

March 22, 2006

To: Interested Persons

From: Jerry Berman, Jim Dempsey, Nancy Libin

Re: CDT ANALYSIS OF CHAIRMAN SPECTER'S BILL ON FISA
The National Security Surveillance Act (NSSA) of 2006

On March 17, Chairman Specter introduced a bill on FISA that would establish procedures for judicial review and approval of a certain type of electronic surveillance program. The bill is a response to the Administration's acknowledgement that it is carrying out wiretaps inside the United States without a court order. We applaud Chairman Specter for insisting that electronic surveillance within the U.S. must be subject to the Foreign Intelligence Surveillance Act and judicial review.

However, upon close reading, we have concluded that the Chairman's bill does not adequately achieve the goal of providing meaningful judicial oversight or privacy protections with respect to the President's publicly disclosed terrorist surveillance program. In addition, it provides incomplete controls on any other, so-far unacknowledged electronic surveillance programs or activities taking place within the U.S. but outside FISA. It covers the interception of the content of communications but does not limit – indeed, it seems to permit without judicial approval -- the interception and analysis of detailed, non-content information concerning the calling patterns and email and other Internet activity of persons, including U.S. citizens, inside the U.S. Nor does the bill ensure that court orders under FISA, even as amended by this bill, will be the sole and exclusive means for the President and the Executive branch to conduct national security electronic surveillance inside the United States. Most important, the bill is being put forward without the Judiciary Committee or the public having sufficient facts about the nature and effectiveness of the program, both of which must be explored before an appropriate legislative response can be drafted.

We recognize that surveillance laws, especially amendments to FISA, are very hard to draft. However, despite the best efforts of the Chairman and his staff, elements of the bill are not clear to us upon initial readings.

Overview – The NSSA Is Far Broader Than the President's Program

The NSSA allows surveillance that is broader than the program the President and the Attorney General have so far described on the public record. The President and the Attorney General have stated that the NSA terrorist surveillance program is limited to intercepting the calls that al Qaeda members and those associated with al Qaeda make from overseas into the U.S. The Administration has said that the program is used in circumstances where immediate monitoring is necessary for some short period of time in

order to determine whether to seek a traditional FISA warrant. In effect, the Administration has described a need for a new emergency exception. The President and the Attorney General have argued that domestic calls are not covered, and that in every case there is some connection to terrorism. The Administration says that the President's program does not involve data mining and is a targeted program.

In contrast, the NSSA –

- covers purely domestic calls involving U.S. citizens and other persons where those persons have a reasonable expectation of privacy;
- is not limited to al Qaeda and those associated with al Qaeda and is not limited to terrorism, but applies to any clandestine intelligence activities, which include a range of non-violent and legal activities;
- is not limited to the communications of suspected terrorists – it permits authorizations to target the calls of anyone in the US “who has had communication” with anyone suspected of being a terrorist, permitting, therefore, the interception of the calls of persons who are talking to persons who once talked to someone suspected of being a terrorist;
- instead of authorizing short term, emergency surveillance as the President and Attorney General have described, it permits surveillance to continue indefinitely (albeit subject to 45 day reviews) for as long as the court permits the program, even if no particular suspicion is ever established against any individual persons whose communications are intercepted;
- allows the collection of many innocent communications in pursuit of a few that may be related to terrorism or foreign intelligence and seems to allow their unlimited retention for later search.

The NSSA Does Not Authorize a Targeted Surveillance Program: It Would Authorize the Recording of All Conversations, Domestic and International

The Chairman's bill is clearly intended to permit surveillance without the specificity that the Constitution normally requires. There are two key fundamental problems with the NSSA as drafted:

1. The key standard in the bill is in a proposed new section 704(a)(3), which requires the FISA court to authorize an electronic surveillance program if it finds “*probable cause to believe that the electronic surveillance program will intercept communications of the foreign power or agent of a foreign power specified in the application, or a person who has had communication with the foreign power or agent of a foreign power that is specified in the application and is seeking to commit an act of international terrorism or clandestine intelligence activities against the United States.*”

If we read this correctly, the person who “is seeking to commit an act of international terrorism” is not the person who has had the communication with the foreign power or agent of a foreign power but rather is the foreign power or agent of the foreign power. In other words, the bill allows ongoing surveillance of anyone who once had a communication with someone who is an agent of a foreign power planning clandestine activities against the U.S. This would permit surveillance of everyone who has ever had a communication with an employee of the Israeli government or employee of an Israeli government-owned corporation, since the Israeli government is a foreign power carrying out clandestine intelligence activities against the United States. It would cover every journalist who has had a conversation with a member of Hamas. Even more narrowly construed, consider the sweep of this in the context of terrorism. According to press reports in the past months, there are now 200,000 to 325,000 names on the terrorist watch list. Anyone "who has had communication" with any of those 200,000 to 325,000 people can be targeted for surveillance under this bill.

