No. 14-35555

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

ANNA J. SMITH,

Plaintiff–Appellant,

v.

BARACK OBAMA, *et al*.,

Defendant–Appellees.

On Appeal from the United States District Court
for the District of Idaho, Boise; Case No. 2:13-cv-00257-BLW
The Honorable B. Lynn Winmill, Chief District Judge

APPELLANT'S REPLY BRIEF

Peter J. Smith IV
LUKINS & ANNIS, P.S.
601 E. Front Avenue,
Suite 502
Coeur d'Alene, ID 83814
Phone: 208-667-0517
Fax: 208-664-4125
Email: psmith@lukins.com

Lucas T. Malek
LUKE MALEK, ATTORNEY
AT LAW, PLLC
721 N 8th Street
Coeur d'Alene, ID 83814
Phone: 208-661-3881
Email:
Luke_Malek@hotmail.com

Cindy Cohn
David Greene
Hanni Fakhoury
Andrew Crocker
ELECTRONIC FRONTIER
FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
Facsimile: (415) 436-9993
Email: cindy@eff.org

Jameel Jaffer
Alex Abdo
Patrick Toomey
AMERICAN CIVIL
LIBERTIES UNION
FOUNDATION
125 Broad St., 18th Floor
New York, NY 10004
Telephone: (212) 549 2500
Facsimile: (212) 549-2654
Email: jjaffer@aclu.org

Richard Alan Eppink
AMERICAN CIVIL
LIBERTIES UNION OF
IDAHO FOUNDATION
P.O. Box 1897
Boise, ID 83701
Telephone: (208) 344-9750
Facsimile: (208) 344-7201
Email: reppink@acluidaho.org

Counsel for Plaintiff-Appellant Anna J. Smith

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Federal Cases

Federal Statutes

Federal Rules

Constitutional Provisions

Other Authorities

INTRODUCTION

The government's ongoing collection of Anna Smith's call records violates the Fourth Amendment. The government contends that *Smith v. Maryland*, 442 U.S. 735 (1979), controls this case, but that case involved the collection of a single criminal suspect's call records over a period of several days; it did not involve dragnet surveillance, which—as the Supreme Court has recognized—raises constitutional questions of an entirely different order. To accept the government's view that the Constitution is indifferent to that distinction is to accept that the government may collect in bulk not just call records, but many other records as well. It is to accept that the government may also create a permanent record of every person Americans contact by email; every website they visit; every doctor or lawyer they consult; and every financial transaction they conduct. The Constitution does not condone that result.

Mrs. Smith is entitled to preliminary relief because she is likely to succeed on the merits, but other factors also weigh in favor of preliminary relief. The call-records program is causing irreparable injury to her privacy on an ongoing, daily basis. Further, both the balance of equities and the public interest weigh in favor of injunctive relief. Since Mrs. Smith commenced this action, the Privacy and Civil Liberties Oversight Board ("PCLOB"), the President's Review Group on Intelligence and Communications Technologies ("PRG"), and even the President

himself have concluded that the government can track the associations of suspected terrorists without collecting Americans' phone records in bulk. Granting preliminary relief would mitigate Mrs. Smith's injuries without compromising any legitimate governmental interest.

ARGUMENT

I. THE LONG-TERM COLLECTION AND AGGREGATION OF MRS. SMITH'S CALL RECORDS VIOLATES THE FOURTH AMENDMENT

A. The Long-Term Collection and Aggregation of Mrs. Smith's Call Records Is a Search.

The long-term collection and aggregation of Mrs. Smith's call records is a search within the meaning of the Fourth Amendment. *See* Pl. Br. 21–26. When collected in bulk, call records reveal religious, familial, political, and intimate relationships; sleeping and work habits; health problems; and business plans. *Id.* at 22–24. When the records of one individual are aggregated with the records of many others, the records become even more revealing. *See*, *e.g.*, Felten Decl. ¶ 64 (ERII 101); Jonathan Mayer & Patrick Mutchler, *MetaPhone: The Sensitivity of Telephone Metadata* (Mar. 12, 2014), http://bit.ly/1CqOaPK (study demonstrating use of telephony metadata to reveal who obtained an abortion, who sought medical treatment, or who owns particular kinds of firearms).

The government contends that this case is controlled by *Smith v. Maryland*, but while that case involved the collection of call records, it did not involve the

collection of call records over an extended period of time or in bulk. It held only that the Fourth Amendment is not implicated by the government's collection of a single criminal suspect's call records over a period of a few days.

