

Protect America Act of 2007: Another Hastily Passed Statute

Copyright 2007 by Ronald B. Standler

no copyright claimed for works of the U.S. Government

Table of Contents

Introduction 2

News During July/August 2007 2
 after the approval on 5 Aug 2007 5

How the Protect America Act Was Passed 8

Text of Protect America Act of 2007 9
 my comments on the Protect America Act 9

News During September 2007 12
 14 Sep 2007 13
 19 Sep 2007 13
 "Fact Sheet" 15

RESTORE Act of 2007 (H.R. 3773) 17

Senate Bill 20

Conclusion 22

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

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".

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 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).

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”.

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.

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 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.

“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

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).

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 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., ACLU¹⁰) 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.

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

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).

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 —

- (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.

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.

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”.

¹⁴ Protect America Act, § 105B(a)(3).

(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 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.

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

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).

- 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 letter¹⁶ 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:

....

... 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.

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

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 not 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 telecommunications 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).

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 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)

House Majority Leader Steny Hoyer (D-Md.) said on 9 Oct 2007 that he would be willing to grant telecomm 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.¹⁷ Because the executive branch has consistently refused to provide Congress with details of this illegal surveillance program,¹⁸ 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 telecomm 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.

¹⁷ Pamela Hess, “Dems Opens Door for Immunity in Spy Bill,” Associated Press (18:00 EDT 9 Oct 2007).

¹⁸ See my essay at <http://www.rbs0.com/TSP.pdf> .

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.**¹⁹

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 relations²⁰ with a key ally in NATO and in the global war on terror.

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.

¹⁹ Boldface added by Standler.

²⁰ Turkey was then threatening to invade northern Iraq.

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 telecommunications 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 telecommunications 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 telecommunication 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 telecomm 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 telecomm companies should consistently be very careful of their legal obligations to protect the privacy of their customers' communications. Moreover, the telecomm companies have large legal departments that could easily challenge unlawful subpoenas and other demands in court.

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).

Senate Bill

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

The draft bill would direct civil courts to dismiss lawsuits against telecommunications 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>

Conclusion

The fear of being blamed for not helping the government prevent another terrorist attack was part of the motivation of Congress in hastily passing the PATRIOT Act in October 2001, as discussed in my essay at <http://www.rbs0.com/patriot.pdf>.

Six years later, 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.

This essay is the least popular²¹ of a series of five essays that I wrote during August/September 2007 on (1) the Foreign Intelligence Surveillance Act (FISA), (2) President Bush's illegal Terrorist Surveillance Program, (3) National Security Letters, (4) a history of the Patriot Act of 2001, and (5) this essay. Consequently, I will not be revising this essay often.

This document is at www.rbs0.com/PAA.pdf
revised 21 Oct 2007

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

²¹ This essay received an average of only 2.7 hits/day during 6-19 Oct 2007. I have several dozens of essays that receive more than 20 hits/day.