

Facts v. Fiction: The Justice Department's "New" Re-Write of FISA

*Prepared by Lisa Graves, Deputy Director, Center for National Security Studies (4-18-07)
For further information, contact Lisa Graves or Kate Martin, Director of CNSS, at 721-5650*

The Justice Department's "Fact Sheet" about its 2007 FISA bill omits the most important effect of its proposed changes: it would permit the government to acquire millions of Americans' international phone calls and e-mails without a warrant, so long as it vacuumed up the contents of these communications en masse, rather than targeting for acquisition the calls of a particular individual in the United States. And it would permit the government to then sort and analyze all those communications and listen to and distribute whichever ones it chose, in secret, with no warrant or meaningful oversight whatsoever. This would be a dramatic and drastic change to current law. Under the guise of "tech neutrality," the proposal would neutralize important protections in current law and authorize the warrantless surveillance of virtually all communications by Americans with anyone, including other Americans, located overseas.*

The bill would permit the vacuuming of all international communications of Americans.

The bill would allow wholesale vacuuming of the international communications of American individuals and businesses by the NSA without judicial approval under FISA. For the content of domestic communications, these would require a warrant under FISA, if the government has "reason to believe" the sender and all recipients are actually located in the US. It is noteworthy that administration officials have said in recent testimony that "there are no zip codes on the world wide web" and that a cell phone number does not necessarily indicate where a particular phone call is made—so the administration may intend this new language to support a statutory presumption that the senders and receivers of some number of domestic e-mails and cell calls are not located in the US and are thus not subject to the warrant requirement. It also appears that the changes to FISA's definitions could create a loophole for surreptitious video surveillance of private spaces without a warrant being required by the foreign intelligence statute. It is also noteworthy that the administration signaled last year that it believes that "surveillance" does not include devices used for analyzing, selecting out, or mining content or data lawfully acquired, and the bill would vastly expand what can be "lawfully" acquired without warrants under FISA.

The bill's changes are not modest updates to modernize FISA and increase privacy, but would dramatically change the law and substantially weaken civil liberties protections in current law. In 2000, General Hayden testified that FISA's "privacy framework is technology neutral and does not require amendment to accommodate new communications technologies." The recent administration claims regarding this proposal stand in stark contrast to that accurate admission.

Accordingly, the Center for National Security Studies strongly opposes this proposed legislation.

* This radical change is buried in the technical amendments to the sophisticated definition of "electronic surveillance" in FISA, which can be unpacked as follows. Current FISA law bars the warrantless "acquisition" of the content of domestic communications--whether they occur by *wire or radio*--as well as "information," if it is intentionally acquired through other means, such as "bugging" or video devices, where a person has a reasonable expectation of privacy. FISA also bars warrantless "acquisition" in the US of the contents of *wire* communications "to or from a person in the United States," meaning domestic or international, whether a known US person is the target of the acquisition or not. It also bars the surveillance of the contents of the *radio* communications to or from a known US person in this country by intentionally "targeting" that person. (The statute is silent about acquiring international *radio* communications without intentionally targeting a particular US person, although at the time FISA was passed Congress recognized that Americans do have Fourth Amendment rights in the privacy of the content of such communications.) By repealing or modifying these statutory prohibitions, the bill would suddenly allow the warrantless acquisition of the content of all international telephone, e-mail or other communications sent by any technology to or from Americans so long as it is acquired en masse rather than by *initially* targeting a particular US person's communications.

DOJ Fact Sheet: "For over two decades, the Foreign Intelligence Surveillance Act (FISA), as amended, has served as an important framework in the nation's ability to collect foreign intelligence information, while simultaneously protecting the civil liberties of Americans. FISA provides the legal framework through which the Intelligence Community lawfully collects information about those who pose national security threats to our country. FISA helps those in the Intelligence Community catch spies, international terrorists, and others who seek to do harm to the US, its citizens and its allies."

The Facts about FISA: This law is not just a "tool" or "framework" for electronic surveillance of Americans; it provides "the exclusive" rules for secretly monitoring Americans' conversations and e-mails and searching their homes or offices in the name of foreign intelligence. But the administration deliberately violated these exclusive requirements in the past five years through the NSA's warrantless surveillance program, justified by claims of unchecked presidential power. FISA has not protected Americans' civil liberties, as asserted by the administration, because it was not followed and was treated as optional, rather than constitutionally required.

