CENTER FOR
DEMOCRACY
&
TECHNOLOGY
Working for Civil Liberties on the Internet

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

Minimization Cannot Be Relied Upon to Protect the Rights of Americans under a Warrantless Surveillance Program

September 17, 2007

"Minimization" is the Administration's one word answer to concerns that the rights of American citizens will be infringed by the warrantless surveillance authority approved by Congress before its August recess in the "Protect America Act" (PAA).

Reliance on "minimization" to defend the PAA fails for two reasons:

(1) Even if "minimization" meant that the government discarded all intercepted communications of Americans – which it does not – it would not cure the damage done to privacy when the communications are intercepted in the first place. The police cannot come into your house without a warrant, look around, copy your files and then claim no constitutional violation because they threw everything away after they looked at it back at the station house.

(2) Under FISA, "minimization" does not mean that the government must discard all of the communications of people in the US "incidentally" collected when the government is targeting someone overseas. To the contrary, the "minimization" rules that would be applicable to the PAA permits the government to retain, analyze, and disseminate to other agencies the communications of people inside the US, including US citizens.

Under the "minimization" rules applicable to the PAA, the American citizen talking to relatives in Lebanon, the charities coordinator planning an assistance program for Pakistan, the businessman trading with partners in the Middle East, or the journalist gathering information about the opium trade in Afghanistan – all while sitting in the US – might have their international calls or emails monitored, recorded and disseminated without judicial approval or oversight if the NSA, in its sole discretion, decided to "target" the person they were talking to overseas.

Summary

There are two very different kinds of "minimization" under FISA. The version that applies to the surveillance authorized under the Protect America Act does not require the

NSA to discard or mask all information concerning Americans that is collected when the government is targeting foreigners. See 50 U.S.C. §1801(h)(1) – (3). **To the contrary, "minimization" gives the NSA authority to collect, retain and disseminate certain communications to which a US citizen is a party.** Anything that is foreign intelligence or evidence of crime can be retained and disseminated. Under the PAA, the NSA has the sole discretion to decide what is foreign intelligence; it has sole discretion to decide what to collect, keep and disseminate, with no judicial oversight of any stage of the process. This kind of minimization offers inadequate protection to the rights of Americans whose calls will inevitably be intercepted under the PAA without judicial approval.

A key point must be stressed: This permissive type of minimization applicable to the PAA was intended under the original FISA to operate in conjunction with a warrant, as an additional protection, not to be a substitute for a warrant. Under traditional FISA, the court approved both the initial search and the minimization procedures, and the court retained jurisdiction over the implementation of the minimization rules. Under the PAA, in contrast to most of FISA, no judge approves either the search or the minimization rules.

There is another, very different type of minimization under FISA, applicable only to a narrow sub-category of surveillance, namely the warrantless surveillance of leased lines used by foreign embassies under circumstances where it is highly unlikely that the communications of Americans will be intercepted. 50 U.S.C. §1801(h)(4). This type of minimization requires the government to promptly discard any communications to which a US person is a party or to obtain a FISA court order to retain and use them. It should be noted that the Administration is urging Congress to repeal this kind of minimization in its broader FISA "reform" bill.

This second, protective type of minimization was specifically intended to apply to warrantless surveillance, but it does not apply to warrantless surveillance under the PAA. Even if this protective type of minimization were applied to the PAA, it could not substitute for court approval of such a broad and ill-defined range of surveillance as that contemplated under the PAA.

In sum, the minimization procedures applicable to the PAA do not provide protection for the rights of Americans.

Background – The Focus of Privacy Concern in the Current Debate Is the International Communications of US Persons – That Is, Communications with One Party in the US

It has long been clear that the debate over FISA this year has not been about terrorism suspects overseas talking to other people overseas. Both Democrats and Republicans were agreed on addressing that problem by making it clear that FISA did not apply to interception of foreign-to-foreign electronic communications even if the surveillance occurred on US soil. (As a result of developments in global communications networks,

calls and Internet communications from one foreign location to another may pass through switching facilities in the US.)

