

**Statement of James X. Dempsey  
Policy Director  
Center for Democracy and Technology**

**before the**

**Senate Select Committee on Intelligence**

**Foreign Intelligence Surveillance Act (FISA)**

**May 1, 2007**

Chairman Rockefeller, Vice Chairman Bond, Members of the Committee, thank you for the opportunity to present this written statement for the Committee's hearing on the Foreign Intelligence Surveillance Act (FISA).

On April 13, the Administration offered a bill to make major amendments to FISA. The bill is cloaked in the rhetoric of modernization, but it would turn back the clock to an era of unchecked surveillance of the communications of US citizens, permitting the NSA's vacuum cleaners to be used on all international calls and email of US citizens without court order.

In this statement, we make four main points:

- Of course, technology has changed since FISA was adopted in 1978, but some of those changes have made snooping easier, and in aggregate they have increased the amount of information about our daily lives that is available electronically to the government, thereby requiring stronger, not weaker privacy protections.
- The Administration's bill would go in the wrong direction, by permitting the untargeted warrantless surveillance of all international communications of US citizens. 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 the international phone calls, email and other communications of American citizens is not "electronic surveillance" and therefore does not require a court order.
- A much narrower set of changes would address the concern that a court order should not be required when the government is collecting foreign-to-foreign communications nor when it is targeting a person abroad who has an incidental number of communications that appear to be with someone in the US.
- In light of press reports that the government has been obtaining massive amounts of transactional records from telephone companies, the Committee should get from the Administration on the public record a clear explanation of the relationship between FISA and the rules for collection of transactional information and stored records.

FISA may need to be updated, but the first step is for the Administration to clearly explain on the public record why FISA is inadequate, which it has failed to do. So far, to the extent that the Administration has actually described issues with FISA, they are ones that could be addressed with much narrower changes. And any changes to FISA should include increased privacy protections, which are clearly needed.

The Administration's proposal is an exercise in cherry-picking: Arguing that FISA is outdated, and claiming to seek consistency and technology neutrality, the Administration proposes to change only aspects of FISA that serve as checks upon its discretion. The Administration accepts unquestioningly those elements of FISA that accord it broad latitude. The result would be a law that is still inconsistent and outdated, but far less protective of the rights of Americans. If there is truly a need to revise FISA, then the reconsideration of Congress' 1978 choices must proceed systematically, not on the basis of a one-sided selectivity. As we explain below, careful consideration should be given to two fundamental elements of FISA: its distinction between wire and radio communications and its distinction between targeted and untargeted surveillance. Consideration should also be given to two areas in which the relationship between FISA and other privacy laws is unclear and may give the Administration unjustified latitude: the relationship between FISA and the criminal statute protecting sensitive transactional data, and the relationship between the FISA and the protections accorded stored communications and records under the Electronic Communications Privacy Act.

### **I. Changes in Technology Require Stronger, Not Weaker, Standards**

The Administration justifies its bill largely on the ground that changes in technology have made FISA outdated. Of course, technology has changed since 1978, but that begs the question of whether FISA should be weakened in response. The Administration never actually explains what technology changes have taken place since 1978, nor does it explain why any such changes justify weakening FISA.

A balanced analysis would show that various technological changes since 1978 require stronger rather than weaker FISA standards.

Perhaps the major change since 1978 that affects FISA is the globalization of personal and economic life, paralleled by the central role of global electronic communications networks in commerce, interpersonal relationships, and the full range of human pursuits. In 1978, it was a rarity for an American citizen to make an international phone call or send an international telegram. In 1978, the signals intelligence activities of the National Security Agency collected some international calls of Americans, but it was pretty rare. Today, interception of communications into and out of the US is likely to pick up the communications of many average American citizens and permanent resident aliens, who are far more likely than in 1978 to have legitimate business dealings overseas or to use the Internet and telephone to keep in touch with relatives overseas. The parent calling her daughter during her junior year abroad, the Chicago lawyer talking to his partner in Brussels, and the small Texas manufacturer with a parts supplier in Vietnam

are all entitled to a reasonable expectation of privacy in their international communications. Far more than in 1978, signals intelligence activity directed at communications entering and leaving the United States is likely to interfere with the privacy of Americans, which means that it must be carefully controlled.