The secret decision of a single FISA court judge on some part of the NSA program earlier this year does not demonstrate that the law is now being followed. This is because there is no evidence that the ruling requires the individualized warrants for Americans' conversations called for by the Fourth Amendment and FISA. DOJ has refused to provide this assurance and the administration has said the president still has "inherent" power as Commander-in-Chief to monitor Americans outside the strictures of FISA.

FISA's individual warrant and probable cause requirements, when followed, do help protect against national security threats by ensuring that federal agents are properly focused on suspected agents of a foreign power, like al Qaeda, and Americans conspiring with them--by requiring individual warrants approved by a judge. (FISA also does allow for emergency wiretaps and searches of Americans in the US if a secret warrant is sought shortly thereafter.)

DOJ Fact Sheet: "Today, following over a year of coordinated effort among the Intelligence Community and DOJ a bill is being submitted to Congress to request long overdue changes to FISA. The proposed legislation's core objective is to bring FISA up to date with the revolution in telecommunications technology that has taken place since 1978, while continuing to protect the privacy interests of persons located in the US. This legislation is important to ensure that FISA continues to serve the nation as a means to protect our country from foreign security threats, while also continuing to protect the valued privacy interests and civil liberties of persons located in the US. The Director of National Intelligence, together with the Attorney General, will work with Congress to ensure enactment of this important proposal to keep America safe."

The Facts about the History of "Updating" FISA: This re-write of FISA is not a technological update to FISA. This proposal is not new and it would severely weaken Americans' privacy protections. These ill-advised proposals were part of the controversial White House-backed bills introduced in the last Congress. And they are still bad ideas this year.

FISA has already been modernized, repeatedly, to take into account changes in technology and threats since 1978. Its provisions have been amended dozens of times, with six major amendments since 9/11, including major changes to "Provide Appropriate Tools to Required to Interrupt and Obstruct Terrorism" in the USA Patriot Act passed by Congress in October 2001.

What has not been done, and what this bill tries to do, is unloose the NSA to acquire countless American conversations and e-mails without any judicial approval or individualized suspicion. This bill would redefine what is subject to judicial orders--creating substantial exceptions to statutory warrant requirements and allowing the government free rein to spy on the content of

Americans' international communications, what Congress sought to prevent after it discovered secret surveillance programs like "Operation Shamrock," where the NSA copied virtually every international telegram cabled to or from people in the US. Contrary to the administration's claims about protecting privacy, the bill actually eliminates key provisions and procedures that "protect the valued privacy interests and civil liberties" of people in the US. It is time to reject the administration's boilerplate claims that it is continuing to protect Americans' privacy when the facts rebut such claims, such as these proposals to delete privacy protections, the years of warrantless wiretapping by the NSA in violation of FISA, and the FBI's documented abuse of the already expansive National Security Letter (NSL) powers.

Now is the time for investigation, not legislation, especially legislation such as this.

DOJ Fact Sheet: "The bill would . . . update the definition of electronic surveillance to account for the sweeping changes in telecommunications technology that have taken place. The proposed legislation is technology neutral. In contrast to the 1978 statute, which contains central provisions that are tied to specific communications technologies, this proposal is not tied to specific technology we have today. That way, as telecommunications technology develops over time--which it surely will do--FISA will not run the risk of becoming out of date."

The Facts about "Tech Neutrality": These "modernization" and "tech neutrality" claims are a Trojan horse, cloaking an administration effort to dramatically cut back FISA's warrant requirements for secretly monitoring Americans' communications. As Congresswoman Jane Harman documented, FISA has been modernized repeatedly since 1978, with major changes since 9/11. This bill does not simply eliminate conceptual distinctions between wire and wireless communications—it rips out major protections for Americans' private communications regardless of the technology used. "Modernization" is an innocuous word being used to distract from the expanded warrantless surveillance the President wants made legal through this bill.

These expansions of unchecked power were first proposed last year, after revelations of the White House's illegal warrantless wiretapping. When the 60 pages of proposed changes to definitions and procedures are scrutinized, it is clear the bill seems design to allow much wider acquisition and mining of conversations and communications of Americans without warrants, by cleverly modifying FISA to exclude them from the warrant requirement through complex changes to the definitions of "electronic surveillance" and "content."

