



Testimony of Jameel Jaffer  
Deputy Legal Director of the  
American Civil Liberties Union Foundation

Before  
The House Committee on the Judiciary  
Subcommittee on Crime, Terrorism, and Homeland Security

Oversight Hearing on  
The FISA Amendments Act of 2008

May 31, 2012

On behalf of the American Civil Liberties Union (ACLU), its hundreds of thousands of members, and its fifty-three affiliates nationwide, thank you for inviting me to testify before the Subcommittee. As you know, the FISA Amendments Act of 2008 will expire in December unless Congress reauthorizes it. For the reasons explained below, Congress should not reauthorize the Act without prohibiting dragnet surveillance of Americans' communications and strengthening minimization requirements, and it should not reauthorize the Act in any form unless and until the executive branch discloses basic information about how the law has been interpreted and used.

The FISA Amendments Act is unconstitutional because it allows the mass acquisition of U.S. citizens' and residents' international communications. Although the Act prohibits the government from intentionally "targeting" people inside the United States, it places virtually no restrictions on the government's targeting of people outside the United States, even if those targets are communicating with U.S. citizens and residents. The Act's effect is to give the government nearly unfettered access to Americans' international communications. It permits the government to acquire these communications:

- Without requiring it to specify the people, facilities, places, premises, or property to be monitored;
- Without requiring it to obtain individualized warrants based on criminal or foreign intelligence probable cause, or even to make prior administrative

determinations that the targets of government surveillance are foreign agents or connected in any way, however tenuously, to terrorism; and

- Without requiring it to comply with meaningful limitations on the retention and dissemination of acquired information.

Congress should not reauthorize the Act without prohibiting the dragnet surveillance of U.S. persons' communications and more narrowly restricting the circumstances in which Americans' communications can be acquired, retained, used, and disseminated.

Further, Congress should not reauthorize the Act in *any* form without first requiring the executive branch to make public more information about its interpretation and use of the Act. The executive branch has not disclosed to the public the number of times the Director of National Intelligence (DNI) and the Attorney General have invoked the Act, the number of U.S. persons who have been unlawfully targeted, or the number of U.S. persons whose communications have been collected in the course of surveillance nominally directed at non-U.S. persons outside the country.<sup>1</sup> It has not disclosed any legal memoranda in which the executive branch has interpreted the authorities granted by the Act; nor has it disclosed, even in part, any relevant opinions issued by the Foreign Intelligence Surveillance Court ("FISA Court"). Given the Act's implications for Americans' privacy rights, it is unacceptable that even this basic information is being withheld from the public and most members of Congress.<sup>2</sup> The secrecy surrounding the Act extends far beyond the executive's legitimate interest in protecting sources and methods.

The little that we do know about the executive's implementation and use of the Act is deeply troubling. Records obtained by the ACLU show that agencies conducting surveillance under the Act have repeatedly violated targeting and minimization procedures, meaning that they have improperly collected, retained, or disseminated U.S. persons' communications. At one point the FISA Court, apparently frustrated with the executive's repeated violations of the Act's limitations, ordered the Justice Department to provide reports every 90 days describing "compliance issues." The *New York Times* reported in 2009 that the National Security Agency (NSA) had "intercepted private e-mail messages and phone calls of Americans . . . on a scale that went beyond the broad

---

<sup>1</sup> The Director of Legislative Affairs for the Office of the Director of National Intelligence wrote last year that "it is not reasonably possible to identify the number of people located in the United States whose communications may have been reviewed under the Authority of the [FISA Amendments Act]." Letter from Kathleen Turner, Director of Legislative Affairs, Office of the DNI, to Senators Ron Wyden and Mark Udall (July 26, 2011), *available at* <http://bit.ly/LYC77M>.

<sup>2</sup> Some of this information has reportedly been made available to the intelligence committees. There is no good reason, however, why this same information should not be made available to Congress more generally and to the American public – with redactions, if necessary, to protect sources and methods.

legal limits established by Congress,” and that the “‘overcollection’ of domestic communications” was “significant and systemic.”<sup>3</sup> We urge Congress not to reauthorize the Act in any form without first requiring the executive to disclose more information about how the Act has been interpreted and used.