2. There is an even bigger problem: As written, this standard encourages the government to use the broadest dragnet possible, because if the government intercepted every call of every person in the world it would definitely intercept the communications of foreign powers and agents of foreign powers who are seeking to commit acts of international terrorism or clandestine intelligence activities, and persons who have had communications with those foreign powers and agents of foreign powers. The broader the program, the more likely it is to meet the standard.

We do not know whether this is the Chairman’s intent, but, in effect, the bill permits the government to scoop up millions of calls of innocent people – people who have never even had a communication with someone suspected of being a terrorist – in order to snag a few conversations of possible value.

In lieu of targeting individuals who are themselves suspected of involvement in terrorism, section 704(b) requires the government to come back to the FISA court and show that the dragnet is producing value. However:

- the bill does not require the government to show initially that the program is unlikely to intercept significant quantities of innocent conversations;
- it does not prohibit the court from reapproving the program even if it is intercepting many innocent conversations in order to acquire a few;
- it does not specify what happens to the possibly millions of innocent conversations that are recorded -- by not requiring that they be destroyed after analysis, it apparently permits them to be retained indefinitely;
- even if the program produces little or no intelligence value, the government can come back at the end of the first 45 days with a new algorithm and obtain approval for a “new” program, again without having to show that the new program is unlikely to obtain large amounts of innocent conversations.

The Constitution, in any event, does not allow searches to be justified after-the-fact. As we discuss in more detail below, particularity is a Fourth Amendment prerequisite. The

fact that a search produces results does not make it reasonable. The government does not get to cast a fishing net and then later justify the search on the grounds that it found something. Under the Constitution, a determination of specificity must precede the search.

Under the Fourth Amendment, the government should have probable cause to believe at the beginning of a search not only that its interception will acquire bad conversations BUT ALSO that it will acquire relatively few innocent ones. This is accomplished in ordinary searches by describing with particularity the place where the search is to be conducted. It must be a place where the government has probable cause to believe it will find evidence of a crime or contraband. In wiretap cases under Title III and normal FISA cases, the particularity requirement requires the government to name both the target and the facility to be searched, limiting the surveillance to a phone line, email account or other facility that there is probable cause to believe a bad guy (or an agent of a foreign power) is using. The NSSA does not require particularity as to either person or place or facility.

In addition, as others have pointed out, the bill places the FISA court in a very unusual position, requiring it to consider the “benefits” of a surveillance program.

As promised by the Chairman, the bill directs the FISA court to make an up-front constitutional determination about any program presented to it. However, the bill provides no guidance to the government or the court on the appropriate standards for such a review. The whole purpose of FISA is to avoid turning every intelligence surveillance program into a constitutional question. The bill does just the opposite and punts to the courts the drafting and deliberations that are the responsibility of the Congress.

The bill is not saved by the minimization requirements. FISA, like the Fourth Amendment, requires both minimization and particularity. Indeed, in FISA, minimization is a limit on dissemination, not on acquisition or interception. It does not satisfy the Constitutional requirement that the government state with specificity the items to be collected.

The new section 703(a)(7) requires the government's application to "include a statement of the facts and circumstances relied upon by the Attorney General to justify the belief that at least one of the participants in the communications to be intercepted by the electronic surveillance program will be the foreign power or agent of a foreign power specified in subsection 5, or a person who has had communication with the foreign power or agent of a foreign power specified in subsection 5." The bill would look very different if section 703 required a "belief that at least one of the participants in EACH OF the communications to be intercepted..." and if section 704(a)(3) required probable cause to believe that the program will intercept only (or primarily) communications of persons in contact with suspected terrorists. That would build particularity into the up-front approval process and, if limited to international communications, would reflect the program the President has described.