The deletions in the bill appear to allow Americans' international calls and e-mails to be scooped up en masse through any technological means (*i.e.*, "tech neutral") so long as a particular American was not targeted in the *initial* "acquisition" or surveillance. Once Americans' international communications would be thus acquired, without a warrant, the subsequent analysis of private personal or business conversations and data would not count as "electronic surveillance" or require a warrant under the statute or the administration's interpretation of it as evinced by its view of what counts as a "surveillance" device. If the NSA believes you and all the recipients of your communications are in the US, a warrant would still be required. However, as noted above, it is not clear how the administration would treat Americans' e-mail accounts or cell phones under this new language about the government having to "reasonably believe" all communicants are in the US for this protection to apply. It is also unclear how the deletion of the catch-all definition in FISA requiring warrants for the intentional acquisition of "information" by other means--which has been interpreted to include video surveillance--would affect judicial oversight of non-audio surveillance in private homes or buildings in the US. It is absolutely crucial that Congress understand completely the consequences of such changes.

The administration will no doubt assert that its internal foreign intelligence "minimization" rules for information gathered that would not fall under the definition of "electronic surveillance" under

FISA 50 USC 1801(f) or (h) provide additional protections for Americans' privacy, but this is little consolation, given the broad mandate for the widespread sharing of intelligence information. Without an external check on broad claims of need or necessity within the Executive Branch, let alone amid claims of plenary presidential power, there is no way to prevent privacy from taking a back seat to the imperative to gather more and more information into intelligence databases.

A sea change like this requires extensive hearings and investigation. The suggestion that these massive changes should be passed this spring is disrespectful of the democratic process.

DOJ Fact Sheet. "The bill would . . . protect civil liberties and privacy interests and improve our intelligence capabilities by focusing FISA on people located in the US. Revolutions in telecommunications technology have brought within FISA's scope communications that Congress did not intend to be covered—and, as a result, extensive resources are now expended obtaining court approval for acquiring communications that do not directly or substantially involve the privacy interests of Americans. Restoring FISA to its original focus will enhance our intelligence capabilities while allowing the Intelligence Community to devote more resources to protecting the privacy interests of people in the US."

The Facts about the Bill's Changes to Privacy-Related Procedures. There are no, zero, amendments to FISA in this bill that add any privacy provisions and, in fact, the bill expressly deletes long-standing privacy protections for the contents of countless American conversations and communications. If the administration simply wanted to clarify that it need not obtain a FISA warrant for conversations between individuals overseas that can be intercepted in the US (so-called "foreign to foreign" communications that have been rerouted through the US by companies), a simple fix to clarify that has been already proposed by both Senator Feinstein and Congresswoman Harman. This bill goes way beyond that fix. Similarly, if the government does not have enough resources to process FISA warrants for searching Americans' conversations or homes in order to protect both security and privacy, it should endorse the proposal by these Members to provide more resources for the FISA process.

Indeed, the essence of DOJ's claim—that the government is so busy getting FISA court orders that it cannot devote enough resources to protecting Americans' privacy—is belied by the facts. For over five years, the administration simply refused to seek court orders for the wiretaps of Americans that the NSA was illegally conducting, even while the President and his Attorney General reassured the American people their privacy was being protected because court orders were being sought. And, for the past three months, the NSA has been operating under a FISA judge's order that is said to have "creatively" interpreted the law to allow such electronic surveillance of people in the US to go forward, with no commitment that these are individualized warrants. This does not constitute extensive resources being expended to get FISA court approval—and, the judge has likely issued only one or two orders related to the so-called "TSP."

Additionally, although the administration has applied to the FISA court for some wiretaps and physical searches beyond this particular warrantless surveillance program (and the court has rarely denied a request), there is no proof that seeking FISA court approval to secretly wiretap or physically search people in the US adversely affects Americans' privacy. And, if protecting privacy requires more resources than have been allocated, then Congress should authorize more funding, not less privacy. The bill does not "restore" the original intent of FISA; it subverts that intent to protect Americans' privacy. This unwise bill should be shelved.

DOJ Fact Sheet. "The bill would . . . improve the way the US does business with communications providers. The country's communications providers are important partners in the ability of the US Government to protect our national security. The bill includes needed

authority both to protect those carriers when they do comply with lawful requests under FISA, and to enable providers to cooperate with authorized intelligence activities.”

The Facts about the Bill's Blanket Immunity: One of the key safeguards built into FISA is the provision that telephone companies and others who intercept Americans' conversations without the judicial warrants required by FISA are potentially criminally liable and may be sued for civil damages. Because FISA provides for secret surveillance, where the targeted individual is unlikely to know of the surveillance, the only check against government violations of the law, is to penalize the communications providers if they do not insist on staying within the law. It is not yet known what the administration told the communications providers that allowed the warrantless NSA surveillance. The administration has refused to provide this information, has blocked the testimony of telecommunications companies and, indeed, is seeking dismissal of the civil lawsuits that are trying to establish responsibility for the illegal surveillance.