The Fourth Amendment analysis is not indifferent to the scale and intrusiveness of the government's surveillance. Just four years after it decided *Smith*, the Supreme Court explicitly recognized that the distinction between narrow surveillance and dragnet surveillance is a constitutionally significant one. *See* Pl. Br. 18 (discussing *United States v. Knotts*, 460 U.S. 276 (1983)). More recently, in *United States v. Jones*, 132 S. Ct. 945 (2012), five Justices concluded that the long-term tracking of an individual in public amounted to a search under the Fourth Amendment. *See* Pl. Br. 18–23; *see also United States v. Maynard*, 615 F.3d 544, 557 (D.C. Cir. 2010), *aff'd sub nom. Jones*, 132 S. Ct. 945. They reached this conclusion even though the Supreme Court had previously concluded that shorter-term tracking did not amount to a search. *See Knotts*, 460 U.S. at 281–82.

Thus, *Smith* no more controls in this case than *Knotts* controlled the outcome in *Maynard* or the reasoning of the concurrences in *Jones*. And it no more controls in this case than the Supreme Court's prior search-incident-to-arrest cases, like *Chimel v. California*, 395 U.S. 752 (1969), controlled in *Riley v. California*, 134 S. Ct. 2473 (2014). As the Supreme Court recognized in *Riley*, any extension of past

doctrine to surveillance that is substantially more intrusive "has to rest on its own bottom." *Id.* at 2489.

The government characterizes the obvious and glaring distinctions between this case and *Smith* as "immaterial." Gov't Br. 44, 47. But this characterization disregards the express acknowledgment in *Knotts* and the later holding of this Court in *United States v. Nerber* that the duration of surveillance *does* matter. *Knotts*, 460 U.S. at 283–84 (stating that "different constitutional principles may be applicable" to "twenty-four hour surveillance"); *United States v. Nerber*, 222 F.3d 597, 600 (9th Cir. 2000). As this Court stated, "We reject the government's broad argument that a court may never consider the severity of the governmental intrusion in determining whether a citizen has a legitimate expectation of privacy." *Nerber*, 222 F.3d at 600. The government's argument also fails to grapple with the reasoning of the D.C. Circuit's decision in *Maynard*, which refused to extend *Knotts* to long-term location tracking, explaining that *Knotts* did not determine whether "prolonged surveillance" requires a warrant. *Maynard*, 615 F.3d at 558. This Court recently echoed that reasoning: "We, like the Seventh Circuit, believe that '[s]hould [the] government someday decide to institute programs of mass surveillance of vehicular movements, it will be time enough to decide whether the Fourth Amendment should be interpreted to treat such surveillance as a search.'" *United States v. Pineda-Moreno*, 591 F.3d 1212, 1217 (9th Cir. 2010) (alterations

in original) (quoting *United States v. Garcia*, 474 F.3d 994, 998 (7th Cir. 2007)), *vacated on other grounds*, 132 S. Ct. 1533 (2012).

Finally, the government's argument ignores the teaching of *Riley*: that quantitative changes can make a qualitative difference. In *Riley*, the government argued that "a search of all data stored on a cell phone is 'materially indistinguishable' from searches of [analogous] physical items." *Riley*, 134 S. Ct. at 2488. The Supreme Court dismissed that argument:

> That is like saying a ride on horseback is materially indistinguishable from a flight to the moon. Both are ways of getting from point A to point B, but little else justifies lumping them together.

Id. at 2488–89; *see also United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) ("Technology has the dual and conflicting capability to decrease privacy and augment the expectation of privacy.").

The upshot is this: legal principles developed in the context of the targeted and short-term collection of call records cannot be extended blindly to contexts involving the collection of call records over long periods of time and *en masse*. Rather, to decide the Fourth Amendment issue here, the Court must answer a question that the Supreme Court has never confronted—whether the government's long-term collection and aggregation of call records invades a reasonable expectation of privacy. *See Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). For reasons already explained, it does. *See* Pl. Br. 21–26;

see also Felten Decl. ¶¶ 38–64 (ERII 92–101); PCLOB, *Report on the Telephone Records Program Conducted under Section 215 of the USA PATRIOT Act and on the Operations of the Foreign Intelligence Surveillance Court* 156–58 (Jan. 23, 2014), http://bit.ly/1d01flI ("PCLOB Report"); PRG, *Liberty and Security in a Changing World* 110–17 (Dec. 12, 2013), http://1.usa.gov/1cBct0k ("PRG Report").[1]

