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.[1] 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.[2] 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

[1] 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.

[2] 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

surveillance; and certified that a "significant purpose" of the surveillance was to obtain "foreign intelligence information."[7] 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."[8]

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."[9]

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."[10] 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 administrat0055>6tt0055f[(howe)u3nC7(e) StB(9005)2sTconducons, t

II. The FISA Amendments Act of 2008

President Bush signed the FAA into law on July 10, 2008.[11] 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."[12] 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.[13]

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").[14] 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."

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.[17]

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,"[18] that are "reasonably designed . . . to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons."[19] 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."[20] The phrase "foreign intelligence information" is defined broadly to include, among other things, all information concerning terrorism, national security, and foreign affairs.[21]

As the FISA Court has itself acknowledged, its role in authorizing and supervising FAA surveillance is "narrowly circumscribed."[22] 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

---

[17] *Id.* § 1881a(g)(4).

[18] *Id.* § 1881a.

[19] *Id.* §§ 1801(h)(1), 1821(4)(A).

[20] *Id.* § 1881a(e) (referring to *id.* §§ 1801(h)(1), 1821(4)(A)).

[21] *Id.* § 1801(e).

[22] *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.[23]

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*.[24] 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*.[25]

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

---

[23] 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.

[24] 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.

[25] 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-

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

disseminated communications that it was not entitled to collect, and that at least some instances of overcollection involved the communications of U.S. persons.