This bill seeks to shut down all such inquiry by providing blanket immunity from all civil or criminal penalties for any companies or individuals who may have violated the law, before the facts are even established about their conduct. (The request for immunity, of course, calls into question the administration's repeated claims of complete confidence that the warrantless NSA program was legal. If so, the industry does not need any protection in their lawsuits.)

Moreover, the DOJ "Fact Sheet" omits a key part of the immunity grant. The bill is a full pardon for White House officials and other government agents who knew what FISA required and ignored it anyway. As the White House pointed out in its Statement of Administration Position (SAP) on the Wilson bill last winter (H.R. 5825), this grant of immunity applies to government employees. By the bill's terms, "any person" who provided "assistance" to the intelligence community regarding the warrantless surveillance program, or other classified communications intelligence activities, is immune. This seemingly covers the lawyers in the White House and DOJ who gave their blessing to violations of the law on their theory of presidential power.

The only condition for this blank check immunity from any civil and criminal liability in federal or state courts is that Attorney General Alberto Gonzales certify that the provision of information, facilities or assistance was or even "would have been" intended to protect us, notwithstanding the lack of any ongoing emergency for the past 2,400 plus days. And, FISA already protects companies that comply with court orders by giving them immunity from suit as well as allowing for compensation for lawful assistance. FISA should not be twisted into rewarding the opposite.

It would be impossible to write a broader or more irresponsible grant of immunity. And Congress would be immunizing conduct it has not even investigated yet.

DOJ Fact Sheet: "The bill would . . . streamline the FISA process. Numerous Congressional and Executive Branch reviews of the FISA process have recommended that the FISA process be made more efficient, and the Department of Justice has made major strides in recent years in improving its practices and procedures. The proposal would make several changes to improve further the efficiency of the FISA process, including extending the period of authorization for non-US persons, which will allow the Department and the FISA Court to concentrate more scarce resources to the cases that concern US persons."

The Facts About "Streamlining" FISA Procedures: The bill does contain some provisions that eliminate what the FISA court must be told to authorize a warrant, but in so doing the bill steamrolls, rather than streamlines, the Fourth Amendment's particularity requirements. A far superior approach is providing more resources for improved FISA applications as reflected in the bills by Senator Feinstein (in the bipartisan S. 3877 from the 109th Congress) and Congresswoman Harman (in the strong "LISTEN Act," H.R. 5371). If DOJ were serious about

efficiency and effectiveness rather than simply trying to water down Americans' Fourth Amendment rights under the FISA statute, they would have endorsed these provisions.

Instead, the bill's "summary" provisions seem intended to eliminate privacy safeguards. For example, it is unclear what the administration intends to accomplish by requiring a "summary" description of the place to be searched with a warrant rather than a "detailed" description of the home or business in the US to be physically searched. The requirement of a detailed description is consistent with the Fourth Amendment's command that warrants "particularly" describe "the place to be searched, and the persons or things to be seized." Yet the administration asserts in essence that requiring such particularity or detail detracts from privacy; to the contrary, such particularity helps ensure that the right person's home or office is searched and minimizes the chance that innocent people will have their private domain secretly invaded. (The bill also contains a peculiar and troubling change to allow warrants to search a home *before* it is owned or occupied by a suspected terrorist, which by definition is then a place occupied by an innocent resident whose drawers and papers should not be searched without the probable cause required by FISA and the Fourth Amendment. This is another example of the wish-list approach of this bill.)

The DOJ "Fact Sheet" omits other ways in which its streamlining diminishes Americans' privacy protections. The bill would substantially extend the period of secret surveillance allowed with a warrant. It would allow round-the-clock surveillance of Americans in one-year increments upon renewal of an order, with no judicial supervision during that time about whether the wiretap was even productive for gathering foreign intelligence.

DOJ Fact Sheet: "The bill . . . reflects today's national security threats. The bill seeks to update FISA to reflect today's national security threats. One of those threats is the proliferation of weapons of mass destruction. This legislation will allow the Intelligence Community to obtain FISA authority to better protect the nation against proliferators."