Secondly, while there has been a huge increase in the volume of international communications, there have also been huge increases in computer processing power, making it possible for the government to process more data than ever before. Everything we know about the digital revolution indicates that, on balance, it has been a windfall for the snoopers: 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. The intelligence agencies are in constant danger of drowning in this information, but they are also constantly improving their processing and analytic capabilities. On balance, the question of volume may be a wash: the agencies have a lot more data to deal with, and they have a lot more ability to handle it. The challenge is daunting, and vital to our national security, but it is hard to see how mere volume justifies lower standards for surveillance of calls to and from Americans in the United States. If anything, the increasing amount of information about our daily lives that is exposed to electronic surveillance calls for stronger, not weaker standards.

A third major technological change is the revolutionary growth of the Internet. Some aspects of the Internet's development, especially the routing of a large percentage of international traffic 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. Other aspects of the Internet cited by the Administration – such as General Hayden's assertion that “there are no area codes on the Internet” – may not be entirely accurate and, even if true, require close scrutiny to determine what effect they actually have on electronic surveillance activities carried out in the United States. (FISA only applies to surveillance inside the United States.)

A fourth major change – one alluded to by the Administration -- is the shift to fiber cables as the dominant means of long distance and international carriage. As we will discuss below, the government's argument hinges on the fact that Congress, in 1978, deferred regulating NSA's interception of the satellite portion of international voice communications. Now, the Administration is arguing that radio's temporary exemption should be made permanent and extended to wire communications as well. This is an extraordinary argument: Essentially the Administration is claiming that Americans never had a privacy right for their international satellite calls and that now, just as Americans have become dependent on the Internet to participate in the global economy, they should not have a privacy right for international communications carried by wire either. CDT believes that, if it is time to reconsider FISA's “radio exception,” it should be to repeal the exception and extend privacy protections to all of the international communications of Americans, not to eliminate privacy protections across the board.

In addition, the Administration never actually explains why the shift to fiber optics requires a lowering of privacy standards for intercepting the international

communications of Americans. The fact that fiber cables are hard to tap into is irrelevant for purposes of FISA, since, as we noted, FISA applies only inside the United States, where the government does not have to tap into the middle of a cable, because it can compel the cooperation of the service provider at the network operator's switching facility. FISA specifically states that a court order, upon request of the government, shall require any communications carrier to provide "forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance." 50 USC 1805(c)(2)(B).

A fifth technology change merits separate highlighting, and that is the development and deployment of new generations of surveillance-enhancing technology by telephone companies and other communications service providers. Partly, the development of tools to facilitate the interception of advanced technologies is business-driven. Network operators need to be able to trace, isolate and analyze communications to manage their networks, for billing purposes, maintenance, quality control, and security. Other developments are driven by intellectual property concerns, as companies develop means of scanning vast data flows looking for copyrighted material.

Another driver has been legislation like CALEA, the Communications Assistance for Law Enforcement Act of 1994, which specifically requires all communications common carriers to design their systems to make them wiretap friendly. European countries have similar (in some cases more onerous) requirements, and both American standards bodies and the European Telecommunications Standards Institute have developed standards to guide equipment developers. In August 2005, the Federal Communications Commission extended CALEA to broadband Internet access providers and providers of interconnected VoIP (Voice over Internet Protocol) providers.

For these and other reasons, a growing number of companies are developing tools and services to intercept Internet traffic and other advanced communications. One company, for example, notes that its surveillance technology for broadband Internet service providers and ISPs "is highly flexible, utilizing either passive probes or active software functionality within the network nodes to filter out traffic of interest."<sup>1</sup> Cisco has developed what it calls the "Service Independent Intercept Architecture," which uses existing network elements and offers an "integrated approach that limits the intercept activity to the router or gateway that is handling the target's IP traffic and only activates an intercept when the target is accessing the network."

<http://www.cisco.com/technologies/SII/SII.pdf> VeriSign and Aqsacom are two other companies offering comprehensive services for interception of traditional and packet-based network deployments.<sup>2</sup>

---

<sup>1</sup> VERINT Systems, Inc., STAR-GATE for Broadband Data and ISP, [http://www.verint.com/lawful\\_interception/gen\\_ar2a\\_view.cfm?article\\_level2\\_category\\_id=7&article\\_level2a\\_id=59](http://www.verint.com/lawful_interception/gen_ar2a_view.cfm?article_level2_category_id=7&article_level2a_id=59)

<sup>2</sup> <http://www.verisign.com/products-services/communications-services/connectivity-and-interopability-services/calea-compliance/index.html>; <http://www.aqsacomna.com/us/>.