The government contends that its collection of call records does not implicate the Fourth Amendment because call records consist of information entrusted by Americans to third-parties. *See* Gov't Br. 39–40, 57–58. As Plaintiff has explained, however, Pl. Br. 24–26, the third-party doctrine has never operated with this kind of rigidity. If the transfer of information to a third party were enough to extinguish an expectation of privacy, the Fourth Amendment would not protect even the content of phone calls and emails—but even the government concedes that this kind of content is protected. A third party's possession of information is surely relevant to the *Katz* analysis in some contexts, but it is not determinative. If

[1] There are other important differences between the surveillance at issue here and the surveillance the Supreme Court considered in *Smith*. The call records collected by the NSA today include call duration, information about location (the "trunk identifier" provides a rough approximation of location), and identification information for the specific device used to make or receive the call. *See* Verizon Secondary Order (ERII 117). The government did not collect any of this information in *Smith*. Indeed, the pen register considered in *Smith* could not even indicate whether any particular call had been completed. 442 U.S. at 741.

it were, many previous cases would have come out the other way. *See* Pl. Br. 24–25 (citing cases).

The government's contention that call records are unprotected because they are "business records," *see* Gov't Br. 40–43, is equally misguided. As an initial matter, it is not clear why Plaintiff's call records should be characterized as business records—the government has not pointed to any evidence that Verizon Wireless uses the records to make business decisions. Moreover, the government has said previously that the call-records program is necessary because many telecommunications providers do not keep their subscribers' call records for long periods. In other words, the program is predicated on the reality that some phone carriers do not maintain the call records as business records.

In any event, the question of Mrs. Smith's expectation of privacy in her call records cannot be answered by a mechanical appeal to formalism. It must be answered, instead, by considering the expectations that society is prepared to accept as reasonable. *See Rakas v. Illinois*, 439 U.S. 128, 143 n.12 (1978) ("Legitimation of expectations of privacy by law must have a source outside of the Fourth Amendment, either by reference to concepts of real or personal property law or to understandings that are recognized and permitted by society.").

The government argues that it would be more convenient for law enforcement if the courts established a bright-line rule that extinguished all privacy

in information shared with others. *See* Gov't Br. 40. The government is surely right about this. The Bill of Rights exists, however, not to serve governmental efficiency but to safeguard individual liberty. *Cf. Bailey v. United States*, 133 S. Ct. 1031, 1041 (2013) ("'[T]he mere fact that law enforcement may be made more efficient can never by itself justify disregard of the Fourth Amendment.'" (quoting *Mincey v. Arizona*, 437 U.S. 385, 393 (1978))); *Riley*, 134 S. Ct. at 2493 ("Our cases have historically recognized that the warrant requirement is 'an important working part of our machinery of government,' not merely 'an inconvenience to be somehow "weighed" against the claims of police efficiency.'" (quoting *Coolidge v. New Hampshire*, 403 U.S. 443, 481 (1971))). Notably, the government made the same appeal for a bright-line rule in *Jones* and *Maynard*, *see, e.g.*, Brief for the United States at 13, *Jones*, 132 S. Ct. 945, but the Supreme Court and D.C. Circuit rejected it.

The government misses the point in arguing that Plaintiff's attempt to distinguish *Smith* ignores the similarities between call records today and call records in 1979. Gov't Br. 50. As in *Riley* and *Maynard*, what is novel here is not primarily the nature of the data collected, but the scale of the collection. *See Riley*, 134 S. Ct. at 2489 ("One of the most notable distinguishing features of modern cell phones is their immense storage capacity."). In 1979, the government simply could not collect or analyze the "vast quantities of personal information" that the digital

era allows it to. *Id.* at 2485. Indeed, new technology "allows even just *one type* of information to convey far more than previously possible." *Id.* at 2489 (emphasis added).

In other words, technological advances have vastly augmented the government's surveillance power and exposed much more personal information to government inspection and intrusive analysis. If courts ignored this reality, the essential privacy long preserved by the Fourth Amendment would be eliminated. *See, e.g.*, *Kyllo v. United States*, 533 U.S. 27, 34 (2001) ("The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy."). As Professor Peter Swire, a member of the President's Review Group, observed:

> Today should be understood as a "golden age for surveillance," in which surveillance activities are in fact greatly enhanced compared to previous periods. Surprising as it may sound to some, law enforcement and intelligence agencies' surveillance capabilities are actually greatly enhanced by the current mix of new technologies.[2]

Ultimately even the government seems uncomfortable with the implications of its theory, and accordingly it places heavy emphasis on the back-end restrictions that limit the circumstances in which the government can access and disseminate the call records it has collected. *See generally* Gov't Br. 37–60. The Supreme Court has already rejected the argument that "government agency protocols" are a