This Is Not the Posner Proposal

Judge Posner and others have suggested that it would be desirable and Constitutional to allow the government to scan communications by computer, and then have humans read only those that fit a certain profile. If such programs exist and are effective, it seems they should be subject to a judicial probable cause determination. Increasingly, all electronic searches use machines to select communications for human review. (An ordinary wiretap is a command to a computer to select out from a computerized switch all calls to or from a particular number.) Already, in the context of Internet communications, a regular Title III wiretap order, based on particularity, requires the service provider to scan by computer millions of packets of communications of innocent persons to select the few that meet the particularity requirements of the warrant, which identifies a particular IP address for surveillance. Even though communications are in packet form, the particularity requirement of the Constitution should still apply. Each packet is specifically identified as to sender and recipient. If there is solid reason to believe that another set of parameters, other than IP addresses, would be as reliable in picking out communications to or from a terrorist, even one whose name is not known, then it might be possible to devise a system under which such parameters would be subject to a probable cause inquiry. Whether a human programs a machine to select calls or clips a pair of alligator clips onto a wire, a person is making the decision what to select, and that decision should be subject to judicial review.

Regardless, however, it appears that the NSSA is NOT a machine-reading bill. It does not expressly contemplate that messages will be scanned first by a machine before a human reads them. It authorizes "interception," which it defines as human reading. The bill neither authorizes nor prohibits machine reading of communications; it seems to leave them in limbo. Rather, the bill allows humans to read any in a very large pool of collected communications, so long as there is probable cause to believe that they may involve relevant communications. In this sense, the bill is arguably broader even than the Posner program, since it does not require machines to filter the messages before humans read them.

The bill refers to "technologies and techniques that defy conventional law enforcement practices." If Congress is going to amend the law to take account of new technology, it should carefully study the ways in which technology may make it possible for the government to conduct more discriminating searches.

The Constitutional Principle of Particularity

The Fourth Amendment requires that a warrant describe with "particularity...the place to be searched and the persons or things to be seized." U.S. Const. Amend. IV. The US Supreme Court has established a "permeated with fraud" exception to the particularity requirement, but this exception does not support the "general" warrant that the NSSA allows.

The findings of the NSSA bill indicate that the requirements of the Fourth Amendment can be flexibly interpreted in cases involving complex, far-reaching and multi-faceted enterprises. The leading case on this is *Andresen v. Maryland*, 427 U.S. 463, 480 (1976), where the Supreme Court emphasized, “General warrants, of course, are prohibited by the Fourth Amendment.” Quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 467 (1971), the *Andresen* Court went on to say, “[T]he problem [posed by the general warrant] is not that of intrusion per se, but of a general, exploratory rummaging in a person's belongings. . . . [The Fourth Amendment addresses the problem] by requiring a ‘particular description’ of the things to be seized.” The Court in *Andresen* upheld a warrant that authorized the government to seize evidence about fraud in the sale of particular lot of real estate and “about other crimes yet unknown.” The Court noted that the crime under investigation was complex, and could be proven only by piecing together many bits of evidence. However, the Court emphasized that the warrant specified the specific place to be searched (a lawyer’s office) and specified the particular lot of real estate to which the documents to be seized related. Significantly, the Court contrasted the warrant in *Andresen* with the overbroad language in the eavesdropping statute found unconstitutional in *Berger v. New York*, 388 U.S. 41 (1967), stating “[t]he specificity with which the documents are named here contrasts sharply with the absence of particularity in *Berger v. New York* [citation omitted], where a state eavesdropping statute which authorized eavesdropping ‘without requiring belief that any particular offense has been or is being committed; nor that the ‘property’ being sought, the conversations, be particularly described,’ was invalidated.” *Andresen*, 427 U.S., at 481 n. 10.

The NSSA bill does not require the application to state with specificity the natural person(s) whose communications will be intercepted, and it requires no specificity as to place or facility. It merely requires the application for the electronic surveillance program to give “the name, if known, identity or description of the foreign power or agent of a foreign power seeking to commit an act of international terrorism or clandestine activities against the United States the electronic surveillance program seeks to monitor or detect. . . .” This permits the government merely to aver that it “seeks to detect al Qaeda,” with no more specificity. This language does not regulate the scope of the program and thus does not serve the limiting function that the “particularity” requirement is meant to achieve. (As stated above, the bill requires a finding of probable cause that the program will intercept *some* communications of the described foreign power or agent of a foreign power—not that it be limited to intercepting only those communications.)