The relevance to intelligence agencies of these tools, developed for business or law enforcement purposes, is a question that merits examination. It is sufficient for our purposes here to note that such tools exist, and they provide a counterweight to the Administration's claims that technology has made its task more difficult. The availability of these tools is particularly relevant to FISA, since, as we noted above, FISA applies only in the US, where the government has the legal authority to compel the cooperation of service providers.

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

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 two broad categories:

### **A. 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>3</sup> If the government were targeting someone who is overseas, they

---

<sup>3</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.

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.

### **1. FISA's "Radio Exception" Should Be Repealed - 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 refer to FISA's distinction between wire and radio communications, without actually explaining it or justifying why an exception for radio portions of communications should be extended to all communications. We will explain here that the "radio exception" was meant to be temporary, that it is now clearly outdated and that it should be abolished.

When FISA was adopted, it exempted international telephone calls (and other communications) entering and leaving the US by satellite. The Administration unquestioningly accepts this exemption for the radio portion of communications and argues that it should be applied to communications carried by wire, thus exempting from privacy protection all international communications of Americans.

It is clear from FISA's legislative history that Congress intended to consider subsequent legislation to regulate interception of radio communications. The Senate Judiciary Committee's 1977 report on FISA, Rept 95-604, states:

"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 provisions of the bill certain signals intelligence activities of the National Security Agency.

Although it is desirable to develop legislative controls in this area, the Committee has concluded that these practices are sufficiently different from traditional electronic surveillance techniques, both conceptually and technologically, that, except when they target particular United States citizens or resident aliens in the United States, they should be considered separately by the Congress. The fact that this bill does not bring these activities within its purview, however, should not be viewed as congressional authorization of such activities." P. 34.

"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. This language insures that certain electronic surveillance activities targeted against international communications for foreign intelligence purposes will not be prohibited absolutely *during the interim period* when the activities are not regulated by chapter 120 and charters for intelligence agencies and legislation regulating international electronic surveillance have not yet been developed." P. 64 (emphasis added).

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 instrument. None of those reasons appears valid today. It is clear that carriers are willing and able 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.

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 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.

**2. FISA’s Dichotomy Between Targeted vs. Non-Targeted Surveillance Should Be Eliminated in Favor of a Court Order Standard for All Methods of Selecting for Processing Communications in Which One Party Is Reasonably Likely to Be a US Person**

The Administration’s bill, without explanation, perpetuates a distinction drawn in 1978 between the targeted and untargeted interception of communications. In 1978, FISA required a warrant for the acquisition of a radio communication to or from the US only if the contents were acquired by “intentionally targeting” a particular, known US person who is in the US. (f)(1). The Administration would extend this rule to wire communications as well, thus allowing the untargeted acquisition of the communications of a US person.

The question Congress should ask is: What difference does it make to an American that the government collected, analyzed and disseminated his communications without suspecting him of any involvement in terrorism or espionage versus specifically targeting him? The privacy intrusion and the likely harm are the same regardless of whether a person’s communications are intercepted because the government was intentionally targeting him or because the government was scanning millions of calls and his were selected as suspicious based on some criteria other than his name. In either case, suspicion may fall on an American and he may face adverse consequences. And in either case, the key question should be how reliable were the selection criteria.

The origins of the distinction between targeting and non-targeting may go back to an issue of major concern at the time FISA was enacted, namely, the “watch-listing” of Americans for NSA surveillance. In the 1960s and 1970s, a practice grew up of watch-listing Americans who were politically active in opposing the Vietnam War or advocating other political positions at odds with the Administration or the views of the leadership of the FBI. One of the purposes of FISA was to prevent the watch-listing of Americans without a court order.

Today, while there are concerns that the Administration has been investigating and harassing political activists, a new concern has emerged: that the data mining and profiling activities of various agencies are causing people real harm in their daily lives. In these cases, the government is not intentionally targeting a particular, known US person. Instead, the government is casting a broad net, using computers to apply selection criteria to oceans of data and selecting out suspicion individuals.

The fact that the selection does not start with a known person does not make the process any less consequential for the privacy of the person whose communications are ultimately selected for scrutiny.

