



**American Civil Liberties Union
Statement for the Record**

**Before the Senate Permanent Select Committee on Intelligence
Regarding the Department of Justice's Proposed Foreign Intelligence
Surveillance Act Amendments**

**Submitted by Caroline Frederickson,
Director, ACLU Washington Legislative Office**

May 1, 2007

AMERICAN CIVIL
LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

CAROLINE FREDRICKSON
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

OFFICERS AND DIRECTORS
NADINE STROSSEN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

KENNETH B. CLARK
CHAIR, NATIONAL
ADVISORY COUNCIL

RICHARD ZACKS
TREASURER

On behalf of the American Civil Liberties Union, and its hundreds of thousands of activists and members, and fifty-three affiliates nationwide, we urge you in the strongest terms to oppose legislation drafted by the Department of Justice (“DOJ”) that would effectively pardon telecommunication companies for illegal behavior over the last five years and rewrite the Foreign Intelligence Surveillance Act (“FISA”) to facilitate further warrantless surveillance on American soil.¹

Only a few short weeks ago this Congress was finally informed about the DOJ’s use of National Security Letters (“NSLs”) and found that this power – no longer limited to collecting information on terrorists – is being abused to collect vast amounts of data on innocent Americans that is stored indefinitely in massive federal databases accessible by tens of thousands of users. Instead of contemplating ways to exponentially increase those powers, this Congress should be figuring out ways to rein them in, protect constitutional rights, and focus our antiterrorism resources on suspected terrorists.

While the Administration claims that the changes it proposes to FISA would “modernize” it, they would better be described as changes to gut the judicial oversight mechanisms carefully crafted to prevent abuse, while expanding the universe of communications that can be intercepted under FISA. They would allow the intelligence community to return to the tarnished practices of the 1970’s and earlier, when warrants were largely optional and abusive spying

¹ FISA Modernization Provisions of the Proposed Fiscal Year 2008 Intelligence Authorization, Title IV, available at <http://www.fas.org/irp/news/2007/04/fisa-proposal.pdf>.

was not limited to subjects who had done something wrong. In fact, despite numerous hearings about “modernization” and “technology neutrality” over the last year, the Administration has not publicly provided Congress with a single example of how current standards in FISA have either prevented the intelligence community from using new technologies or proven unworkable for the personnel tasked with following them. Congress should not approve sweeping new authorities without such a showing by the Administration.

Granting Immunity to the Companies Who Facilitated Illegal Spying Is Inappropriate.

We are disappointed and very concerned that the first hearing in this Congress to address five years of illegal spying would consider a legislative, congressional pardon for the telecommunication companies that broke the law. Congress’ priority should be a full and public airing of the government’s illegal spying, including determining exactly how many people the government and telecommunications companies spied on for five years and what is now being done with records of those phone calls; holding those who broke the law responsible; and then fashioning a response to make sure these grave violations of privacy never happen again.

This Committee should be holding a hearing to determine how to contract, rather than expand, the government’s illegal spying to bring it into conformity with the law and Constitution; yet the Administration’s proposed bill proposes an unwise new power grab. For example, sections 408 and 411 attempt to terminate all pending and future actions against the NSA’s warrantless wiretapping in any court anywhere, except for a FISA court whose judges are handpicked by the Chief Justice. The US District Court in the Eastern District of Michigan recently ruled that the president’s program to wiretap Americans without warrants is illegal and unconstitutional. The Administration, having lost in one forum, asks Congress to give it a new one.

The Administration’s proposed bill is objectionable because it eliminates independent court review of the Administration’s past and future spying and eavesdropping requests. The proposed bill would allow the administration to rip that case from that court’s jurisdiction, and ship other federal and state court challenges off for secret hearings and proceedings before the FISA Court of Review, which has handled only one case in nearly 30 years. And, only the government would be allowed to appeal to the U.S. Supreme Court to seek review of any adverse ruling by that Court. The bill abrogates rights granted under state law as well, by stopping state law enforcement and regulatory agencies from enforcing local consumer privacy laws that may offer more protection than federal law. Beyond the mandatory transfer provision, the bill allows companies to assert immunity for complying with secret requests of the AG under provisions that state that:

No action shall lie or be maintained in any court, and no penalty, sanction or other form of remedy or relief shall be imposed by any court or any other body, against any person for the alleged provision to an element of the intelligence community of any information (including records or other information pertaining to a customer), facilities or any other form of assistance during the period of time beginning on September 11, 2001, and ending on the date that is the effective date of this Act....²

This exemption is both overbroad and unwise.