## **I. FISA, the Warrantless Wiretapping Program, and the 2007 FISA Orders**

In 1978, Congress enacted FISA to regulate government surveillance conducted for foreign intelligence purposes. The statute created the FISA Court and empowered it to grant or deny government applications for surveillance orders in foreign intelligence investigations.<sup>4</sup> Congress enacted FISA after the Supreme Court held, in *United States v. U.S. District Court*, 407 U.S. 297 (1972), that the Fourth Amendment does not permit warrantless surveillance in intelligence investigations of domestic security threats. FISA was a response to that decision and to a congressional investigation that revealed that the executive branch had engaged in widespread warrantless surveillance of U.S. citizens—including journalists, activists, and members of Congress—“who engaged in no criminal activity and who posed no genuine threat to the national security.”<sup>5</sup>

Congress has amended FISA multiple times. In its current form, the statute regulates, among other things, “electronic surveillance,” which is defined to include:

the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States.<sup>6</sup>

Before passage of the FAA, FISA generally foreclosed the government from engaging in “electronic surveillance” without first obtaining individualized and particularized orders from the FISA Court. To obtain an order, the government was required to submit an application that identified or described the target of the surveillance; explained the government’s basis for believing that “the target of the electronic surveillance [was] a foreign power or an agent of a foreign power”; explained the government’s basis for believing that “each of the facilities or places at which the electronic surveillance [was] directed [was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power”; described the procedures the government would use to “minimiz[e]” the acquisition, retention, and dissemination of non-publicly available information concerning U.S. persons; described the nature of the foreign intelligence information sought and the type of communications that would be subject to

---

<sup>3</sup> Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. Times, Apr. 16, 2009, available at <http://nyti.ms/LBPPrn>.

<sup>4</sup> 50 U.S.C. § 1803(a).

<sup>5</sup> S. Rep. No. 95-604(I), at 6 (1977), reprinted in 1978 U.S.C.C.A.N. 3904, 3909 (internal quotation marks omitted).

<sup>6</sup> 50 U.S.C. § 1801(f)(2).

surveillance; and certified that a “significant purpose” of the surveillance was to obtain “foreign intelligence information.”<sup>7</sup> The FISC could issue such an order only if it found, among other things, that there was “probable cause to believe that the target of the electronic surveillance [was] a foreign power or an agent of a foreign power,” and that “each of the facilities or places at which the electronic surveillance [was] directed [was] being used, or [was] about to be used, by a foreign power or an agent of a foreign power.”<sup>8</sup>

In late 2001, President Bush secretly authorized the NSA to inaugurate a program of warrantless electronic surveillance inside the United States. President Bush publicly acknowledged the program after *The New York Times* reported its existence in December 2005. According to public statements made by senior government officials, the program involved the interception of emails and telephone calls that originated or terminated inside the United States. The interceptions were not predicated on judicial warrants or any other form of judicial authorization; nor were they predicated on any determination of criminal or foreign intelligence probable cause. Instead, according to then-Attorney General Alberto Gonzales and then-NSA Director Michael Hayden, NSA “shift supervisors” initiated surveillance when in their judgment there was a “reasonable basis to conclude that one party to the communication [was] a member of al Qaeda, affiliated with al Qaeda, or a member of an organization affiliated with al Qaeda, or working in support of al Qaeda.”<sup>9</sup>

On January 17, 2007, then-Attorney General Alberto Gonzales publicly announced that a judge of the FISA Court had effectively ratified the warrantless wiretapping program and that, as a result, “any electronic surveillance that was occurring as part of the [program] will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court.”<sup>10</sup> The FISA Court orders issued in January 2007, however, were modified in the spring of that same year. The modifications reportedly narrowed the authority that the FISA Court had extended to the executive branch in January. After these modifications, the administration pressed Congress to amend FISA to permit the warrantless surveillance of Americans’ international communications in certain circumstances.

---

<sup>7</sup> *Id.* § 1804(a) (2006). “Foreign intelligence information” was (and still is) defined broadly to include, among other things, information concerning terrorism, national security, and foreign affairs.

<sup>8</sup> 50 U.S.C. § 1805(a)(2)(B).

