No. 17-5126

In the Supreme Court of the United States

MOHAMED OSMAN MOHAMUD,
PETITIONER
v.
UNITED STATES,
RESPONDENT.

ON PETITION FOR WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

BRIEF OF *AMICUS CURIAE* CENTER FOR CONSTITUTIONAL RIGHTS IN SUPPORT OF PETITIONER

SHAYANA KADIDAL
Counsel of Record
J. WELLS DIXON
BAHER AZMY
Center for Constitutional Rights
666 Broadway, 7th Floor
New York, NY 10012
kadidal@ccrjustice.org
(212) 614-6438

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

INTEREST OF *AMICUS CURIAE*[1]

The Center for Constitutional Rights (CCR) is a national nonprofit public interest law firm that has litigated several of the leading cases challenging post-9/11 detention, interrogation and rendition practices that violate fundamental rights, including the Guantánamo litigation, the leading case on behalf of "special interest" domestic immigration detainees, and the notorious rendition case of Canadian citizen Maher Arar. *See Rasul v. Bush*, 542 U.S. 466 (2004); *Ziglar v. Abbasi*, 137 S. Ct. 1843 (2017); *Arar v. Ashcroft*, 585 F.3d 559 (2d Cir. 2009) (*en banc*). In the course of that litigation and related work, CCR lawyers and legal staff communicated regularly by telephone and email with persons outside the United States who the government accused at some point of some association—however attenuated or unsubstantiated by evidence—with terrorism. Prior to 9/11 CCR was best known for rediscovering the Alien Tort Statute, *see Filártiga v. Peña-Irala*, 630 F.2d 876 (2d Cir. 1980), and the Center engages in a wide variety of international human rights litigation on behalf of foreign clients who face hostile political environments in their home countries.

CCR has a long history of challenging overbroad warrantless government surveillance, including in the landmark warrantless wiretapping case *United States v. United States District Court* (*Keith*), 407 U.S. 297 (1972),

---

[1] Pursuant to this Court's Rule 37.2(a), counsel of record for both parties received timely notice of *amicus curiae's* intent to file this brief; letters of consent from both parties to the filing of this brief have been submitted to the Clerk. Pursuant to this Court's Rule 37.6, *amicus* states that this brief was not authored in whole or in part by counsel for any party, and that no person or entity other than *amicus*, its members, or their counsel made a monetary contribution intended to fund the preparation or submission of this brief.

and one of the first challenges to the National Security Agency's post-9/11 program of warrantless surveillance, *Center for Constitutional Rights v. Bush*, 522 Fed. Appx. 383 (9th Cir. 2013), *cert. denied*, 134 S. Ct. 1497 (2014).

SUMMARY OF ARGUMENT

This Court has yet to rule on the constitutionality of Section 702 (50 U.S.C. § 1881a) of the FISA Amendments Act of 2008. Its constitutionality was challenged on the day of its passage by a large group of lawyers and journalists whose professional work was chilled by the new law, but that case was dismissed five years later on standing grounds, *Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013). The dismissal was based on representations by the government that it provides notice in criminal cases to defendants against whom evidence gleaned from Section 702 surveillance is used, *see* Transcript of Or. Arg., *Clapper v. Amnesty Int'l USA* (U.S. Oct. 29, 2012) at 4, ll. 12-17, and that these defendants would have "clear" standing to challenge the statute, *id.* at 4, l. 10; *see also Clapper*, 133 S. Ct. at 1154. Mr. Mohamud is one of a very small number of defendants to have received such notice in the four years since *Clapper*: the government has admitted to using Section 702-derived evidence to prosecute him.

The Court should take advantage of this rare opportunity and grant certiorari to clarify the scope of Section 702 and decide for the first time whether it is constitutional. Surveillance conducted under the statute implicates the rights not only of criminal defendants such as Mr. Mohamud, but also of any American who communicates with individuals abroad. As currently implemented, Section 702 allows for the collection, retention, and search of Americans' communications without individualized suspicion or probable cause. The targeting and min-

imization procedures that purport to protect Americans' communications are flawed and inadequate. This leaves the sensitive communications of a variety of Americans particularly vulnerable to surveillance and incidental collection under Section 702, including journalists, members of the legislative and judicial branches, and attorneys whose work routinely requires them to communicate with clients, witnesses, co-counsel, and business associates abroad.