If Congress grants these companies immunity for violating longstanding privacy laws, what incentive will they have to follow them in the future? Without consequences, these laws ring hollow, and end up being a mere suggestion instead of a mandate or bright line requirement. For nearly 30 years, FISA has included a clear liability and immunity scheme that creates bright lines for telecommunication companies: if they turn over private information in response to a legal demand from the government, they are 100 percent immune from any liability. However, if they cut a side deal with the executive branch in an attempt to bypass the duly enacted laws of this Congress, they are liable to the consumers whose privacy they have betrayed. If our government wants to “improv[e] the way the United States does business with communications providers,” as the DOJ claims on the fact sheet it conveyed to Congress with its legislative proposal,³ it should return to the days of clear cut requirements, instead of enticing those providers to break the law with the promise of a congressional pardon after the fact.

Finally, this rush to retroactive immunity for an entire industry in the absence of full and thorough airing of the facts is unprecedented. Numerous leaders in this Congress have promised to investigate the President’s illegal Terrorist Surveillance Program. It is highly unlikely those investigations will yield any useful information if Congress starts the process giving the companies a get out of jail free card.

Changing Technical Definitions in FISA to Undercut the Warrant Requirement of the Fourth Amendment.

Sections 401 and 402 of the proposed Administration bill alter FISA’s current definitions of “electronic surveillance” to greatly reduce the number

² *Id.* at § 408 (a).

³ FACT SHEET: TITLE IV OF THE FISCAL YEAR 2008 INTELLIGENCE AUTHORIZATION ACT, MATTERS RELATED TO THE FOREIGN INTELLIGENCE SURVEILLANCE ACT, Office of Public Affairs, Apr. 13, 2007.

and scope of spying activities that are subject to court review. The DOJ's Office of Public Policy, claims these changes are necessary "to account for the sweeping changes in telecommunications technology that have taken place."⁴ This includes making FISA "technology neutral" by deleting the longstanding requirement that all wire communications into and out of the U.S. are accessed only on the basis of a warrant.⁵

These changes have absolutely nothing to do with "modernizing" FISA – rather, they substantially and unconstitutionally declare whole categories of communications exempt from the warrant requirement, namely, 1) international phone calls, even when made in the U.S. by a U.S. person, and 2) phone calls collected as a part of a general dragnet, as long as no one U.S. person was targeted. Technology may have changed, but the Fourth Amendment has not. Except for a few very narrow circumstances, warrants are required to listen to phone calls or otherwise access the content of a communication and we ask this committee to make sure that requirement remains a cornerstone of FISA.

The Justice Department has claimed that this proposal restores the "original intent" of the law but the legislative history makes clear that Congress intended FISA to prevent the National Security Agency ("NSA") from engaging in just the sort of electronic dragnet this bill permits. The Church Committee's discovery that the NSA was improperly monitoring millions of international telegrams to and from Americans and U.S. businesses through "Operation Shamrock" led a bipartisan coalition in Congress to enact FISA to prevent future presidents from intercepting the "international communications of American citizens whose privacy ought to be protected under the Constitution" ever again. See, Book III of the Final Report on Intelligence Activities and the Rights of Americans, Apr. 23, 1976, at pp. 735-36.

This draft proposal would also allow the NSA to acquire Americans' private e-mail messages if the government says it does not know that "the sender and all intended recipients are located within" the U.S. This provision would authorize the NSA to vacuum up all of the international e-mails of Americans. The NSA would likely capture purely domestic e-mails in this program as well because, as Central Intelligence Agency Director General Michael Hayden said, "there are no zip codes on the world wide web." For example, if an American in New York City sends an email to his sister in San Francisco, that communication could be intercepted without a warrant because it went through Canada. This bill would allow the NSA to keep these "accidentally" captured communications. Once "lawfully" acquired under