<sup>9</sup> Alberto Gonzales, Attorney General, Press Briefing by Attorney General Alberto Gonzales and General Michael Hayden, Principal Deputy Director for National Intelligence (Dec. 19, 2005), *available at* <http://bit.ly/JSLH4Z>.

<sup>10</sup> Letter from Alberto Gonzales, Attorney General, to Senators Patrick Leahy and Arlen Specter (Jan. 17, 2007), *available at* <http://bit.ly/JSMPWu>.

## II. The FISA Amendments Act of 2008

President Bush signed the FAA into law on July 10, 2008.<sup>11</sup> While leaving FISA in place for purely domestic communications, the FAA revolutionized the FISA regime by permitting the mass acquisition, without individualized judicial oversight or supervision, of Americans' international communications. Under the FAA, the Attorney General and Director of National Intelligence ("DNI") can "authorize jointly, for a period of up to 1 year . . . the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information."<sup>12</sup> The government is prohibited from "intentionally target[ing] any person known at the time of the acquisition to be located in the United States," but an acquisition authorized under the FAA may nonetheless sweep up the international communications of U.S. citizens and residents.<sup>13</sup>

Before authorizing surveillance under § 1881a—or, in some circumstances, within seven days of authorizing such surveillance—the Attorney General and the DNI must submit to the FISA Court an application for an order (hereinafter, a "mass acquisition order").<sup>14</sup> A mass acquisition order is a kind of blank check, which once obtained permits—without further judicial authorization—whatever surveillance the government may choose to engage in, within broadly drawn parameters, for a period of up to one year. To obtain a mass acquisition order, the Attorney General and DNI must provide to the FISA Court "a written certification and any supporting affidavit" attesting that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, "targeting procedures" reasonably designed to ensure that the acquisition is "limited to targeting persons reasonably believed to be located outside the United States," and to "prevent the intentional acquisition of any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States."<sup>15</sup> The certification and supporting affidavit must also attest that the FISA Court has approved, or that the government has submitted to the FISA Court for approval, "minimization procedures" that meet the requirements of 50 U.S.C. § 1801(h) or § 1821(4). Finally, the certification and supporting affidavit must attest that the Attorney General has adopted "guidelines" to ensure compliance with the limitations set out in § 1881a(b); that the targeting procedures, minimization procedures, and guidelines are consistent with the Fourth Amendment; and that "a significant purpose of the acquisition is to obtain foreign intelligence information."<sup>16</sup>

---

<sup>11</sup> The FISA Amendments Act replaced the Protect America Act, which President Bush signed into law on August 5, 2007.

<sup>12</sup> 50 U.S.C. § 1881a(a).

<sup>13</sup> *Id.* § 1881a(b)(1).

<sup>14</sup> *Id.* § 1881a(a), (c)(2).

<sup>15</sup> *Id.* § 1881a(g)(2)(A)(i).

<sup>16</sup> *Id.* § 1881a(g)(2)(A)(iii)–(vii).

Importantly, the Act does not require the government to demonstrate to the FISA Court that its surveillance targets are foreign agents, engaged in criminal activity, or connected even remotely with terrorism. Indeed, the statute does not require the government to identify its surveillance targets at all. Moreover, the statute expressly provides that the government’s certification is not required to identify the facilities, telephone lines, email addresses, places, premises, or property at which its surveillance will be directed.<sup>17</sup>

Nor does the Act place meaningful limits on the government’s retention, analysis, and dissemination of information that relates to U.S. citizens and residents. The Act requires the government to adopt “minimization procedures,”<sup>18</sup> that are “reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons.”<sup>19</sup> The Act does not, however, prescribe specific minimization procedures or give the FISA Court any authority to oversee the implementation of those procedures. Moreover, the FAA specifically allows the government to retain and disseminate information—including information relating to U.S. citizens and residents—if the government concludes that it is “foreign intelligence information.”<sup>20</sup> The phrase “foreign intelligence information” is defined broadly to include, among other things, all information concerning terrorism, national security, and foreign affairs.<sup>21</sup>

As the FISA Court has itself acknowledged, its role in authorizing and supervising FAA surveillance is “narrowly circumscribed.”<sup>22</sup> The judiciary’s traditional role under the Fourth Amendment is to serve as a gatekeeper for particular acts of surveillance, but its role under the FAA is simply to issue advisory opinions blessing in advance the vaguest of parameters, under which the government is then free to conduct surveillance for up to one year. The FISA Court does not consider individualized and particularized surveillance applications, does not make individualized probable cause determinations, and does not supervise the implementation of the government’s targeting or minimization procedures. In short, the role that the FISA Court plays under the FAA bears no resemblance to the role that it has traditionally played under FISA.