ARGUMENT

The case now before this Court presents a ripe opportunity to decide the constitutionality of Section 702. The government used evidence derived from acquisitions made pursuant to Section 702 at Mr. Mohamud's trial. *United States v. Mohamud*, 843 F.3d 420, 431 (9th Cir. 2016). Court-ordered declassification revealed that through its targeting of a non-U.S. person, the government incidentally swept up Mr. Mohamud's communications. *Id.* at 438. It then used these incidentally-intercepted communications to obtain a FISA warrant to further surveil Mr. Mohamud. *Id.* Evidence gleaned through surveillance under this FISA warrant was used at trial.

Mr. Mohamud was notified of the derivative reliance on Section 702 after the trial had concluded, as a result of a shift in policy driven by the Solicitor General's representations in *Clapper*. *See United States v. Mohamud*, 2014 U.S. Dist. LEXIS 188804, at *8-9 (D. Or. Mar. 19, 2014); *see also* Charlie Savage, *Door May Open for Challenge to Secret Wiretaps*, N.Y. Times (Oct. 16, 2013); Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & The Right To Notice*, 54 Santa Clara L. Rev. 843, 868-72 (2015) (describing history). Mr. Mohamud represents

precisely the type of plaintiff who this Court acknowledged in *Clapper* would have standing to challenge the constitutionality of Section 702. 133 S. Ct. at 1154. Notwithstanding the extraordinarily broad use of Section 702, detailed below, there are only a handful of plaintiffs with similarly-clear standing: to our knowledge, in only seven other cases have individuals received such notices.[2]

I. Section 702 Allows for the Collection of an Enormous Quantity of Americans' International Communications

The Foreign Intelligence Surveillance Act of 1978 (FISA) created a comprehensive statutory scheme for conducting surveillance for foreign intelligence purposes. Such surveillance was predicated on individualized suspicion: the government was required to show a judge cause to believe that the target of surveillance was a foreign power or an agent of a foreign power. 50 U.S.C. § 1805(a)(2)(A). While the definition of "agent of a foreign power" in the original statute was broad enough to authorize surveillance in many instances where there would be no probable cause of criminal activity,[3] the gov-

---

[2] *See United States v. Muhtorov*, No. 12-cr-00033 (D. Colo.); *United States v. Hasbajrami*, No. 11-cr-00623 (E.D.N.Y.); *United States v. Khan*, No. 12-cr-00659 (D. Or.); *United States v. Mihalik*, No. 11-cr-0833 (S.D. Cal.); *United States v. Zazi*, No. 09-cr-663 (E.D.N.Y.); *United States v. Mohammad*, No. 15-cr-358 (N.D. Ohio) (in which multiple defendants received notice); and *United States v. Al-Jayab*, No. 16-cr-00181 (N.D. Ill.). (Hasbajrami had served most of her sentence by the time she received her notice and declined to litigate the validity of the surveillance. *See* Toomey & Kaufman, 54 Santa Clara L. Rev. at 871-72 nn. 112-116.)

[3] For example, any officer or employee of "a foreign-based political organization" whose actions affect the United States (even if the

ernment has long maintained that any U.S. person fitting the definition would colorably have committed a crime,[4] and this Court has never opined (and need not do so in this case) on whether surveillance under orders issued under the original FISA scheme would be consistent with the Fourth Amendment.

The FISA Amendments Act of 2008 (FAA) drastically expanded the government's surveillance authority. Most notably, it dispensed with the requirement to show individualized cause for suspicion to a judge. *See Clapper*, 133 S. Ct. at 1144-45. Under Section 702 of the FAA, the Attorney General and the Director of National Intelligence may authorize "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information,"[5] defined so broadly as to include any information "necessary to … the national defense or the security … [or] the conduct of the foreign affairs of the United States,"[6] by submitting a certification to the Foreign Intelligence Surveillance

---

individual is not located inside the United States) qualifies. *See* 50 U.S.C. § 1801(a)(5), (b)(1)(A).