⁴ *Id.*

⁵ Nearly identical language was introduced in the House and Senate last Congress. H.R. 5825, 109th Cong. (2nd Sess. 2006); S. 3931, 109th Cong. (2nd Sess. 2006).

this authority, the administration could — and most likely already does — interpret the statute to allow the NSA to target any particular American’s communications from such a dragnet for data mining, analysis, or dissemination. Because this activity is not considered “electronic surveillance” under the new language proposed in this bill, a substantial number of innocent Americans’ private conversations would be exempt from the oversight of the court and congressional reporting. While the bill retains FISA’s minimization rules, those rules only apply to “electronic surveillance” which is redefined in this draft bill to exclude innocent Americans’ international conversations and e-mails. Thus, this supposed protection is illusory.

The proposal also amends FISA to require a warrant only when a surveillance device acquires conversations by “intentionally directing the surveillance” at a specific U.S. person. Under the Justice Department’s draft bill, if the NSA’s surveillance devices — as distinguished from its data mining devices — are directed at wholly domestic conversations but not at a specific American, no warrant need be sought. FISA’s targeting language is a shield against sweeping up the conversations of innocent Americans. The proposed language turns this into a sword to cut down statutory protections for our Fourth Amendment rights.

Stripping Non-citizens – And Anyone Who Comes Into Contact With Them -- of the Protection of a Warrant.

Section 402 greatly reduces the protection against government spying on non-U.S. persons and puts at risk the privacy of any U.S. persons who may come into contact with them. Current law has a narrow exception to the warrant requirement that allows the Attorney General to issue wiretap orders for 1) communications that are exclusively between foreign powers, such as contact between embassies and foreign countries, or 2) technical intelligence from property under the exclusive control of a foreign power, when either of these activities has “no substantial likelihood that the surveillance will acquire the contents of any communication to which a United States person is a party.”⁶ Section 402 strips both the requirement that communications or technical intelligence be exclusively between or on the property of a foreign power, and the requirement that there be no substantial likelihood that a U.S. person be caught up in the surveillance. This greatly increases the chances, and in fact expressly allows, that a U.S. person may have his or her communications scooped up in surveillance of foreign powers.

This bill even expands the definition of “agent of a foreign power” to include anyone in the U.S. who is not a citizen, lawful permanent resident or company incorporated in the U.S. who “is expected to possess, control,

⁶ 50 U.S.C. § 102 (a).

transmit or receive foreign intelligence information” in the U.S. This is dangerous because FISA’s definition of “foreign intelligence” is not limited to international terrorism but includes information about the “national defense,” “security,” or “conduct of the foreign affairs” of the U.S., which has been construed to include trade matters. All foreign journalists and foreign-owned media companies, financial institutions, airlines, telecommunications companies, or Internet Service Providers (ISPs) could be considered “agents of a foreign power” whose communications could be seized without any suspicion of wrongdoing, just because they all can reasonably be expected to “possess,” “transmit” and “receive” foreign intelligence information within the United States. Communications of many foreign businesses in the U.S. transmit or hold information that involves foreign affairs, particularly foreign media and financial institutions. All the Administration would have to show to get a FISA order to search or wiretap these entities for an entire year is that these entities possess such information, not that they have done or are expected to do anything improper.

Expands Disclosure of Information Obtained in Warrantless Searches of Homes and Businesses

Section 409 makes dangerous changes to the provisions of FISA that allow the Attorney General to authorize physical searches in the absence of a warrant in times of emergency.⁷ First, it expands the period of time the Attorney General has to search a home without judicial approval from three days to a full week.

Second, and most importantly, section 409 allows the Attorney General to share information obtained in emergency physical searches even when the court later finds that the search was wrongly conducted. The current emergency search statute bars the government from using or distributing any information or evidence collected during an emergency search if subsequent judicial review denies the retroactive warrant.⁸ The only exception is when that information “indicates a threat of death or serious bodily harm to any person.”⁹ This ban on later use operates to deter the government from conducting “emergency” searches in cases where no true emergency exists or when the government knows it will not be able to meet the subsequent warrant requirements.

⁷ 50 U.S.C. § 1821, et. Seq.

⁸ 50 U.S.C. § 1824 (e) (4).

