

**“Modernization”  
of the Foreign Intelligence Surveillance Act (FISA):**

1634 I Street, NW Suite 1100  
Washington, DC 20006  
202.637.9800  
fax 202.637.0968  
<http://www.cdt.org>

**Administration Proposes Broad, Warrantless Surveillance of Citizens**

**Updated - April 18, 2007**

On April 13, the Administration offered a bill to make major amendments to the Foreign Intelligence Surveillance Act. The bill is cloaked in the rhetoric of modernization, but it would turn back the clock to an era of unchecked domestic surveillance and permit the NSA’s vacuum cleaners to be used on international and purely domestic calls and email of US citizens without court order. This is CDT’s preliminary analysis.

The most important part of the bill would change FISA’s definition of “electronic surveillance” to say, in Alice in Wonderland fashion, that the sweeping collection of information about the domestic and international phone calls, email and other communications of American citizens is not “electronic surveillance” and therefore does not require a court order. The bill would permit untargeted warrantless surveillance of the contents of all international communications of US citizens and the collection of identifying data about all our purely domestic communications.

It is impossible to tell whether the Administration really intends to authorize such sweeping warrantless surveillance. That would certainly be the effect of the proposed legislative changes, but the limited justifications the Administration has given for the changes are much less sweeping. The Administration’s section-by-section analysis of the bill is not at all clear. Key parts of that analysis are rhetorical rather than explanatory. In other places, the analysis seems to intentionally avoid discussing the true significance of the proposal. As we explain below, FISA may need to be updated, but the first step is for the Administration to clearly explain why FISA is inadequate, which it has failed to do. To the extent that the Administration has actually described issues with FISA, they could be addressed with much narrower changes. And any changes to FISA should include increased privacy protections, which are clearly needed.

**-- Changes in Technology Require Stronger, Not Weaker, Standards**

The Administration justifies the bill largely on the ground that changes in technology have made FISA outdated. The Administration never actually explains what those technology changes are, although they have hinted at them. Some of these changes, such as the routing of international communications through the United States, actually make the job of the intelligence agencies much easier in some ways, since they can

access foreign-to-foreign communications from US soil. Beyond that, everything we know about the digital revolution indicates that, on balance, it has been a windfall for the snoopers: With globalization, cell phones, and the Internet, more electronic information than ever before is available to the government, and the government's ability to process that information is exponentially greater than ever before. Whether the government is able to digest the massive amount of information at its disposal is a different question, but the availability of oceans of sensitive personal data is no reason to weaken standards for government collection of that data. If anything, the increasing amount of information about our daily lives that is exposed to electronic surveillance calls for stronger, not weaker standards.

The Administration argues that it is no longer appropriate to have different standards for surveillance, as FISA has since its adoption, depending on how or where communications are intercepted. (For example, FISA has different rules for interception of a communication carried on a wire versus the same communication when it is being transmitted by satellite or microwave.) However, the Administration is 100% wrong when it argues that consistency should be achieved by permitting warrantless surveillance for all forms of communication. Contrary to the Administration's press release, the proposed bill would weaken privacy protections for Americans.

### **The Administration Bill Would Expand Warrantless Surveillance**

In this memo, we focus on the ways in which the Administration bill would expand the warrantless surveillance of US citizens. There are many other features of the bill, and CDT will endeavor to comment on them in coming weeks.

In order to understand the impact of the Administration bill, it is necessary to appreciate that much of the weight of FISA is carried by its definitions. Most importantly, FISA regulates only "electronic surveillance" as that term is uniquely defined in the Act. If the collection of information fits within the Act's definition of "electronic surveillance," it requires a court order or must fall under one of FISA's exceptions. If the collection of information is *excluded* from the definition of electronic surveillance, then it is not regulated by the Act, and the government can proceed without a court order and without reporting to Congress. Therefore, narrowing the definition of electronic surveillance places more activity outside the judicial and Congressional oversight of the Act.

That is precisely what the Administration bill does: It changes the definition of electronic surveillance to exclude from the Act's coverage the collection of a great deal of information about the communications of US citizens that the average person would call "electronic surveillance." Simply put, the changes sought by Administration would authorize large-scale warrantless surveillance of American citizens and the indefinite retention of citizens' communications for future data-mining.