[4] Supplemental Brief of the United States, Appendix A: Comparison of FISA and Title III, *In re Sealed Case*, No. 02-001 (FISA Ct. Rev. filed Sep. 25, 2002) ("a U.S. person may not be an 'agent of a foreign power' unless he engages in activity that either is, may be, or would be a crime if committed against the United States or within U.S. jurisdiction") *available at* https://fas.org/irp/agency/doj/fisa/092502sup.html; *In re: Sealed Case No. 02-001*, 310 F.3d 717, 723 (FIS Ct. of Rev. 2002) ("The definition … is closely tied to criminal activity.").

[5] 50 U.S.C. § 1881a(a). The persons targeted under Section 702 need not fit FISA's definition of "agent of a foreign power."

[6] 50 U.S.C. § 1801(e)(2)(A-B). There seems to be no reason why this definition as framed would not extend to information "necessary" to protect national economic "security" interests.

Court (FISC) that sets forth targeting and minimization procedures, *id.* (c)(1), (i).

The FAA allows the government to receive judicial approval of these general criteria to be used in choosing targets ("targeting procedures"), *id.* (d); the choice of particular individual targets that fit the general targeting criteria approved by the FISC is then left to the executive. Those individual targeting decisions occur without any judicial oversight: "Under the FAA, in contrast to the preexisting FISA scheme, the FISC may not monitor compliance with the targeting and minimization procedures on an ongoing basis." *Amnesty Int'l v. Clapper*, 638 F.3d 118, 125 (2d Cir. 2011), *rev'd*, 568 U.S. 398 (2013). So long as the target is a non-U.S. person[7] who is not physically located within the U.S. and fits the targeting criteria in the certification, the government can intercept and analyze all electronic communications sent and received by the target—including communications with Americans which are incidentally collected.

Rather than being constrained by the reasonableness, individualized cause and particularity requirements of the Fourth Amendment, the government's surveillance authority under the FAA is subject only to the generalized "targeting" and "minimization" protocols submitted to the FISC with each certification. *See* 50 U.S.C. § 1881a(i), (d)-(g). The targeting procedures that have been made public appear to do no more than restate what the statute already permits: the government may target any non-U.S. persons "reasonably believed" to be located outside the United States, but may not intentionally acquire any communication where *all* parties

---

[7] A "U.S. person" is a citizen of the U.S., lawful permanent resident, corporation incorporated in the U.S., or an unincorporated association of which a substantial number of members are U.S. citizens. 50 U.S.C. § 1801(i).

are *known* to be inside the country. *See, e.g.*, Ellen Nakashima, Barton Gellman & Greg Miller, *New documents reveal parameters of NSA's secret surveillance programs*, Wash. Post (Jun. 20, 2013); 2009 NSA Targeting Procedures, *available at* http://wapo.st/1VRbVLU. Minimization procedures are designed to curtail "the acquisition and retention, and prohibit the dissemination," of Americans' communications. 50 U.S.C. § 1801(h)(1); *see* 50 U.S.C. § 1881a(e). Following acquisition, NSA analysts determine whether a communication is a domestic or foreign communication[8] to or from a target and is "reasonably believed" to contain foreign intelligence information or evidence of a crime. 2016 NSA Minimization Procedures § 3(b)(3), *available at http://* bit.ly/2vM7IFl. Domestic communications can be retained if they contain foreign intelligence information, evidence of a crime, or fall under another exception permitting retention. *See id.* § 5. Foreign communications of U.S. persons that contain evidence of a crime or foreign intelligence information, or fall within one of nearly a dozen exceptions, may be retained indefinitely and disseminated. *See id.* § 6(a)-(b). Foreign communications of U.S. persons that contain neither foreign intelligence information nor evidence of a crime may nonetheless be retained for up to five years. *See id.* § 3(b)(1).

Like its targeting procedures, the FAA's minimization procedures are woefully inadequate in protecting Americans' private communications. "Minimization" traditionally refers to the set of safeguards, approved by the court issuing a warrant but applied by the eavesdropping officers, designed to restrict interception and

---

[8] A "foreign communication" is a communication that has at least one communicant outside of the United States. All other communications are domestic communications. 2016 NSA Minimization Procedures § 2(e).

recording of individuals who are not the targets of a wiretap, and of conversational topics that are not related to the cause of the investigation (or are legally privileged). Judicially-supervised minimization under Title III or FISA permits surveillance of a particular target for no more than 30 or 90 days, respectively. *See* 18 U.S.C. § 2518(5); 50 U.S.C. § 1805(d)(1). A judge assesses ongoing compliance with the minimization procedures by reviewing the circumstances under which information concerning U.S. persons was acquired, retained, or disseminated. 50 U.S.C. § 1805(d)(3). *See also* 18 U.S.C. § 2518(5).