The FISA Amendments Act is unconstitutional. The Act violates the Fourth Amendment by authorizing warrantless and unreasonable searches. It violates the First Amendment because it sweeps within its ambit constitutionally protected speech that the

---

<sup>17</sup> *Id.* § 1881a(g)(4).

<sup>18</sup> *Id.* § 1881a.

<sup>19</sup> *Id.* §§ 1801(h)(1), 1821(4)(A).

<sup>20</sup> *Id.* § 1881a(e) (referring to *id.* §§ 1801(h)(1), 1821(4)(A)).

<sup>21</sup> *Id.* § 1801(e).

<sup>22</sup> *In re Proceedings Required by § 702(i) of the FISA Amendments Act of 2008*, No. Misc. 08-01, slip op. at 3 (FISA Ct. Aug. 27, 2008) (internal quotation marks omitted), available at <http://www.fas.org/irp/agency/doj/fisa/fisc082708.pdf>.

government has no legitimate interest in acquiring and because it fails to provide adequate procedural safeguards. It violates Article III and the principle of separation of powers because it requires the FISA Court to issue advisory opinions on matters that are not cases and controversies.<sup>23</sup>

On behalf of a broad coalition of advocacy, human rights, labor, and media groups, the ACLU has raised these claims in *Clapper v. Amnesty International USA*.<sup>24</sup> In August 2009, the district court dismissed the Complaint on the grounds that the plaintiffs could not establish with certainty that their communications would be monitored under the Act, but in March 2010 the United States Court of Appeals for the Second Circuit reinstated the suit. The Supreme Court recently granted the DNI's petition for *certiorari*.<sup>25</sup>

Our concerns about the Act include:

- a. The Act allows the government to collect Americans' international communications without requiring it to specify the people, facilities, places, premises, or property to be monitored.**

Until Congress enacted the FISA Amendments Act, FISA generally prohibited the government from conducting electronic surveillance without first obtaining an individualized and particularized order from the FISA court. In order to obtain a court order, the government was required to show that there was probable cause to believe that its surveillance target was an agent of a foreign government or terrorist group. It was

---

<sup>23</sup> In litigation, the government has cited *In re Directives Pursuant to Section 105B of the Foreign Intelligence Surveillance Act*, 551 F.3d 1004 (FISA Ct. Rev. 2008), in support of its argument that the FISA Amendments Act is constitutional. That decision, however, concerned surveillance that was individualized—i.e. directed at specific foreign powers or agents of foreign powers “reasonably believed to be located outside the United States.” *Id.* at 1008. Moreover, while the Court of Review concluded that the surveillance at issue was consistent with the Fourth Amendment, it reached this conclusion only after noting that the surveillance had been predicated on probable cause and a determination of necessity and had been limited in duration. *See* Letter from ACLU to Hon. John G. Koeltl (Feb. 4, 2009), *available at* [http://www.aclu.org/files/pdfs/natsec/amnesty/02\\_04\\_2009\\_Plaintiffs\\_Letter\\_re\\_In\\_Re\\_Directives.pdf](http://www.aclu.org/files/pdfs/natsec/amnesty/02_04_2009_Plaintiffs_Letter_re_In_Re_Directives.pdf).

<sup>24</sup> The plaintiffs are Amnesty International USA, Global Fund for Women, Global Rights, Human Rights Watch, International Criminal Defence Attorneys Association, *The Nation* Magazine, PEN American Center, Service Employees International Union, Washington Office on Latin America, and attorneys Daniel N. Arshack, David Nevin, Scott McKay, and Sylvia Royce. The Complaint and other legal filings are available at <http://www.aclu.org/national-security/amnesty-et-al-v-clapper-legal-documents>.