[2] Peter Swire & Kenesa Ahmad, *Encryption and Globalization*, 13 Colum. Sci. & Tech. L. Rev. 416, 464 (Nov. 16, 2011), http://ssrn.com/abstract=1960602.

substitute for a warrant. *Riley*, 134 S. Ct. at 2491. But more importantly, the government's argument is a bait and switch. If the government is right about *Smith*, nothing would preclude it from eliminating virtually all of the restrictions it highlights. It could collect subscribers' names. It could review all of the call records it collects and for any reason at all. It could do so without court involvement. It could keep the records indefinitely. And it could disseminate them without restriction. Moreover, it could do all of this for every category of information arguably analogous to the phone numbers dialed in *Smith*, such as email metadata, text-message metadata, and internet-usage records. This is the true reach of the government's argument. If the government is right that *Smith* controls this case, then all of the restrictions it emphasizes are constitutionally superfluous—they are simply a matter of executive or legislative grace.[3]

[3] The government relies heavily on the fact that the call-records program was authorized by the FISC, *see generally* Gov't Br. 37–60, but this Court owes the FISC no deference. Proceedings before the FISC are not adversarial, and many of the arguments presented by Plaintiff here have never been presented to the FISC, much less by any party with an interest in presenting them persuasively.

The government's argument that Congress ratified the FISC's interpretation of Section 215 when it reauthorized that provision in 2009 and 2011, *see* Gov't Br. 59, is also misguided. Even if Congress had ratified the program, Congress's ratification would not be an answer to Plaintiff's claim here, because Plaintiff's claim is a *constitutional* one. But there was no ratification. The FISC did not issue any opinion explaining its basis for authorizing the program until 2013; the government never shared its legal analysis of the program with Congress prior to that time; many members of Congress did not know about the program at all; and even those members of Congress who knew about the program were foreclosed

B. The Call-Records Program Is Unconstitutional Because It Is Unreasonable.

The phone-records program violates the Fourth Amendment's warrant clause. Even if an exception to that clause applied, the program would be unconstitutional because it is unreasonable. *See* Pl. Br. 29–36.

1. The Call-Records Program Is Unconstitutional Because It Is Warrantless and No Exception to the Warrant Requirement Applies.

The bulk collection of call records is per se unreasonable because it is warrantless and no exception to the Fourth Amendment's warrant requirement applies. The government invokes the special-needs doctrine, Gov't Br. 60, but the special-needs doctrine applies only where compliance with the probable-cause and warrant requirements would be impracticable. *See* Pl. Br. 29–30. Thus, in *Al-Haramain Islamic Foundation v. Department of Treasury*, 686 F.3d 965, 992–93 (9th Cir. 2011), the Court rejected a warrantless seizure based on a foreign-intelligence need after concluding that the government could accomplish its purpose by obtaining a warrant.[4]

---

from conferring with staff, exchanging views with each other, or disclosing even the existence of the program to their constituents. *See* PCLOB Report 95–102.

[4] The Supreme Court has never endorsed the application of the special-needs exception to foreign-intelligence activities. *See United States v. U.S. Dist. Ct.* (*Keith*), 407 U.S. 297, 321–22 (1972). Lower courts that have recognized a foreign-intelligence exception have done so only where the government's surveillance was narrowly targeted at foreign agents. *See, e.g.*, *United States v. Buck*, 548 F.2d 871, 875 (9th Cir. 1977).

The same logic applies here. It would not be impracticable for the government to acquire phone records—including those within one or two hops of its surveillance targets—on an individualized basis. *See id.* Indeed, the government does not dispute that fact, *see* Gov't Br. 67–68, and it has endorsed legislation that would end bulk collection in favor of targeted requests to phone companies.[5] *See* White House, Office of the Press Secretary, *Fact Sheet: The Administration's Proposal for Ending the Section 215 Bulk Telephony Metadata Program* (Mar. 27, 2014), http://1.usa.gov/1gS2HK0; Letter from Att'y Gen. Eric Holder and Dir. of Nat'l Intel. James Clapper to Sen. Patrick Leahy (Sept. 2, 2014) http://bit.ly/1tum5r1 (supporting the USA FREEDOM Act, S. 2685, as an "approach [that] will accommodate operational needs while providing appropriate privacy protections").