Minimization procedures under the FAA do not even approach that level of protection. FAA minimization is qualitatively different than that required under other surveillance statutes. Under the FAA, the judiciary does not monitor compliance on an ongoing basis. The FISC reviews minimization procedures only *prospectively*, once every year when the government seeks its initial surveillance authorization. Thereafter, only the Attorney General and Director of National Intelligence are authorized to monitor and report ongoing compliance, and the FISC cannot rely on these reports to revoke its previous surveillance authorizations. *See Clapper*, 638 F.3d at 126; 50 U.S.C. §1881a(g)(2).

Indeed, allowing judicial approval for proposed programs of broad-brush surveillance that do not specify individual targets is at odds with the very idea of minimization, which was originally conceived of by this Court as a means of implementing the particularity requirement in the novel telephonic warrant context. *See Berger v. New York*, 388 U.S. 41, 56-60, 63-64 (1967) ("The need for particularity and evidence of reliability in the showing required when judicial authorization of a search is sought is especially great in the case of eavesdropping[, because b]y its very nature eavesdropping involves an intrusion

on privacy that is broad in scope.").[9] (The substantive flaws in the minimization procedures applied under the FAA are set forth in more detail in part II.B, below.)

The government's implementation of Section 702 allows for "substantial quantities" of Americans' international communications to be swept up, searched, and retained. *See* [Redacted], Docket [Redacted], at *27 n.25

---

[9] Whereas a traditional search warrant named a particular place to be searched and the specific items to be seized, a wiretap order might at minimum specify a phone line to be bugged. When this Court extended the warrant requirement to phone taps in *Katz v. United States*, 389 U.S. 347 (1967), it had to confront the reality that bugging a line is inherently much more open-ended and intrusive than searching a specific place for evidence related to a crime. Multiple people besides the target of a criminal investigation may use a line, the target may speak about private things unrelated to the crime under investigation, and in fact may even speak about privileged matters—conversations with his attorney being a prime example. A tap is typically in place around the clock, and usually results in recording.

In *Berger*, decided just a few months before *Katz*, this Court noted most of these problems and suggested that any warrant for wiretapping would need to meet higher standards, to be a super-warrant of sorts. *Berger* suggested that wiretaps, being inherently intrusive, might only be justifiable at all in investigations of serious crimes. And they would require a variety of safeguards to ensure they were as narrow in concept as the physical search warrants the Founders envisioned: they would need to include time limits, the application should establish why no other method of evidence gathering would work, and the application would need to provide for "minimization"—meaning, there would need to be procedures proposed for implementing the warrant that would minimize the interception and recording of irrelevant (or legally-privileged) conversations outside the scope of the warrant.

The government has conceded before the Foreign Intelligence Surveillance Court of Review that courts have constitutionalized the minimization requirement. See Supplemental Brief of the United States, Appendix A: Comparison of FISA and Title III, *In re Sealed Case, No. 02-001* (FISA Ct. Rev. filed Sep. 25, 2002) at n.1.

(FISC Nov. 6, 2015) [hereinafter "Hogan Opinion"], http://bit.ly/1SNQRUe. Despite repeated requests from Congress, the NSA has declined to release official estimates on how many Americans' communications are collected. *See* Letter from Sen. Ron Wyden to Dan Coats, Dir. of Nat'l Intelligence (Mar. 8, 2017), http://bit.ly/2u6sMCa. However, targeting statistics released by the agency show that, in 2016 alone, there were an estimated 106,469 targets of Section 702 surveillance, and 5,288 queries of data acquired pursuant to Section 702 with "search terms concerning a known U.S. person." *See* Statistical Transparency Report Regarding the Use of National Security Authorities at 7-8 (Apr. 2017), http://bit.ly/2uJRYQR. The Ninth Circuit noted "the most troubling aspect of this 'incidental' collection is … its volume, which is vast...." *Mohamud*, 843 F.3d at 440.