The Administration's language would permit warrantless surveillance of the communications of American citizens in three broad categories:

## **1. Untargeted Warrantless Surveillance of the International Communications of US Citizens**

Under the proposed new definition, all communications to or from the US could be intercepted without a warrant, so long as the government is not targeting a known person in the US.<sup>1</sup> If the government were targeting someone who is overseas, they would be able to intercept communications between that person and citizens in the US without a warrant. But the bill goes even further: the government also would not need a warrant if it were engaged in broad, unfocused collection. Under the Administration's bill, the government could intercept all international communications without a warrant, even those originated by citizens and even those involving citizens on both ends.

The bill would permit warrantless surveillance far beyond the President's Terrorist Surveillance Program. Until recently, the Administration consistently argued that it should not need a court order when it is targeting a suspected terrorist overseas calling the US. The problem with the TSP even thus narrowly defined is that, of course, there are two parties to the call, one of whom is in the US and is quite likely a citizen. The person on the phone in the US may be a journalist, an innocent relative, an aid worker, or any other variety of innocent person. Yet under this bill the conversations of those innocent Americans will be intercepted without a warrant.

However, the bill would authorize a program of warrantless surveillance far, far broader than what the President authorized. The President assured the American public that his program was limited to situations where someone from al Qaeda was overseas, calling into the US. The Administration's new bill would authorize warrantless surveillance of all international calls, whether or not there is any reason to believe that al Qaeda is on the line. It would also cover all international calls that originate in the US. Under this bill, for the first time ever, NSA would be able to train its vacuum cleaner on the contents of all international calls, recording every single one, so long as it was not targeting a specific person in the US.

The NSA resents the use of the phrase "vacuum cleaner." It argues that it doesn't want to vacuum up all international calls and couldn't process them even if it did. We use "vacuum cleaner" because the bill would permit without a warrant the untargeted collection of many, many calls, without the particularized suspicion required by the Constitution for government searches.

---

<sup>1</sup> The new definition of "electronic surveillance" would have two parts: intentionally intercepting international communications of a particular, known person reasonably believed to be in the US, and the acquisition of the contents of communications when all parties are reasonably believed to be in the US. That excludes the collection of the contents of all communications to and from the US so long as the government is not targeting a known, particular person here.

-- **FISA’s “Radio Exception” - Technology Neutrality Does Not Require Weak Standards**

As partial justification for the warrantless interception of all international calls, the Administration’s section-by-section analysis and its earlier discussions of this issue hint at FISA’s distinction between wire and radio communications. When FISA was adopted, it exempted international telephone calls (and other communications) entering and leaving the US by satellite. The reasons for this exemption are lost in the legislative process, but Congress may have been merely deferring the question.<sup>2</sup> Whatever was the purpose of the radio exception in 1978, there is no reason to apply different standards today. But rather than reconciling the standards by providing to satellite communications the same protections that have always applied to wire communications, the Administration would respond by rolling back the protections afforded wire communications and exempting all international communications from FISA, unless the government is targeting a known person in the US. A much better way to make the statute technology neutral is to require a warrant for all interception of communications with one leg in the US.

Indeed, by citing the radio exception and arguing that it wants it to apply to all communications, the Administration reinforces our conclusion that the bill would carve out from FISA’s coverage the wholesale interception of all international communications.

The “radio exception” may have been justified in 1978 on the ground that the government was worried about disclosing to carriers the subjects of its interest, or that the carriers were reluctant to cooperate with surveillance, or that the carriers may not have had the ability to isolate the communications of a targeted person or communications

---

<sup>2</sup> The Senate Judiciary Committee report on FISA, Rept 95-604 states on page 34:

“The reason for excepting from the definition of "electronic surveillance" the acquisition of international radio transmissions, including international wire communications when acquired by intercepting radio transmission when not accomplished by targeting a particular United States person in the United States, is to exempt from the procedures of the bill certain signals intelligence activities of the National Security Agency.”