Instead, the debate for the past year has been over the rights of American citizens and others inside the US, where the Constitution's special protections apply. The NSA repeatedly stresses that it wants to target persons overseas, but it is undeniably certain that some of those persons overseas will communicate with people in the US. The individuals in the US retain their reasonable expectation of privacy in their communications, including their communications with persons overseas. The government will "listen" to both ends of the communication, infringing on the privacy rights of the Americans.

Thus, the program at the center of the debate – a program legitimately intended to provide speed and agility to the NSA in targeting persons overseas, but certain to infringe on the privacy of some Americans – poses two questions: (1) how does the government decide who might be a terrorist overseas, and (2) what happens when the target overseas communicates with someone in the US?

The Administration's stock answer to both questions is that it "minimizes" the communications of the person inside the US. As we will show, minimization does not mean that the government must destroy all communications of Americans. To the contrary, minimization rules allow the government to retain and disseminate certain communications of citizens and other U.S. persons.

But no definition of minimization could answer the first question: Is the surveillance program reasonably calibrated to intercept communications of terrorists overseas (or others overseas with foreign intelligence information)? When surveillance will intrude on the privacy of persons inside the United States, the question of how to target that surveillance is one our democratic system generally commits to prior judicial review. It should be a judge who decides in the first place that the government's filtering and selection methods are reasonably designed to intercept the communications of terrorists and are not likely to unnecessarily intercept the communications of innocent Americans.[1] The question of what communications to intercept cannot be resolved by administrative procedures that limit the use of the information once it is collected.

Nor would we want an overly rigid rule limiting use of communications between persons overseas and persons in the US. The second question, which is what to do with the communications of Americans that will inevitably be intercepted, cannot be answered by a blanket rule that the NSA must ignore all those communications. If a terrorist overseas is talking to a person in the US, that might be precisely the kind of communications that

---

[1] The PAA submits the wrong question to judicial review. The PAA requires the Administration to submit to the court procedures for ensuring that the persons being targeted are outside the U.S. The question that should be reviewed by the court is whether the targeting procedures reasonably ensure that the communications being targeted will contain foreign intelligence.

we would want the NSA to keep and to disseminate to the FBI, DHS and other law enforcement and intelligence agencies. Minimization rules ***should*** allow the retention and use of some communications of Americans. That is why some independent (although not necessarily particularized) review of targeting practices is necessary upfront, and it is also why oversight of minimization practices is necessary. Picking and choosing which communications of Americans to retain and which to discard should not be left to the sole discretion of the Executive Branch. Just as the police in carrying out an ordinary search must make a return of service –that is, police must report back to the judge after the search on how they conducted the search and what they seized – so the minimization decisions of the NSA must be subject to judicial oversight.

The NSA has entered a new era. During the Cold War, the NSA had a philosophy – not actually required by law or applied in practice, but a strongly held philosophy nevertheless – that it would have nothing to do with US person data. That philosophy has been abandoned.[2] The NSA is collecting, and finding intelligence value in, a lot more communications to and from the US persons than ever before. A reasonable set of checks and balances needs to be developed for this new era. The PAA provides for none.

The Statutory Definition of Minimization

Warrantless surveillance authorized under the Protect America Act is subject to minimization procedures that meet the definition of "minimization procedures" in section 101(h) of FISA. 50 U.S.C. §1801(h). That definition states:

> (h) ``Minimization procedures'', with respect to electronic surveillance, means--
>
> > (1) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purpose and technique of the particular surveillance, to minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning un-consenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;
> >
> > (2) procedures that require that non-publicly available

[2] In its "Transition 2001" report, completed in December 2000, the NSA concluded, "The National Security Agency is prepared organizationally, intellectually and--with sufficient investment--technologically, to exploit in an unprecedented way the explosion in global communications. This represents an Agency very different from the one we inherited from the Cold War. It also demands a policy recognition that the NSA will be a legal but also a powerful and permanent presence on a global telecommunications infrastructure where protected American communications and targeted adversary communications will coexist."