There are two types of collection under Section 702. Through PRISM surveillance the government collects all communications to or from particular user accounts directly from U.S service providers.[10] *See* Privacy and Civil Liberties Oversight Board, *Report on the Surveillance Program Operated Pursuant to Section 702 of FISA* at 7 (2014) [hereinafter "PCLOB Report"]. "Upstream surveillance" entails the bulk interception of *all* of Americans' international communications passing through a particular network gateway. *Id.* Data collected through these programs is retained in intelligence databases that the government can query for information relating to specific Americans. *See* Transcript, In re: [Redacted], at

---

[10] The 2016 NSA targeting and minimization procedures no longer allow for "about" collection, the acquisition of Americans' international communications that only mention names of foreign targets being surveilled. *See* Charlie Savage, *N.S.A. Halts Collection of Americans' Emails About Foreign Targets*, N.Y. Times, Apr. 28, 2017, http://nyti.ms/2qzz63I.

34 (D.D.C. Oct. 20, 2015) (Department of Justice attorney: "these systems ... queried on such a routine basis ... are [the] FBI's Google"), *available at* http://bit.ly/2ump2S0. This backdoor search loophole allows the government to search through Americans' communications in bulk without a warrant. Indeed, the loophole was *designed* to swallow the rule; as advocates for the FAA made clear before Congress, the fact that one end of a call or email was in the U.S. made these communications the most important intended targets of the statute.[11]

II. The Targeting and Minimization Procedures Fail to Protect Sensitive Communications of American Journalists, Attorneys, and Members of the Legislative and Judicial Branches

Surveillance conducted pursuant to Section 702 particularly impacts amicus CCR's staff, who represent clients outside the U.S. and who frequently travel internationally and communicate with individuals abroad. The statutory language allows for virtually any foreigner to

---

[11] *See, e.g.*, FISA for the 21st Century: Hearing Before the S. Comm. on the Judiciary, 109th Cong. at 9 (2006), http://1.usa.gov/1kbgHm3 (statement of NSA Director Michael Hayden) (stating that communications originating or terminating in the United States were those of most importance to the government); *see also* Privacy & Civil Liberties Oversight Board, *Workshop Regarding Surveillance Programs Operated Pursuant to Section 215 of the USA PATRIOT Act and Section 702 of the Foreign Intelligence Surveillance Act* at 109:9–17 (July 9, 2013) (statement of Steven G. Bradbury, Former Principal Deputy Ass't Att'y Gen., DOJ Office of Legal Counsel) (stating that the FAA is "particularly focused on communications in and out of the United States because ... those are the most important communications"); *see also* PCLOB Report at 82, 114 ("such collection is not accidental or inadvertent, but rather is an anticipated collateral result of monitoring an overseas target.").

be targeted, and the post-seizure restrictions designed to address the broad and imprecise nature of Section 702 surveillance provide insufficient protection against the collection, search, and use of Americans' information. Privileged attorney-client communications are protected only in the narrowest of circumstances. There appears to be nothing preventing the international communications of judges and members of Congress from being subject to acquisition and search, raising separation of powers issues. Lawmakers have also raised concerns that wholly domestic communications are being swept up.

A. Targeting Criteria

Section 702 targeting criteria are construed broadly and likely result in the collection of communications between amicus' staff and the foreign parties they interact with in the course of their work. Targeting is not based on individualized cause to suspect that the target is an agent of a foreign power, but merely on whether the information sought meets the statutory definition of "foreign intelligence information." Surveillance can occur for any foreign intelligence purpose that "relates" to "the conduct of the foreign affairs of the United States" or its "national defense" or unspecified other "security" interests (including, presumably, economic ones).[12] 50 U.S.C. § 1801(e)(2)(B), (A).

