On 10 July, immediately after President Bush signed the FISA Amendments Act of 2008, the ACLU filed litigation in federal court in New York City that challenged the constitutionality of the surveillance. In the initial complaint, the ACLU alleged as causes of action:

> 104. The challenged law violates the Fourth Amendment because it authorizes defendants to acquire the constitutionally protected communications of U.S. citizens and residents without identifying the people to be surveilled; without specifying the facilities, places, premises, or property to be monitored; without observing meaningful limitations on the retention, analysis, and dissemination of acquired information; without obtaining individualized warrants based on criminal or foreign intelligence probable cause; and without making prior administrative determinations that the targets of surveillance are foreign agents or connected in any way, however tenuously, to terrorism.
>
> 105. The challenged law violates the First Amendment by substantially burdening a broad range of lawful expressive activity without adequate justification and by authorizing defendants to acquire constitutionally protected communications without meaningful judicial oversight.
>
> 106. The challenged law violates Article III by requiring the FISC to rule on questions that do not constitute cases or controversies.
>
> 107. The challenged law violates the principle of separation of powers by allowing the government to continue surveillance activities even if the FISC has held those activities be illegal.

Amnesty International, et al. v. John McConnell, et al., Complaint at ¶¶ 104-107 (S.D.N.Y.).

For more information on *Amnesty International, et al. v. John McConnell, et al.,* see the American Civil Liberties Union website at: http://www.aclu.org/safefree/nsaspying/faachallenge.html .

The legal challenge to constitutionality of the retroactive immunity for telecoms will be argued by attorneys for the Electronic Freedom Foundation in *Hepting v AT&T* (N.D.Calif. MDL Nr. 06-1791). I think it is arguable that such retroactive immunity is an unlawful taking of a property right from plaintiffs who sued for damages under statutes that were valid at the time of the TSP was conducted — which taking is a violation of the Fifth Amendment to the U.S. Constitution.

In reading comments posted by people on the internet, as well as speeches by some Congressmen,[79] I notice that some people have condemned the retroactive immunity as unconstitutional, because it is an *ex post facto* law. They are wrong about retroactive immunity being an *ex post facto* law. The U.S. Supreme Court has held that the constitutional prohibition against *ex post facto* laws only applies to retroactive punishment. See, e.g., *Carmell v. Texas,* 529 U.S. 513, 521-525 (2000). The retroactive immunity for telecoms in the FISA Amendments Act of 2008 is an immunity — *not* a punishment. Furthermore, the retroactive immunity for telecoms applies to damages in a civil action — *not* a punishment for a crime. Therefore, for these two reasons, the retroactive immunity for telecoms does *not* violate the constitutional prohibition against ex post facto laws.

Hepting v. AT&T is the consolidation of approximately forty cases filed in federal courts nationwide. For more information on these cases, see the Electronic Freedom Foundation website at: http://www.eff.org/cases/att . For more information on *Hepting v. AT&T* see the Electronic Freedom Foundation website at: http://www.eff.org/cases/hepting .

---

[79] For example, Ron Paul, M.D. — a member of the U.S. House of Representatives and a Republican presidential candidate in early 2008 — asserted in a speech on 20 June 2008 that H.R. 6304 was unconstitutional because it was an ex post facto law.

Conclusion

The explanation of *why* Democrats capitulated to President Bush on the FISA Amendments Act of 2008 (i.e., Democrats did not want to be called weak on national security during an election year, or the fear of being blamed for not helping the government prevent another terrorist attack) is the same reason that Democrats have offered little resistance to any of Bush's security programs, beginning with the PATRIOT Act[80] in 2001, and continuing with the intrusive searches of airline passengers.[81]

Six years after the PATRIOT Act debacle, the same motivation appeared during the hasty passage of the Protect America Act of 2007. It's a bad motivation. If the government legitimately needs changes in statutes authorizing surveillance, those changes should be calmly and rationally discussed over an interval of at least months, and not pushed through Congress in a few days or few weeks.

When I began this essay in early August 2007, I hoped to inform citizens and encourage opposition to proposals in the U.S. Congress to increased surveillance of American citizens. Given the trivial number of hits on this essay through November 2007,[82] my intention now is simply to chronicle how U.S. citizens abandoned their privacy rights through apathy and inaction. Maybe someday people in the USA will wonder how it became legal to wiretap people without a warrant that seems to be required by the Fourth Amendment.

This document is at **www.rbs0.com/PAA.pdf**
first posted 8 Aug 2007, revised 14 Jul 2008

return to my homepage at http://www.rbs0.com/

---

[80] Standler, Brief History of the USA PATRIOT Act of 2001, http://www.rbs0.com/patriot.pdf , 43 pp., (Sep 2007).

[81] Standler, Legal Aspects of Searches of Airline Passenger in the USA, http://www.rbs2.com/travel.pdf 64 pp., (Dec 2004).

[82] This essay has been indexed in Google since 4 Oct 2007. This essay received an average of only 3.2 hits/day from 6 Oct 2007 to 16 Nov 2007. From 6 Oct 2007 to 4 July 2008, this essay received an average of 4.5 hits/day. I have dozens of essays that have more than 30 hits/day.