<sup>25</sup> Robert Barnes, *Supreme Court Agrees to Hear Case on Electronic Surveillance*, Wash. Post, May 21, 2012, *available at* <http://wapo.st/KZSUWY>.

also generally required to identify the facilities to be monitored. The FISA Amendments Act allows the government to conduct electronic surveillance without indicating to the FISA Court who it intends to target or which facilities it intends to monitor, and without making any showing to the Court—or even making an internal administrative determination—that the target is a foreign agent or engaged in terrorism. The target could be a human rights activist, a media organization, a geographic region, or even a country. The government must assure the FISA Court that the targets are non-U.S. persons overseas, but in allowing the executive to target such persons overseas, the Act allows it to monitor communications between those targets and U.S. persons inside the United States. Moreover, because the Act does not require the government to identify the specific targets and facilities to be surveilled, it permits the acquisition of these communications *en masse*. A single acquisition order may be used to justify the surveillance of communications implicating thousands or even millions of U.S. citizens and residents.

**b. The Act allows the government to conduct intrusive surveillance without meaningful judicial oversight.**

The Act allows the government to conduct intrusive surveillance without meaningful judicial oversight. It gives the FISA Court an extremely limited role in overseeing the government’s surveillance activities. The FISA Court does not review individualized surveillance applications. It does not consider whether the government’s surveillance is directed at agents of foreign powers or terrorist groups. It does not have the right to ask the government why it is inaugurating any particular surveillance program. The FISA Court’s role is limited to reviewing the government’s “targeting” and “minimization” procedures. And even with respect to the procedures, the FISA court’s role is to review the procedures at the outset of any new surveillance program; it does not have the authority to supervise the implementation of those procedures over time. Even at the outset of a new surveillance program, the government can initiate the program without the court’s approval so long as it submits a “certification” within seven days. In the highly unlikely event that the FISA Court finds the government’s procedures to be deficient, the government is permitted to continue its surveillance activities while it appeals the FISA Court’s order. In other words, the government can continue its surveillance activities even if the FISA Court finds those activities to be unconstitutional.

**c. The Act places no meaningful limits on the government’s retention and dissemination of information relating to U.S. citizens and residents.**

As a result of the Act, thousands or even millions of U.S. citizens and residents will find their international telephone and e-mail communications swept up in surveillance that is “targeted” at people abroad. Yet the law fails to place any meaningful limitations on the government’s retention and dissemination of information that relates to U.S. persons. The law requires the government to adopt “minimization” procedures—procedures that are “reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning

unconsenting United States persons.” However, these minimization procedures must accommodate the government’s need “to obtain, produce, and disseminate foreign intelligence information.” In other words, the government may retain or disseminate information about U.S. citizens and residents so long as the information is “foreign intelligence information.” Because “foreign intelligence information” is defined so broadly (as discussed below), this is an exception that swallows the rule.

**d. The Act does not limit government surveillance to communications relating to terrorism.**

The Act allows the government to conduct dragnet surveillance if a significant purpose of the surveillance is to gather “foreign intelligence information.” There are multiple problems with this. First, under the new law the “foreign intelligence” requirement applies to entire surveillance programs, not to individual intercepts. The result is that if a significant purpose of any particular government dragnet is to gather foreign intelligence information, the government can use that dragnet to collect all kinds of communications—not only those that relate to foreign intelligence. Second, the phrase “foreign intelligence information” has always been defined extremely broadly to include not only information about terrorism but also information about intelligence activities, the national defense, and even the “foreign affairs of the United States.” Journalists, human rights researchers, academics, and attorneys routinely exchange information by telephone and e-mail that relates to the foreign affairs of the U.S. (Consider, for example, a journalist who is researching drone strikes in Yemen, or an academic who is writing about the policies of the Chávez government in Venezuela, or an attorney who is negotiating the repatriation of a prisoner held at Guantánamo Bay.) The Bush and Obama administrations have argued that the new law is necessary to address the threat of terrorism, but the law in fact sweeps much more broadly and implicates all kinds of communications that have nothing to do with terrorism or criminal activity of any kind.