This definition of "foreign intelligence information" is so broad that it can easily encompass nearly all communications between Americans and their friends, relatives, associates, clients, or business partners abroad. When a Guantánamo detainee communicates with his attorney, CEOs of Fortune 100 corporations negotiate a merger

---

[12] *Cf. supra* note 6.

that could impact global markets, or a human rights organization communicates with activists abroad protesting their government's policies, such interactions arguably "relate" to U.S. foreign affairs and could be collected. The targeting procedures list factors the NSA may consider when determining whether a target is likely to have foreign intelligence information. These factors, such as whether there is "reason to believe" the target has communicated with an individual "associated with" a foreign power, are themselves susceptible to broad interpretation and provide little, if any, added limitation. *See, e.g.*, 2009 NSA Targeting Procedures at 4-5.[13] (Note that the precise procedures that were applied to the surveillance in Mohamud's case have never been specified.)

Even a certification with an expressly national-security related targeting criterion—seeking, say, "all communications by individuals associated with Al Qaeda"—in practice could reach every conversation of a Guantánamo detainee with their lawyer in meeting rooms at the prison, since the government asserts (typically without plausible evidence) that nearly everyone at Guantánamo is a member of al Qaeda, and that the base itself is not within the United States. As described in the next section, the minimization procedures applied to Section 702 surveillance by the government would not protect the contents of these privileged conversations from retention, search, and dissemination.

The breadth of section 702 also implicates freedom of the press. Journalists covering international affairs, for instance, maintain contact with sources throughout the world, some of whom may be outspoken critics of the

---

[13] The 2016 NSA Targeting Procedures are heavily redacted, so it is unclear whether, if at all, the criteria have changed. *See* 2016 NSA Targeting Procedures at 4-6, *available at* http://bit.ly/2vi8wkR.

U.S. government and its allies and engage in social protest to effect change. The ability to gather information from these sources depends on the ability of the journalists to ensure that the contents of the communications (and often, the identities of the sources) will be kept confidential. Such communications can be intercepted under Section 702, deterring sources from speaking to journalists for fear of retaliation by the repressive regimes they live under that might be supported economically and militarily by the U.S. The plaintiffs in *Clapper* included journalists with concerns that past sources—indigenous groups opposed to local terrorist groups as well as the policies of both the U.S. and their home governments—would cease communicating with them due to fears that FAA surveillance would result in lost confidentiality and retaliation.[14] Human rights reporting organizations such as Amnesty International and Human Rights Watch noted similar concerns.[15] Six years later, an extensive study by Human Rights Watch reported that journalists had "adopt[ed] elaborate steps to protect sources and information, and eliminate any digital trail of their investigations—from using high-end encryption, to resorting to burner phones, to abandoning all online communication and trying exclusively to meet sources in person," and yet still found sources drying up and reporting on governmental activities becoming more difficult in the wake of the FAA.[16]

---

[14] *See, e.g.*, Decl. of Naomi Klein, *Amnesty Int'l USA v. McConnell*, No. 08 Civ. 6259 (S.D.N.Y. Sep. 11, 2008) at ¶¶ 6-9.

[15] *See* Complaint, *Amnesty Int'l USA v. McConnell*, No. 08 Civ. 6259 (S.D.N.Y. Jul. 10, 2008), at ¶¶ 52-56, 68-73.

[16] *See* Human Rights Watch, *With Liberty to Monitor All* 22-48 (Jul. 2014); *see also* Pew Research Center, *Investigative Journalists and Digital Security: Perceptions of Vulnerability and Changes in Behavior* 8-11, 13-15 (Feb. 5, 2015).

B. Minimization Procedures

Once information is amassed under Section 702's sweeping targeting authority, the minimization procedures provide insufficient protection against retention and search of communications of Americans who could not otherwise be targeted directly under the statute. Information collected may be stored indefinitely and the government can comb through it for U.S. person identifiers, such as telephone numbers or email accounts. *See* 2016 NSA Minimization Procedures § 3(b). Even though *collecting* this information *for the purpose of* searching it for U.S. person identifiers would be prohibited by the statute's "reverse targeting" provision, 50 U.S.C. 1881a(b)(2),[17] doing such searches on information *already collected* is not prohibited under the minimization protocols.