The Senate Judiciary Committee report went on to say:

“The activities of the NSA pose particularly difficult conceptual and technical problems which are not dealt with in this legislation. Although many on the Committee are of the opinion that it is desirable to enact legislative safeguards for such activity, the committee adopts the view expressed by the Attorney General during the hearings that enacting statutory controls to regulate the NSA and the surveillance of Americans abroad raises problems best left to separate legislation.” P. 64.

instrument. None of those reasons seem valid today. It is clear that carriers are willing to cooperate, and the Communications Assistance for Law Enforcement Act of 1994 requires all carriers to build into their networks the ability to isolate the communications to and from specific users. The Administration has offered no explanation as to why changes in technology require it to conduct warrantless surveillance of international calls. The way to make FISA technology neutral is to require a warrant for interception of both wire and radio (satellite) communications.

## **2. Warrantless Collection of Transactional Information about the Purely Domestic Communications of US citizens**

Just as dramatically, the bill would allow the vacuum cleaner of the NSA to be used to compile information identifying the source and destination of every telephone call and email sent in the US. It would do so by excluding from the definition of “electronic surveillance” the untargeted collection of “non-content” information about purely domestic communications between US citizens inside the US. The bill would allow the NSA to scoop up all records of all calls made and email sent in the United States. Information on purely domestic calls could be collected without a court order. The government would be able to compile and keep forever a record of who is calling whom, and to analyze that database at any time. The bill would thus authorize a massive datamining program against US citizens.

### **-- Clarifying FISA’s Treatment of Transactional Data**

Surveillance law has long distinguished between the interception of the content of communications and the interception of dialing or signaling information about communications. The Supreme Court held three decades ago – in cases that look increasingly shaky – that transactional data about calls is not constitutionally protected. Nevertheless, call detail records and Internet records are clearly sensitive; they give a full picture of a person’s associations and activities. In the law enforcement context, Congress long ago required a court order for interception of transactional details about telephone calls and email.

In contrast, the status of transactional data under FISA has always been unclear. FISA includes a definition of “content” that is broader than the definition of content under the law enforcement wiretapping law. Under FISA, “content” includes information about the existence of a communication or identifying the parties to it.

In 1998, Congress amended FISA to include a new section authorizing orders in intelligence matters for pen registers and trap and trace devices, which collect transactional information about communications. However, Congress did not amend the definition of content, so the Act seemed to be internally inconsistent, defining transactional information as content requiring a full probable cause based order while also authorizing the collection of transactional information under the lower standard of the pen register/trap and trace section. As far as we know, successive Administrations have not said how they reconcile the conflict.

The Administration bill would eliminate the conflict, by redefining content to exclude transactional information. In the process, it would seem to render the pen register/trap and trace provision of 1998 merely voluntary, for nowhere does FISA state that a pen/trap order must be obtained to collect transactional information. In other words, by eliminating transactional data from the definition of content, the Administration bill would eliminate it from any requirement of judicial control at all.

### **3. Warrantless Surveillance of the Content of Purely Domestic Communications of Citizens**

With a third change, the Administration bill would allow warrantless interception of the content of the domestic calls of US citizens. Section 402 of the Administration bill would allow warrantless surveillance of the content of purely domestic calls so long as it is “directed at the acquisition of the contents of communications of a foreign power.” Basically, this would allow warrantless surveillance of all calls into and out of all embassies, consulates, government-owned corporations like Olympic Airlines, and the US offices of “factions” like the Iraqi Kurds. Many of those calls are to and from US citizens. Indeed, since most foreign embassies and consulates inside the US employ large numbers of US citizens, it is likely that the people on both ends of the calls would be citizens. Under this bill, they can be intercepted without a court order.

Question: As noted, the key language is “directed at the acquisition of the contents of communications of a foreign power.” Would that be more inclusive than calls into and out of facilities owned or occupied by foreign governments, government owned corporations, or factions? When a foreign national employed by his country’s embassy or consulate in the US uses his home phone, is that the “communication of a foreign power?”

FISA contained a narrowly crafted “embassy exception.” It was not available if there was likelihood of intercepting the communications of Americans. The Administration’s bill would lift that limitation, permitting warrantless surveillance of every school child’s effort to get information about France (see <http://www.ambafrance-us.org/kids/>) and every vacationer’s call about visa requirements or immunizations for their overseas travel, let alone every journalist’s call to an embassy official.