> information, which is not foreign intelligence information, as defined in subsection (e)(1) of this section, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance;
>
> (3) notwithstanding paragraphs (1) and (2), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and
>
> (4) notwithstanding paragraphs (1), (2), and (3), with respect to any electronic surveillance approved pursuant to section 1802(a) of this title, procedures that require that no contents of any communication to which a United States person is a party shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1805 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

Of the four numbered paragraphs of the definition, two are restrictive, one is permissive and one applies only to surveillance pursuant to the "embassy exception." The restrictive provisions are subject to exceptions, so the overall effect of the definition is to permit the government to collect, retain and disseminate certain communications of American citizens and other US. persons.

Paragraph (1) requires the Attorney General to adopt "procedures that minimize the acquisition and retention, and prohibit the dissemination, of non-publicly available information concerning un-consenting United States persons." This restriction is limited, however, for the procedures must be "consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." In other words, the NSA can acquire, retain and disseminate to other agencies information about US persons if it constitutes "foreign intelligence information."

The FISA definition of "foreign intelligence information" is broad. It includes not only information concerning potential attacks by foreign nations or international terrorists, but also "information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to -- (A) the national defense or the security of the United States; or (B) the conduct of the foreign affairs of the United States." 50 U.S.C. §1801(e)(2).

A lot could hinge on the interpretation of what is "necessary," but there is no public definition in statute, case law or Administration guideline as to what is "necessary." Under the PAA, since the FISA court has no supervisory role over the warrantless

surveillance of international calls, the determination of what is "foreign intelligence" and what is "necessary" is left to the NSA.

Paragraph (2) of the definition of "minimization procedures" requires the NSA to redact the identity of a U.S. person before disseminating information "which is ***not*** foreign intelligence information, as defined in subsection (e)(1)" of the FISA definitions (emphasis added). This is pretty convoluted, but it apparently permits the NSA to disseminate the identity of US persons in connection with information that ***is*** foreign intelligence under (e)(1), which is the prong of the definition of foreign intelligence information that relates to international terrorism. In other words, if the information ***is*** foreign intelligence under (e)(1), paragraph (2) provides no protection to the U.S. person. Also, paragraph (2) clearly permits NSA to disseminate **any** intelligence concerning US persons so long as it redacts the identity of the U.S. person. General Hayden described the redaction process in his 2005 confirmation hearing:

> … it is not uncommon for us to come across information to, from or about what we would call a protected person--a U.S. person. … The rule of thumb in almost all cases is that you minimize it, and you simply refer to ``named U.S. person'' or ``named U.S. official'' in the report that goes out. http://www.fas.org/irp/congress/2005_hr/shrg109-270.pdf p. 20.

So minimization doesn't mean that NSA has to purge the identity of the US person from its files. The information remains in storage along with the identifying information, which is available for later search and retrieval. Officials at other agencies can request the names of U.S. persons that were redacted from NSA reports. *Newsweek* reported in May 2006 that between January 2004 and May 2006, the agency had supplied the names of some *10,000* American citizens to various interested officials in other agencies.[3]

Finally, paragraph (2) permits the NSA to disseminate identifying information about a US person when it is "necessary to understand foreign intelligence information or assess its importance." It has been reported that, after 9/11, the head of the NSA changed internal interpretations of the redaction procedures to allow routine dissemination of identifying information about US persons, presumably on the ground that information identifying U.S. persons was necessary for the FBI and other agencies to follow-up on the intelligence.[4] Indeed, under the NSA's new practice, the FBI was flooded with

---

[3] http://www.msnbc.msn.com/id/7614681/site/newsweek/. The practice came to light most recently when U.N. ambassador nominee John Bolton explained to a Senate confirmation hearing that he had requested that the names of U.S persons be unmasked from NSA intercepts on 10 occasions when he was at the State Department.