In other cases, such as administrative searches, the Supreme Court has allowed searches without particularity. But there are some very important differences between the type of search allowed in *Andresen* and in the administrative search cases versus the kind of electronic surveillance anticipated by the Chairman’s bill:

- Nature of search—the clandestine interception of private communications is recognized to be inherently more troublesome even than a physical search (hence, the multiple special protections in Title III and ECPA);

- No notice ever – under the Chairman’s bill, as under FISA in general, the target of surveillance is never notified, while administrative searches and the kind of search approved in *Andresen* are carried out with contemporaneous notice, so that there is an opportunity to challenge overbroad conduct;
- Longer duration – as far as we can determine, the administrative search cases all relate to one-time physical searches, not on-going intrusions.

In the criminal context, the interception of conversations of innocent persons who are not the target of the wiretap resembles a random stop-and-search without probable cause, of every person who appears in the company of some known person who is suspected of being involved in some criminal activity. The bill would allow a repeated, ongoing stop-and-search of unlimited innocent persons who speak—knowingly or unknowingly—to suspected terrorists.

Congressional Oversight

The NSSA directs the President to report to each member of the congressional intelligence committees *or special subcommittees established to oversee electronic surveillance programs under FISA* on the management, operational details, effectiveness and necessity of the electronic surveillance programs. Specifically, under a new section 705, the bill requires the President to

- “submit [a report] to each member of the congressional intelligence committees (*or any subcommittee thereof designated for oversight of electronic surveillance programs under this title*)....”;
- “submit...a report...on any specific surveillance conducted under the electronic surveillance program whenever requested by either of the committees, *or any such subcommittee, as applicable*”;
- “fully inform each member of the congressional intelligence committees (*or any subcommittee thereof designated for oversight of electronic surveillance programs under this title*)....”

As currently written, the bill has the potential to limit the authority of the full intelligence committees.

Under the National Security Act of 1947, the President already is required to ensure that the full congressional intelligence committees are kept “fully and currently informed” of U.S. intelligence activities, including any “significant anticipated intelligence activity.” According to legislative history, the term “fully and currently informed” is intended to mean that the executive branch must provide the committees complete and timely notice of actions and policies and inform the committees of intelligence activities in such detail as they may require. Another provision of the National Security Act specifically requires that the Director of National Intelligence (DNI) and the intelligence agency heads “keep the intelligence committees fully and currently informed of all intelligence activities...” and “...furnish the congressional intelligence committees any information or material concerning intelligence activities, other than covert actions...” that is within their control.

The statute specifically defines “covert action” to exclude intelligence gathering activities. Therefore, the full committees must be informed of intelligence collection activities.

Other Questions or Concerns About the NSSA

As noted above the bill does not limit, and seems to permit, surveillance, retention and analysis without limit and without any suspicion of transactional information showing who is calling whom – a powerful and intrusive technique that can give a full picture of a persons associations and activities. The bill does nothing to clarify the ambiguities under FISA regarding this type of surveillance.

The bill’s definition of “electronic surveillance program” is limited to programs “where effective gathering of foreign intelligence information requires an extended period of electronic surveillance.” Therefore, the bill seems to exclude from the requirements of FISA review untargeted programs involving the interception of communications inside the United States for less than extended periods. However, the bill does not define “extended period.”

An Alternative, and More Cautious, Response to the President’s Program

The first step is to define the problem. There must be a congressional inquiry to determine the full extent of surveillance that the administration is conducting outside of the FISA procedures. The NSSA permits a much broader program than the one that the administration has described.

Congress should not consider legislation unless the administration agrees that with the new authority granted by the Congress it will conduct all electronic surveillance, as defined by FISA, pursuant to the FISA standards.

As we understand that Attorney General’s testimony, the sole reason he presented why FISA could not be used was that the emergency procedure was not flexible enough. Legislation addressing that problem can be developed. If there is another problem, it must first be defined by the Administration.

We believe it is crucial to frame the legislative debate in terms of the public record to date. Following an appropriate congressional inquiry and an acceptance by the Administration that it would, after the enactment of the legislation, conduct all surveillance pursuant to FISA procedures, we would work on a bipartisan basis to craft an appropriate response.

For more information contact Jerry Berman, Nancy Libin or Jim Dempsey (202) 637-9800.