#### **What Protection Do “Minimization Procedures” Provide?**

The draft bill and the explanatory statement point to “minimization procedures,” which are secret rules written by the Attorney General governing the acquisition, retention and dissemination of information. We have no doubt that NSA employees take minimization very seriously, but the concept itself offers little protection. Minimization does not mean that the government cannot collect, retain or disseminate information about US persons. To the contrary, minimization procedures allow the collection, retention and dissemination of “foreign intelligence” regarding US persons.

Since the main purpose of intelligence gathering is to gather foreign intelligence – since the intelligence agencies have no reason to be collecting or disseminating anything that is not foreign intelligence whether it relates to a US person or not -- the minimization rules offer little added protection. The concern is not that the intelligence agencies will be collecting information about the extramarital affairs of Americans. The concern is that the intelligence agencies can collect and disseminate ambiguous, incomplete and potentially misleading information about the foreign travels, relationships and activities of Americans that may relate to some aspect of US foreign policy. Whether such collection and dissemination is appropriate in any case should be a matter for judicial review, not left to secret minimization rules written by the Attorney General.

The bill also cuts back on the minimization requirement. Under current law, if the government, acting without a warrant under Section 102(a) of FISA, obtains the communications of a US person, those communications cannot be disclosed, disseminated or used, and the government must destroy them within 72 hours unless the Attorney General obtains a court order or determines that the information indicates a threat of death or serious physical harm. The Administration bill would permit unrestricted retention and use of the communications of US citizens obtained without a warrant under the vastly expanded Section 102. This change is especially important in light of the changes made to Section 102(a), which include new authority for warrantless surveillance of domestic calls involving US citizens.

### **Reducing Judicial Oversight by Reducing the Detail in FISA Applications**

The bill would cut back on the information the government is required to include in its applications to the FISA court. Some of the information the bill would cut from the government's applications is useful to the court in determining if the surveillance is reasonable. Without this information, it will be hard for the court to issue an order specifying the scope of permitted surveillance. Given what we have learned about the tendency of intelligence agencies to cut corners (for example, the FBI's issuance of emergency records demands when no emergency existed), this does not seem to be the time to cut back on the amount of information provided to those responsible for checks and balances.

### **Congress Should Proceed Cautiously and Engage in an On-the-Record Exploration of the Issues Raised by the Administration's Proposals**

There is a long, secret history to the Administration's proposed bill. The Administration states that its proposed language has been under development for more than a year. The issues addressed by the bill have been debated intensively inside the Administration since soon after 9/11 and were percolating before then. Congress has not been part of those debates and should not simply accept the Administration's proposals. It should move cautiously and take time to understand the issues and to consider the impact of the changes sought by the Administration on the rights of the American people.

The first step is for Congress to get on the public record the full story on the Administration's warrantless surveillance activities. The proposed bill would give immunity to the telecommunications carriers involved in those activities and thus terminate the various pending lawsuits, which may be one of the best means of getting to the bottom of the Administration's violations of FISA.

Before going forward with any amendments to FISA, Congress should hold public hearings to examine what problems, if any, the Administration has with the current law. Those hearings can be held without jeopardizing national security. Based on such hearings, Congress can identify which issues—if any-- raised by the Administration are real and require narrowly focused changes. At the same time, Congress should address the ways in which FISA should be strengthened to provide better privacy protection. In holding those hearings, Congress should distinguish between the criticality of the mission of the National Security Agency and the weak standards proposed in this bill. Of course, when al Qaeda is calling the US, we want to be listening. The question is, what should be the legal standard when a US citizen is on the other end of the call? And should the government be able to conduct surveillance when it has no reason to believe al Qaeda is on the line?

\* \* \*

CDT will continue to refine its analysis and will endeavor to analyze other provisions of the draft bill in coming weeks. We urge Congress to reject this sweeping proposal. We welcome dialogue with the Administration over the issues at stake.

For further information: Jim Dempsey (202) 365-8026, [jdempsey@cdt.org](mailto:jdempsey@cdt.org).