[4] Eric Lichtblau and Scott Shane, "Files Say Agency Initiated Growth of Spying Effort." *New York Times*, January 4, 2006. In the context of court-authorized surveillance, this may have been appropriate. For a discussion of the dissemination of identifying information, see the recommendation on "authorized use" in the Third Report of the Markle Task Force on National Security in the Information Age. It is unclear whether the

information identifying U.S. persons.[5]

Paragraph (3) of the minimization definition allows the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed, with all identifiers intact.

Paragraph (4) is the only provision that requires the government to delete communications to which a person is a party within 72 hours. This applies only to communications intercepted under FISA's leased line exception (sometimes called the "embassy exception"). It is inapplicable to surveillance authorized by the PAA.

It is important to note that the Administration's broader FISA "reform" bill, which it promises to push this fall, would repeal paragraph (4). See Administration April 2007 proposal, page 4 of 66 http://www.cdt.org/security/nsa/Bush2007FISAbill.pdf. In other words, the Administration would repeal the only provision of FISA that actually requires it to discard communications of US persons.[6]

Suzanne Spaulding, former Minority Staff Director for the House Intelligence Committee and former Assistant General Counsel at CIA, argued in her September 5 testimony to the House Judiciary Committee that the protective type of minimization in paragraph (4) should be extended to the PAA. However, even the strictest form of minimization would not be a substitute for prior court approval in light of how broad and ill defined is the range of surveillance contemplated under the PAA (and Spaulding did not suggest otherwise). Moreover, while it was expected that the "embassy exception" would almost never result in the interception of the communications of Americans, it *is* expected that the surveillance authorized by the PAA will sweep in a number of international communications to which an American is a party. Almost certainly, some of these foreign-to-domestic communications will contain foreign intelligence. Because it will be much more frequently necessary to decide which U.S. person communications to retain and which to discard, any minimization rules applicable to the surveillance of communications between people overseas and people in the US should be subject to judicial approval and monitoring. Yet the PAA denies the FISA court the power to review the minimization rules for the program or monitor their application. The Reyes-

---

Administration intends to apply these same liberal dissemination rules to information acquired under the PAA, which is likely to result in an increase in the collection of information identifying US persons.

[5] Lowell Bergman, Eric Lichtblau, Scott Shane and Don Van Natta Jr, "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends," *New York Times* (January 17, 2006).

[6] The Administration bill would also vastly expand the scope of the so-called embassy exception, *id.* at pp. 5-6, so that the government could, without a warrant, intercept, retain and disseminate many more domestic-to-domestic calls, including calls to, from and between citizens in the US.

Rockefeller bill presented a workable approach for judicial approval and ongoing judicial oversight of surveillance programs that will likely intercept communications with US persons can be found in the Reyes-Rockefeller draft.

In sum, the FISA definition of "minimization" permits the NSA to collect, retain and disseminate throughout the government any information extracted from the communications of US citizens that the NSA believes is foreign intelligence or evidence of a crime. Under the PAA, that judgment is left solely to the discretion of the NSA. There are no checks and balances against NSA mistakes.

USSID 18

Further detail about minimization is found in United States Signals Intelligence Directive 18. This is a major document prescribing policies and procedures for conducting signals intelligence activities affecting the US persons. A redacted, declassified version of USSID 18 issued in 1993, by DNI McConnell when he was Director of NSA, is online at http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB23/07-01.htm. There may have been amendments since then, but it is probably safe to assume that they are no more restrictive (privacy protective) than the 1993 version.