The Facts about WMD in this Context. There is no doubt the proliferation of unconventional weapons is dangerous, but it is unclear why the current definitions and provisions in FISA do not already provide ample authority to wiretap anyone in the US who is conspiring to develop or use such weapons illegally for terrorism or sabotage. FISA expressly allows for the wiretapping of suspected agents of a foreign power, regardless of the mechanism used. To borrow a page from DOJ, FISA is already "weapons neutral"--FISA should not start listing weapons in any way that would make such a list seem exclusive or too narrow. FISA should remain focused on the nature and status of the people under surveillance rather than listing specific weapons.

The administration gives no explanation about what difference it would make to add the proposed language. Is it meant to allow the secret surveillance of every foreign scientist working on nuclear energy in this country? Or are the WMD definitions so broad that possession of common items such as pool chemicals or gunpowder--precursors that are lawful for Americans to possess--could be used as a basis for surveillance? Or is the intent simply a political strategy to try to claim that anyone who dares to oppose this package of bad ideas is refusing to prevent WMD terrorism? That would be a wrong claim, in every sense of the word.

DOJ Fact Sheet: "The bill would . . . add an additional definition of an agent of a foreign power for non-US persons whom the Government believes possess significant intelligence information, but whose relationship to a foreign power is unclear. This proposed change would apply only to non-US persons in the US, and collection of information from such an individual would be subject to the approval of the FISA Court."

The Facts about "Agent of a Foreign Power": Congress already provided the administration with a very controversial "lone wolf" amendment, in the President's first term, to allow wiretaps of non-US persons in the US who are plotting international terrorism unconnected to a foreign power. See Section 6001 of the Intelligence Reform and Terrorism Prevention Act, 75 Pub. L. 108-458, 118 Stat. 3742 (2004) (subject to the sunset provisions). Thus, Congress has already addressed potential foreign terrorists "whose relationship to a foreign power is unclear."

This bill would allow extremely widespread surveillance of any non-green card holder in this country, not on any suspicion of terrorism, espionage or any crime at all, but simply on the basis that the individual might know "foreign intelligence information" of interest to the government. Such information is not limited to information about sabotage or international terrorism but includes broad information about "the conduct of US foreign affairs" or "defense." The fact that a warrant would be required does not provide much protection because the statute would be changed to permit such surveillance, meaning it provides for the court to legally approve it.

And, in our global economy, many well known companies, even news services, in the US do not count as US persons under FISA's definitions because of the location of their incorporation—even if they employ or do business here with numerous Americans. This new provision would open such companies as well as foreign nationals to secret, round-the-clock monitoring of phone conversations or e-mails, when there is no suspicion of wrongdoing. The person or business might not even know they possess foreign intelligence information and might not actually possess any such information. Such surveillance would undoubtedly intercept countless innocent communications, including numerous conversations with Americans, including employees of such companies. The bill does not contain any significant protection against agents listening to, keeping and using such communications.

Other Facts Ignored in DOJ Fact Sheet: The bill also attempts to short-circuit existing judicial review of the warrantless NSA surveillance program. In addition to the grant of immunity discussed above, the bill would strip federal and state courts, except the FISA court, of the power to hear existing claims against that program or any other classified intelligence activities. That is, it would prevent fairly and randomly chosen judges from state and federal courts with pending or future constitutional or state privacy claims from considering the merits of these claims. The bill would force such claims to go before the FISA court, constituted of judges picked by the Chief Justice, for largely secret proceedings to adjudicate the constitutional rights of Americans. And, under the terms of these provisions, if the government sought access to the judge without the other party present, the court would be required to grant such requests.

The administration's bill also replaces the narrow exception to the warrant requirement for embassies in the US with broader authority to acquire communications in the US without a court order, simply based on the Attorney General's certification or directive. For example, section 102 of FISA would be changed to eliminate the narrow exception that a warrant is not required if the surveillance is directed "solely" at the communications of foreign governments here, and it deletes the bar on such warrantless surveillance even when there is a "substantial likelihood" Americans' conversations will be swept in. That is, the Attorney General could order warrantless surveillance directed toward a foreign government here even if such surveillance was likely to sweep in Americans' conversations. And the bill strikes the statutory protections for American conversations obtained inadvertently without warrants, by eliminating FISA's requirement in 50 USC 1801(h)(4) that such conversations be deleted within three days of acquisition unless the government obtains a court order or there is a threat to life or bodily injury. The bill would also add new sections, 102A-C, to allow "acquisition of information" without a court order relating to a person believed to be outside the US. These and changes to the rules for warrants proposed in the administration's bill should be thoroughly evaluated.