Limiting the definition of “electronic surveillance” to the intentional targeting of a particular, known person seems especially unjustified given the fact that today most selection of communications is computerized, either by the service provider at the direction of the government or by the government itself. Sometimes selection is done by name, sometimes by telephone number or email address or IP address number, and sometimes based on another set of parameters. In all cases, the government should have a solid reason to believe that its criteria will isolate communications that are to or from a foreign power or an agent of a foreign power and that will contain foreign intelligence. In all cases, whether the government uses a name, a telephone number, or a complex set of screens, the process of defining those selection criteria should be subject to judicial scrutiny, based on a finding of probable cause to believe that the communications to be processed will be those of an agent of a foreign power and will contain foreign intelligence.

The current rule and the Administration’s bill make no sense, requiring a court order when the government is selecting for interception the communications of a particular, known person but not requiring a court order when the government is selecting communications based on some other criteria. The solution, it seems, is to require a court order for all processing intended to select communications for presentation to a human being. Whether that is a name or a number or a complicated set of screens, the government is selecting for scrutiny the private communications of individuals in circumstances in which those individuals may face adverse consequences, and in our society that is precisely the type of question that should be submitted to prior judicial approval.

### **3. A Far Narrower Alternative Is Available to Meet the Concerns Expressed by the Administration**

The Administration argues that it should be unnecessary to obtain a warrant when it is targeting someone overseas. CDT has been on the record supporting an amendment to FISA that would make it clear that a warrant is not needed when the government is intercepting foreign-to-foreign communications that happen to be available inside the US. An extension of this principle would be to say that the government, when it is collecting foreign-to-foreign communications, should not have to turn off its tap if the overseas target suddenly makes a call to the US.

The simplest and narrowest change would be an exception to the current (f)(2) saying that no warrant is needed when the government, in the course of acquiring the communications of persons outside the US, incidentally collects a communication with a person in the United States. The exception could be narrowly drawn to make it clear that, if the acquisition begins to involve a significant number of communications with a person

in the US, a court order should be required on the grounds that the interception has begun to implicate the rights of an American.

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

Another section of 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.” It is completely unclear what this means. Essentially, all foreign intelligence surveillance is “directed at the acquisition of the communications of a foreign power.” The problem is that the person on the other end of the line may be a US citizen, which is why we require a court order.

The proposed change builds on the so-called “embassy exception” to FISA. But that exception was limited to circumstances where it was unlikely that the calls of a US person would be intercepted. The Administration’s change would go too far. Basically, it 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 could be intercepted without a court order.

As noted, the key language is “directed at the acquisition of the contents of communications of a foreign power.” 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.

### **III. The Committee Should Address Important Issues Regarding Access to Transactional Data and Stored Communications**

In an earlier analysis, CDT concluded that the Administration’s bill would allow the government, without court order, to intercept information identifying the source and destination of every telephone call and email sent in the US. On closer examination, it appears that our initial analysis was not correct with respect to purely domestic calls, although honestly the relationship between FISA and Title 18 is so circular that it is hard to tell. We urge the Committee to require the Administration to make clear its

interpretation of the relationship between FISA and the rules in Title 18 for the interception of transactional (non-content) data.

Surveillance law has long distinguished between the interception of the content of communications and the interception of dialing or signaling information that indicates who is communicating with whom. The Supreme Court held three decades ago – in cases that look increasingly shaky – that transactional data about calls is not constitutionally protected. Call detail records and Internet records are clearly sensitive, however; they give a full picture of a person’s associations and activities. Accordingly, Congress in 1986 required a court order for realtime interception of transactional details about telephone calls, email and other communications (using what are now computer processes but which are still called pen registers or trap and trace devices). 18 U.S.C. 3121- 3127. In criminal investigations, that court order is issued on a very low standard, less than probable cause, and without many of the additional elements of judicial and public oversight accorded to content interceptions. 18 U.S.C. 3123. CDT has long argued that the standard for collection of transactional data should be strengthened.

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, suggesting that a full FISA order is needed to collect transactional data..