**e. The law gives the government access to some communications that are purely domestic.**

The Act prohibits the government from “intentionally acquiring any communication as to which the sender and all intended recipients are known at the time of the acquisition to be located in the United States.” The government itself, however, has acknowledged that, particularly with email communications, it is not always possible to know where the parties to the communication are located. Under the Act, the government can acquire communications so long as there is uncertainty about the location of the sender or recipient.

**f. The Act has a chilling effect on activity that is crucial to our democracy and protected by the First Amendment.**

The government’s surveillance activities have implications even for those whose communications may never be acquired. Thus, in the debate before passage of the FAA, Senator Cardin observed:

[F]ormidable, though incalculable, is the chilling effect which warrantless electronic surveillance may have on the constitutional rights of those who were not targets of surveillance, but who perceived themselves, whether reasonably or unreasonably, as potential targets. Our Bill of Rights is concerned not only with direct infringements on constitutional rights, but also with Governmental activities which effectively inhibit exercise of these rights. The exercise of political freedom depends in large measure on citizens' understanding that they will be able to be publicly active and dissent from official policy within lawful limits, without having to sacrifice the expectation of privacy they rightfully hold. Warrantless electronic surveillance can violate that understanding and impair that public confidence so necessary to an uninhibited political life.<sup>26</sup>

### **III. Implementation and Use of the FISA Amendments Act**

Publicly available information about the executive's implementation and use of the FISA Amendments Act is very limited. The executive branch has not disclosed any legal memoranda in which the executive branch has interpreted the authorities granted by the Act; nor has it disclosed, even in part, any relevant opinions issued by the FISA Court. It has not disclosed to the public the number of times the DNI and the Attorney General have invoked the Act, the number of Americans who have been unlawfully targeted, or the number of Americans whose communications have been collected in the course of surveillance nominally directed at non-Americans outside the country.<sup>27</sup>

Some of this information has reportedly been made available to the intelligence committees and FISA Court, but there is no reason why this same information—redacted to protect intelligence sources and methods, if necessary—should not be made available to the general public. The public surely has a right to know how the government interprets its surveillance authorities, and it surely has a right to know, at least in general terms, how these authorities are being used. Further, Congress cannot responsibly reauthorize a surveillance statute whose implications for Americans' privacy the executive branch refuses to explain. Oversight by the intelligence committees is crucial,

---

<sup>26</sup> Cong. Rec. S574 (Feb. 4, 2008). *Cf.* Intelligence Activities and the Rights of Americans, Book II, Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities, United States Senate, S. Rep. No. 94-755, at 96 (1976) (“Unless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature.”).

<sup>27</sup> The Director of Legislative Affairs for the Office of the DNI wrote last year that “it is not reasonably possible to identify the number of people located in the United States whose communications may have been reviewed under the Authority of the [FISA Amendments Act].” Letter from Kathleen Turner, Director of Legislative Affairs, Office of the Director of Nat'l Intelligence, to Senators Ron Wyden and Mark Udall (July 26, 2011), *available at* <http://bit.ly/LYC77M>.

but the last decade has confirmed that such oversight is not a substitute for oversight by Congress more generally or by the American public.

It is particularly important that Congress require the executive to disclose more information about its implementation and use of the Act because it is still unclear why the Act was necessary at all. As noted above, the Bush administration pressed Congress to amend FISA after the FISA Court issued orders in the spring of 2007 withdrawing or modifying January 2007 orders that had allowed the warrantless wiretapping program to continue in some form. These orders, however, have never been released.<sup>28</sup> Nor has the executive released all of the Office of Legal Counsel memoranda that were the basis for the program. Using the FOIA, the ACLU has learned that the OLC produced at least ten such memoranda. Of these, only two have been released, and one of the two is very heavily redacted.<sup>29</sup>