There is no requirement that USSID 18 apply to surveillance under the PAA. However, the guideline reaffirms that minimization permits the retention and dissemination of communications of Americans inadvertently collected when targeting persons overseas.[7]

One of the more interesting provisions of USSID 18 is Section 6, which describes the circumstances in which communications to, from, or about US persons can be retained. The authority specifically permits retention of communications in databases for "traffic analysis":

> Except as otherwise provided in Annex A, Appendix 1, Section 4, communications to, from or about U.S. PERSONS that are intercepted by the USSS may be retained in their original or transcribed form only as follows:
>
> (1) Unenciphered communications not thought to contain secret meaning may be retained for five years unless the DDO determines in writing that retention for longer periods is required to respond to authorized FOREIGN INTELLIGENCE requirements.
> (2) Communications necessary to maintain technical data bases for cryptanalytic or traffic analysis purposes may be retained for a period

[7] USSID 18 and its Annexes contain revealing, and not always intuitive, definitions of "collection," "interception," and "acquisition" that may give the NSA quite broad discretion to record international communications for later processing.

> sufficient to allow a thorough exploitation and to permit access to data that are, or are reasonably believed likely to become, relevant to a current or future FOREIGN INTELLIGENCE requirement. … If a U.S. PERSON'S identity is not necessary to maintaining technical databases, it should be deleted or replaced by a generic name when practicable.

Congress should look into the current scope of these NSA "technical data bases."[8]

Minimization Must Be Measured Against Something, Butt the PAA is Without Standards

Minimization is part of the constitutional essence of a reasonable search. It is the way that the government complies with the fundamental requirement that a search must be confined to the grounds that justified it in the first place. If a search is pursuant to a warrant, the scope of the search must be limited to that specified in the warrant. If a search is conducted without a warrant, "[t]he scope of the search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible." Terry v. Ohio, 392 U.S. 1, 17 (1968). In United States v. Ross, the Supreme Court said, "The scope of a warrantless search ... is defined by the object of the search and the place in which there is probable cause to believe that it may be found." 456 U.S. 798, 820 (1982). *See also* Horton v. California, 496 U.S. 128, 139 (1990) ("a warrantless search [must] be circumscribed by the exigencies which justify its initiation").

Minimization, therefore, must relate to something – there must be some parameters for the search against which minimization can be measured. One of the reasons why the PAA is almost certainly unconstitutional is because it authorizes searches inside the US with no criteria other than "the acquisition of foreign intelligence concerning persons reasonably believed to be outside the United States." Even if one were to accept the argument that a court order is not be required in some cases for national security searches, it seems highly unlikely that a warrantless search program intruding on the communications privacy of Americans could be justified solely on the ground that the surveillance was intended to collect foreign intelligence concerning persons overseas with no guidance on how to identify those persons and communications. Looking at every international communication as a way of finding foreign intelligence is a blanket search.

---

[8] Under Section 5 of the FISA court minimization procedures appended to USSID 18, even domestic communications that are reasonably believed to contain technical data base information may be disseminated to the FBI and to other elements of the U.S. SIGINT system.

Minimization Is Not a Substitute for Judicial Approval

One of the seminal wiretap cases, Katz v. US, 389 U.S. 347 (1967), made it clear that minimization does not make a warrantless search constitutional. In Katz, the government agents had probable cause. They limited their surveillance in scope and duration to the specific purpose of establishing the contents of the target's unlawful communications. They took great care to overhear only the conversations of the target himself. On the single occasion when the statements of another person were inadvertently intercepted, the agents refrained from listening to them. None of this saved the surveillance constitutionally. The Supreme Court said:

> It is apparent that the agents in this case acted with restraint. Yet the inescapable fact is that this restraint was imposed by the agents themselves, not by a judicial officer. They were not required, before commencing the search, to present their estimate of probable cause for detached scrutiny by a neutral magistrate. They were not compelled, during the conduct of the search itself, to observe precise limits established in advance by a specific court order. Nor were they directed, after the search had been completed, to notify the authorizing magistrate in detail of all that had been seized. In the absence of such safeguards, this Court has never sustained a search upon the sole ground that officers reasonably expected to find evidence of a particular crime and voluntarily confined their activities to the least intrusive means consistent with that end. Searches conducted without warrants have been held unlawful "notwithstanding facts unquestionably showing probable cause," Agnello v. United States, 269 U.S. 20, 33 , for the Constitution requires "that the deliberate, impartial judgment of a judicial officer . . . be interposed between the citizen and the police . . . ." Wong Sun v. United States, 371 U.S. 471, 481 -482. "Over and again this Court has emphasized that the mandate of the [Fourth] Amendment requires adherence to judicial processes," United States v. Jeffers, 342 U.S. 48, 51 … . [389 U.S. at 356 – 357]

Conclusion

In many ways, minimization is reminiscent of "the Wall" – a widely misunderstood rule, rigidly but unevenly applied, that does not well serve either national security or civil liberties.

The effort to define workable, truly protective minimization rules cannot be abandoned. Minimization is part of the constitutional reasonableness standard, which provides the rock-bottom minimum for all government searches infringing upon a privacy interest. Minimization is also desirable operationally: in some ways, it is part of the selection and filtering process of separating relevant from irrelevant information that is the heart of the intelligence process.

We do not question the good faith of NSA employees, who have always taken pride in their scrupulous approach to U.S person data. However, these employees operate under tremendous pressure. In the new age of terror, minimization committed to the NSA's discretion cannot be relied upon to fully protect the rights of Americans. The factors impinging on NSA's work include:

- The targets are poorly defined: Given the fragmented, decentralized nature of the terrorist threat, the government often may not have precise targeting criteria. If we are looking for needles in a haystack, we don't even have a good idea of what a needle looks like anymore. As a result, the government feels compelled to intercepts and analyzes a lot of communications whose intelligence significance is uncertain.
- The haystack is enormous: The blessing and the curse of the digital revolution is that there is so much information readily available to the government.
- The threshold for action has been lowered: Given the risk of catastrophic attack, information about ambiguous and in fact innocent matters will be disseminated and acted upon and individuals will suffer consequences of mistaken inferences.

In this environment, the NSA is acquiring and disseminating significantly larger quantities of conversations to which a U.S person is a party, and it is more likely that the NSA is analyzing and disseminating information about seemingly relevant but in fact innocent behavior. As more information about citizens and other U.S persons is being relied upon to make decisions directly affecting individuals, checks and balances are needed at each step of the process.

The terrorist watch list is a perfect example of how this new intelligence environment can affect ordinary Americans. The watch list now contains over 700,000 entries, created on the basis of reports from a range of intelligence agencies. The list is growing at the rate of 20,000 entries a month. A recent study by the Department of Justice Inspector General found that, even after vetting by the Terrorist Screening Center, 38% of the records on the list contained errors or inconsistencies. In 20% of the cases that have been resolved where members of the public complained that they were inappropriately lists, the complaint was resolved by entirely removing the name from the watchlist. The list, however, is secret. Individuals must guess as to whether they are on it in order to seek redress.[9] The list is used not only as the basis for the passenger-screening program that affects 1.8 million air travelers a day. The watchlist feeds into the Violent Gang and Terrorist Organization File, which is made available through the NCIC to over 60,000 state and local criminal justice agencies and may be relied upon by police in ordinary encounters with citizens on a daily basis.

---

[9] Ellen Nakashima, "Terrorism Watch List Is Faulted For Errors," Washington Post September 7, 2007 at p. A12. The IG report is at http://www.usdoj.gov/oig/reports/FBI/a0741/final.pdf.

In this environment, we need lots of checks and balances. Minimization is part of that. But minimization is not enough, constitutionally or practically. And minimization defined and applied solely at the discretion of the Executive Branch is clearly not enough.

For more information, contact Jim Dempsey (202) 365-8026 or Greg Nojeim (202) 637-9800 x 113.