In 1998, Congress amended FISA to include a new section authorizing orders in intelligence matters for pen registers and trap and trace devices. 50 U.S.C. 1842-1846. However, Congress did not amend FISA’s 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. As we now interpret the Administration’s bill, the effect of the changes would be as follows:

18 U.S.C. 3121, which is part of Chapter 206, prohibits the collection of transactional data in real-time without first obtaining a court order issued under 18 U.S.C 3123 (for criminal investigations) or under FISA. However, 18 U.S.C 2511(2)(f) provides that Chapter 206 does not affect the acquisition by the government of foreign intelligence from foreign and international communications utilizing a means other than “electronic surveillance” as defined under FISA. Since the acquisition of non-content from international communications would not be electronic surveillance under the new definitions unless the government is targeting the communications of a particular, known person in the United States, this allows the government to collect transactional information on international calls without a court order. However, 18 U.S.C 2511(2)(f) only applies to foreign and international communications, so 18 USC 2131 would

continue to require a court order for the targeted or untargeted collection of transactional information about domestic calls (as well as for targeted collection of transactional information about international calls).

We urge the committee to confirm this interpretation with the Administration on the public record, especially that 3121 requires a pen/trap order under 50 USC 1842-1846 for collection of transactional information on all domestic calls, whether the information is collected on a targeted or untargeted basis.

Of course, this allows the government access without a court order to all transactional data for international calls when the government is not targeting a particular, known person in the US, even though such data gives a rich picture of the associations and activities of US citizens. In addition, even with respect to domestic calls, FISA sets a very low standard, merely requiring the government to certify (with no factual explanation) that the information likely to be obtained is foreign intelligence not concerning a US person or is relevant to an ongoing investigation to protect against international terrorism or clandestine intelligence activities. CDT believes that this standard should be raised, to at least require the government to offer some basic facts reasonably supporting the claim that the surveillance will yield foreign intelligence or information relevant to an ongoing investigation of international terrorism or clandestine intelligence activity.

CDT also urges the Committee to determine whether the Administration reads 50 USC 1842 as requiring particularity. That is, does FISA's pen/trap standard, as amended by the PATRIOT Act, require the government to obtain pen/trap orders only on specific phone lines or email accounts used by particular persons, or has the government been obtaining FISA pen/trap orders authorizing the collection of transactional data pertaining to many individuals? Judicial oversight would be largely meaningless if the government could get pen/trap orders without particularity, i.e., without focusing on a particular individual.

The Committee should also explore reports that the Administration has been obtaining large quantities of transactional data in stored formats. If the telephone companies are turning over large volumes of transactional data on a regular basis, that would be a major evasion of the provisions of 18 USC 3121 and 50 USC. It seems to make little difference between recording massive amounts of transactional data in realtime versus acquiring that data in stored form soon after the communications.

Finally, we note that the Administration bill seems to preserve part of the inconsistency of current law, for the new (f)(1) requires a full probable cause-based court order to collect any "information" about the communication of a particular, known person who is reasonably believed to be in the United States. Thus, the Administration bill would set a higher standard for the targeted use of pen registers and trap and trace devices to collect transactional data in some national security cases than would be required in criminal cases.

#### **IV. 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.

#### **V. 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.

The alternative, bipartisan legislation introduced by Senators Feinstein and Specter, S. 1114, appears to take a far more measured approach than the radical revisions the Administration has urged.

**VI. The Administration Bill Would Deprive Communications Companies of the Certainty They Deserve When Presented with Government Surveillance Requests**

Effective government surveillance depends on the prompt cooperation of the operators of communications networks. It is appropriate that telephone companies and other operators of communications networks should be required to cooperate with court-approved electronic surveillance. However, carriers should not be placed in the position of having to evaluate the legality of each government request. The court order provision gives carriers the certainty they deserve: if the government presents a court order, the carrier must comply and will be protected from liability even if the order was improperly obtained. If the government does not have a court order, the carrier can safely and confidently decline to cooperate. What is crucial is that those companies should be afforded clear rules. Carriers should not be left guessing as to when to cooperate.

Section 408 of the bill would upset this balance and deprive communications carriers of the certainty they deserve. It would grant immunity to certain carriers who cooperated with government surveillance requests in the absence of a court order. The change would place those carriers and all other carriers in an impossible position during the next crisis: If the government approached them with a questionable request, should they cooperate in the expectation that they would later get immunity, or should they resist in the face of government claims that national security was at stake? The provision diminishes the meaning of the court order process as a means of affording companies protection.

**VII. Conclusion: 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 urges the Committee to reject this sweeping proposal. We look forward to working with the Committee to craft any needed FISA amendments on a narrow and balanced basis.