Furthermore, the FBI, CIA, and possibly other law enforcement agencies have access to unminimized Section 702-acquired information. Each agency is governed by its own set of minimization protocols for handling this raw information. The FBI queries incidentally-collected records for U.S. person identifiers and uses the data to initiate investigations for domestic crimes. *See* Hogan Opinion at 29-30, n. 27. *See also Foreign Intelligence Surveillance Act: Hearing Before the S. Comm. on the Judiciary, 114th Cong.* (2016) (testimony of David Medine, former Chairman of the PCLOB) (the FBI "routinely looks into 702 databases, and not just in investigations, but even in assessments where the FBI has absolutely

---

[17] This provision states that the government "may not intentionally target a person reasonably believed to be located outside the United States if the purpose of such acquisition is to target a particular, known person reasonably believed to be in the United States."

no suspicion of wrongdoing … they're just sort of entitled to poke around and see if something is going on"). Access to the huge volume of Section 702-derived data gives FBI agents the ability to learn about "sensitive" political, religious, and other First Amendment-protected activities of Americans. If this sensitive information appears to contain "foreign intelligence information," it can be retained, searched, and disseminated just as any non-sensitive information might be. *See, e.g.*, 2014 FBI Minimization Procedures at 10, *available at* http://bit.ly/2ftqRpu.

The inadequacy of the targeting and minimization procedures is compounded by the lack of judicial oversight of the underlying surveillance. The Attorney General and the Director of National Intelligence, and not a "neutral, disinterested" judge, *Dalia v. United States*, 441 U.S. 238, 255 (1979), have complete discretion over whose communications to target. They are not required to describe targets with particularity to a judge or show probable cause that a target is a foreign agent or involved in any wrongdoing. *Compare* 50 U.S.C. § 1881a(a)-(b) (authorizing generalized targeting of non-U.S. persons "to acquire foreign intelligence information") *with* 18 U.S.C. § 2518(3)(a) (requiring a judicial probable cause finding for a Title III wiretap order) *and* 50 U.S.C. § 1805(a)(2) (requiring a judicial probable cause finding for a traditional FISA surveillance order). The FAA does not limit surveillance to specific targets but allows bulk collection so long as it falls within the broad parameters of the targeting and minimization procedures. This makes it an outlier among surveillance statutes such as FISA and Title III, which mandate particularity, requiring the government to submit an individualized application identifying the particular target and cause to surveil them, the facility to which surveil-

lance would be directed, the type of information sought, and the procedures to be used.

The lack of judicial supervision of minimization is of special concern for attorneys. Previously, under any regime of statutorily-authorized surveillance, attorneys could rest assured that a judge had ensured that procedures designed to minimize the interception and retention of privileged conversations had been implemented with the initial surveillance order, and that the implementation of these minimization procedures would be supervised on a continuing basis by judges. Surveillance under Section 702 lacks these safeguards. Once they are incidentally collected, attorney-client communications containing "foreign intelligence information" can be used and disseminated by the NSA so long as the client is not "known to be under criminal indictment in the United States." *See* 2011 NSA Minimization Procedures § 4, *available at* http://bit.ly/2uo2cFy; *cf.* 2016 NSA Minimization Procedures § 4(b-c) (more heavily redacted, but appearing similar); *see also* PCLOB Report at 132 n.543 (noting similar provisions in CIA, FBI minimization procedures).

As a result, an American attorney talking to client family members or fact or expert witnesses or co-counsel in a Guantanamo detainee case, or giving pre-indictment counseling to someone located abroad would not have her communications protected by minimization, despite the fact that they clearly fall within the work-product or attorney-client privileges. Indeed, there seems to be no reason this cramped view of minimization would prevent interception of an attorney's conversations with foreign-national clients detained at Guantánamo (which is, in the government's view, outside the United States), whether in meeting rooms at the base or phone calls from the Se-

cure Facility in the mainland.[18] Even those few Guantánamo detainees who are currently charged before military commissions are not (in the government's view) "under criminal indictment *in the United States*"; presumably the government views their communications with their attorneys as fair game under Section 702. The ramifications of this are staggering, given that the most important criminal proceeding of the century—the trial of the alleged 9/11 conspirators—is currently before the commissions (and may well one day end up transferred to the Article III courts).