⁹ *Id.*

Section 409 greatly expands the threat of death exception and allows the government to use and disseminate this information or evidence, which in retrospect was wrongly collected, based on the incredibly low standard that it “*is significant foreign intelligence information.*” FISA already defines “foreign intelligence information” extremely broadly, including any information that allows the United States to protect itself against a potential attack or international terrorism.¹⁰ This is so broad that the government would be authorized to retain, use and distribute virtually all information it collects under the guise of an “emergency” physical search, even if a court later finds that there was no basis whatsoever in the law to claim emergency circumstances.

If these changes are enacted, the government will have no incentive to limit its use of this authority. Some may claim such a scenario is highly unlikely, and that our intelligence professionals should be given the benefit of the doubt. However, the Inspector General’s report recently confirmed that the FBI routinely lied about emergencies to access telecommunication records. This section will simply grant legislative approval of that practice – except in far more serious situations: the highly sensitive searches of homes, businesses, cars or other physical space. Concerns about the DOJ concocting emergencies can no longer be dismissed as fantastical, paranoid hyperbole. The American public has recently learned from the DOJ’s Inspector General that fabricated “emergencies” led to the issuance of so-called “exigent letters” where no emergency existed. It would be unwise for Congress to follow that revelation of abuse of authority with a new grant of authority to use information gathered from searches after it was determined the search was improperly grounded. If Congress authorizes such use of wrongly gotten search results, how long will it be before a subsequent Inspector General’s report documenting the abuse of such an authority to conduct fishing expeditions?

Other Deletions of Checks and Balances.

¹⁰50 U.S.C. § 1801(e) defines “foreign intelligence information” as:

(1) information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against—

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

(2) information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to—

- (A) the national defense or the security of the United States; or
- (B) the conduct of the foreign affairs of the United States.

A number of other provisions in this proposed bill appear to have no purpose other than to reduce the checks and balances in FISA. Section 405 extends the maximum time period for a FISA warrant for a non-U.S. citizen from 120 days to one year, and extends the duration of emergency wiretap orders that allow the government to surveil suspects without prior judicial review from 72 hours to one week. Section 410 extends the period of emergency trap and trace orders from 48 hours to one week. Again, the Administration has provided no evidence that the current time limits are unworkable. While the Justice Department has requested “flexibility,” and justifies less court review under the guise of saving time, periodic and timely review of orders is necessary to ensure that the government does not continue spying on people in the absence of some evidence that the person is a terrorist.

Sections 404 and 405 further reduce judicial oversight. They amend the application and order process so that the DOJ no longer need provide either meaningful descriptions of key intelligence activities, such as “the nature of the information sought and the type of communications or activities to be subjected to the surveillance,”¹¹ or “a statement of the means by which the surveillance will be effected and a statement whether the physical entry is required to effect the surveillance.”¹² Instead, if enacted, the DOJ would be empowered to simply produce a summary, reducing the information a court may use to determine whether certain types of surveillance are appropriate.

Conclusion: this Committee Should Hold Hearings to Document and Reform the Government’s Abusive Spying and Should Refrain from Adopting the Administration’s Proposed Legislation.

The proposed amendments to FISA do not “modernize” intelligence-gathering activities. They simply declare certain communications outside of the warrant requirement and reduce judicial oversight, in violation of the Fourth Amendment. In light of recent revelations that the government is gravely abusing the authorities it already has, allowing this exponential increase in spying authority would not only be unconstitutional, but irresponsible. We urge you to resist any such expansion.

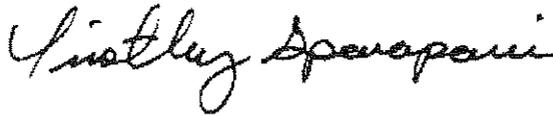
¹¹ 50 U.S.C. § 1804 (a) (6).

¹² *Id.* at § (a) (8).

Sincerely,

A handwritten signature in black ink, appearing to read 'Caroline Fredrickson'. The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Caroline Fredrickson
Director, Washington Legislative Office

A handwritten signature in black ink, appearing to read 'Timothy Sparapani'. The signature is cursive and somewhat stylized, with a prominent 'T' and 'S'.

Timothy Sparapani
Legislative Counsel for Privacy Rights