The limited publicly available information about the executive's implementation and use of the FISA Amendments Act supplies additional reason for concern. Using the FOIA, the ACLU has learned that multiple "assessments" conducted by the DNI and Attorney General between August 2008 and March 2010 found violations of the FAA's targeting and minimization procedures, indicating that the executive had improperly collected, retained, or disseminated Americans' communications. Some of the violations apparently concerned failures by the executive to properly assess "U.S. person status"—in other words, failures to afford U.S. persons the privacy protections that the Act mandates. At one point the FISA Court, apparently frustrated with the executive's repeated violations of the Act's limitations, ordered the Justice Department to provide reports every 90 days describing "compliance issues." The FOIA documents are heavily redacted, and accordingly it is difficult to draw firm conclusions from them. They strongly suggest, however, that the executive repeatedly collected, retained, and

---

<sup>28</sup> In August 2007, the ACLU filed a motion with the FISA Court requesting the unsealing of the January 2007 orders; any subsequent orders extending, modifying, or vacating the January 2007 orders; and any legal briefs submitted by the government in connection with the January 2007 orders or in connection with subsequent orders that extended, modified, or vacated the January 2007 orders. The motion requested that the Court make the materials public "with only those redactions essential to protect information that the Court determine[d], after independent review, to be properly classified." The FISA Court denied the motion. *In re Motion for Release of Court Records*, 526 F.Supp.2d 484 (FISA Ct. 2007).

In 2010, the Justice Department and DNI established a process to declassify FISA Court opinions that contained "important rulings of law," but the process has not resulted in the release of any opinion. See Steven Aftergood, *Move to Declassify FISA Court Rulings Yields No Results*, Secrecy News, May 29, 2012, [http://www.fas.org/blog/secrecy/2012/05/fisa\\_null.html](http://www.fas.org/blog/secrecy/2012/05/fisa_null.html).

<sup>29</sup> The two released memoranda are available here: <http://www.aclu.org/national-security/justice-department-memos-heavily-redacted-conceal-full-scope-bush-administration-s>.

disseminated communications that it was not entitled to collect, and that at least some instances of overcollection involved the communications of U.S. persons.<sup>30</sup> In light of the documents, it is not surprising that the *New York Times* reported in 2009 that the NSA had “intercepted private e-mail messages and phone calls of Americans . . . on a scale that went beyond the broad legal limits established by Congress,” and that the “‘overcollection’ of domestic communications” was “significant and systemic.”<sup>31</sup>

#### IV. Recommendations

The ACLU recommends:

1. Congress should not reauthorize the FISA Amendments Act without prohibiting the dragnet surveillance of Americans’ communications. Congress could effectively prohibit such dragnet surveillance in a variety of different ways. The ACLU is ready to work with Congress to develop a provision that respects constitutional rights while preserving the executive’s legitimate interest in monitoring communications of suspected terrorists and foreign agents.
2. Congress should not reauthorize the FISA Amendments Act without strengthening minimization requirements—i.e. more narrowly restricting the circumstances in which Americans’ communications can be acquired, retained, used, and disseminated.
3. Congress should not reauthorize the FISA Amendments Act in any form without first requiring the executive branch to disclose basic information about its implementation and use of the Act. Such information would include:
  - Statistics indicating how many times the DNI and AG have invoked the Act, how many U.S. persons have been inappropriately or unlawfully targeted, and how many U.S. persons’ communications have been collected in the course of surveillance nominally directed at non-Americans outside the country
  - Any legal memoranda in which the executive branch has interpreted the authorities granted by the Act, and any FISA Court opinions interpreting the authorities granted by the Act.
  - The January 2007 FISA Court orders that reportedly allowed the warrantless wiretapping program to continue in some form, and the spring 2007 FISA Court orders that reportedly extended, modified, or vacated the

---

<sup>30</sup> The FOIA documents are available at <http://www.aclu.org/national-security/faa-foia-documents>.

<sup>31</sup> Eric Lichtblau & James Risen, *Officials Say U.S. Wiretaps Exceeded Law*, N.Y. Times, Apr. 16, 2009, available at <http://nyti.ms/LBPPrn>.

January 2007 orders.

- The OLC memoranda that were the basis for the warrantless wiretapping program.

To the extent these records reference intelligence sources and methods, the records could be released with redactions. Congress should not, however, allow the government's legitimate interest in protecting intelligence sources and methods from disclosure to serve as a pretext for denying the public basic information about government policy that implicates Americans' constitutional rights.

Thank you for giving us the opportunity to provide our views.