The scope of use and dissemination of attorney-client communications, including sharing with foreign governments, is unclear. This raises concerns amongst attorneys who work with particularly vulnerable foreign clients. For instance, CCR represents foreign LGBTI rights activists challenging repression by their home country's government. Absent aggressive counter-surveillance measures, it is conceivable that CCR attorneys' communications with their clients and other litigation participants abroad could be swept up and shared with that government, placing clients in grave danger. CCR attorneys who are assisting in litigation pending before European courts are routinely in contact with colleagues in several other countries in Europe, Asia and Africa, as well as witnesses, experts, and cooperating counsel abroad, all of whom are susceptible to surveillance. The surveillance impacts attorneys working domestically as well, as FBI teams charged with prosecuting a criminal matter are permitted to handle related attorney-client material obtained through Section 702

---

[18] Regarding whether this would fit the targeting limitations, *see supra* page 13 (hypothesizing a certification proposing to target "all communications by individuals associated with Al Qaeda").

programs. *See* [Redacted], Docket [Redacted], at *89-93 (FISC Apr. 26, 2017) (finding that such practice violates the FBI's own minimization procedures), http://bit.ly/2w7S1VU.

The broad scope of surveillance under section 702 raises further separation of powers concerns because it implicates the confidential communications of judges, members of Congress, and administration officials. Members of Congress and administration officials, all of whom routinely communicate directly with agents of foreign governments, can have their communications intercepted. It is unclear whether separate, more rigorous minimization protocols shield these communications; though several sets of minimization protocols have been officially released since Edward Snowden's disclosures, no protocols touching on this subject have been. Several Senators have expressed concerns—unaddressed by the NSA—that their conversations are being incidentally acquired and searched and may be used by executive branch officials for political purposes. *See* Charlie Savage, *NSA Warrantless Surveillance Aided Turks After Attack, Officials Say*, N.Y. Times (Jun. 27, 2017), *available at* http://nyti.ms/2vfOY1O. The fact that the judiciary is not involved in the targeting decisions either at the time of collection or subsequently simply exacerbates these concerns. *See also* Walter F. Mondale, Robert A. Stein & Caitlinrose Fisher, *No Longer a Neutral Magistrate: The Foreign Intelligence Surveillance Court in the Wake of the War on Terror*, 100 Minn. L. Rev. 2251, 2278 (2016) ("very questionable" whether Section 702 comports with Article III because "bulk adjudication" of search techniques does not entail adjudication of an individual case or controversy).

The NSA may also have assumed the power in practice to collect and query wholly domestic communications pursuant to Section 702. While the language of the stat-

ute expressly prohibits such acquisitions, lawmakers have raised concerns that the agency might be exploiting a loophole that allows domestic communications to be retrieved from a server once the sender or recipient has left the United States. *See* Letter from Sen. Ron Wyden to Dan Coats, Dir. of Nat'l Intelligence (Jun. 15, 2017), http://bit.ly/2vg3qa2 (seeking clarification as to whether communications the government knows to be purely domestic can be collected under Section 702); *see also* Letter from Sen. Ron Wyden to Dan Coats, Dir. Of Nat'l Intelligence (Jul. 31, 2017), http://bit.ly/2wvoO8w (following up on previous inquiry).

CONCLUSION

The FAA's broad targeting criteria allow the FISC to rubberstamp open-ended programs of surveillance under which the executive chooses the targets without individualized judicial oversight. The minimization guidelines that are applied to this surveillance are so narrow as to allow inclusion of many communications subject to attorney-client privilege. As implemented, backdoor search practices allow the government to "Google" at will a database of communications of Americans "incidentally" swept into this vast pool. This scheme has been in place for nearly a decade, operating under its own momentum to gather up a previously unimaginable sampling of our digital lives. It has evaded review for years, despite the best efforts of plaintiffs who did not belong to the tiny group of criminal defendants with clear-cut standing of which petitioner Mohamud is a rare representative. This Court should grant *certiorari* to decide, at long last, whether this scheme, which is entirely at odds with the very concept of particularized surveillance, is consistent with the Fourth Amendment and the separation of powers.

Respectfully submitted,

Shayana Kadidal
Counsel of Record
J. Wells Dixon
Baher Azmy
CENTER FOR CONSTITUTIONAL RIGHTS
666 Broadway, 7th Floor
New York, NY 10012
(212) 614-6438
kadidal@ccrjustice.org

Counsel for Amicus Curiae

August 10, 2017