In this litigation, the government claims that there is a marginal advantage to possessing at the outset all of the records it might one day want to review. *See* Gov't Br. 61, 65; Giacalone Decl. ¶ 29 (ERII 76) (stating that the bulk collection of call records "enhances and expedites the ability to identify chains of

[5] The government emphasizes that it queried fewer than 300 phone numbers using the NSA's call-records database in 2012, *see* Gov't Br. 13, but that only underscores its ability to make such requests on a targeted basis. *See Al-Haramain*, 686 F.3d at 993 (finding that special-needs exception did not apply where "the number of designated persons located within the United States appears to be very small").

communications across multiple providers"); *see also Klayman v. Obama*, 957 F. Supp. 2d 1, 39–40 (D.D.C. 2013). But the claim that bulk collection is more *efficient* for the government does not establish that obtaining a warrant would be *impracticable*. If efficiency alone were determinative, the Fourth Amendment's warrant requirement would have no force at all.

In any event, the public record does not support the contention that a more narrowly targeted program would actually be less effective or efficient. *See* PRG Report 118–19 (concluding that "there are alternative ways for the government to achieve its legitimate goals, while significantly limiting the invasion of privacy and the risk of government abuse"); PCLOB Report 146 ("[W]e have seen little indication that the same result could not have been obtained through traditional, targeted collection of telephone records."); *see also* Pl. Br. 34–35 (citing statements of Sen. Ron Wyden and NSA Dir. Keith Alexander).

2. The Call-Records Program Is Unreasonable.

Even if an exception to the warrant requirement applied, the call-records program would be unconstitutional because it is unreasonable. *See* Pl. Br. 30–36. The Supreme Court has never applied that doctrine to searches as intrusive, sweeping, or extended as those at issue here. *See, e.g.*, *Skinner v. Ry. Labor Executives' Ass'n*, 489 U.S. 602, 631 (1989) (testing train operators for drug use); *Mich. Dep't of State Police v. Sitz*, 496 U.S. 444, 455 (1990) (checking automobile

drivers for sobriety); *Camara v. Mun. Court*, 387 U.S. 523 (1967) (conducting sporadic building inspections for health-code purposes).

When the special-needs doctrine has been properly invoked, "a search may be reasonable despite the absence of [individualized] suspicion" only "where the privacy interests implicated by the search are minimal, and where an important governmental interest furthered by the intrusion would be placed in jeopardy by a requirement of individualized suspicion." *Chandler v. Miller*, 520 U.S. 305, 314 (1997) (quoting *Skinner*, 489 U.S. at 624).

The bulk collection of Americans' call records is extraordinarily intrusive, as the record shows, *see* Felten Decl. ¶¶ 38–64 (ERII 92–101), and as the government's own analyses confirm. *See* PCLOB Report 12, 156–58; PRG Report 110–14, 116–17. The cases relied upon by the government, in contrast, involved minimally invasive searches or searches of individuals with diminished expectations of privacy. *See* Gov't Br. 65; *Maryland v. King*, 133 S. Ct. 1958, 1978 (2013) (comparing the "reduced" expectation of privacy of one arrested on probable cause for a dangerous offense with that of "the average citizen"); *Vernonia Sch. Dist. 47J v. Acton*, 515 U.S. 646, 665 (1995) (diminished expectation of privacy of student athletes "[t]he most significant element in this case"); *Bd. of Educ. v. Earls*, 536 U.S. 822, 830–32 (2002) (same); *Sitz*, 496 U.S. at 447 ("drivers briefly examined for signs of intoxication" at sobriety checkpoint).

In *King*, for example, the State of Maryland took DNA samples from certain arrestees for the sole purpose of creating DNA fingerprints that revealed nothing more than the individuals' identities. 133 S. Ct. at 1979 ("[T]he CODIS loci come from noncoding parts of the DNA that do not reveal the genetic traits of the arrestee."). Here, the government collects and stores Americans' call records for the very purpose of later querying them in full.

The government argues that the privacy intrusion here is mitigated by the fact that most of the collected data is never reviewed. *See* Gov't Br. 65. The government's bulk collection of such personally revealing information, however, cannot be made reasonable by back-end protocols. *Cf. Riley*, 134 S. Ct. at 2491. The privacy intrusion occurs at the moment of collection, when the government obtains personal information protected by the Fourth Amendment. *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990) ("[A] violation of the [Fourth] Amendment is 'fully accomplished' at the time of an unreasonable governmental intrusion." (quoting *United States v. Calandra*, 414 U.S. 338, 354 (1974))); *accord Soldal v. Cook Cnty.*, 506 U.S. 56, 67 n.11 (1992); *see also Kyllo*, 533 U.S. at 37 ("[T]here is certainly no exception to the warrant requirement for the officer who barely cracks open the front door and sees nothing but the nonintimate rug on the vestibule floor." (citing *Silverman v. United States*, 365 U.S. 505, 512 (1961))).

Moreover, the zone of privacy is pierced whether the government uses a human agent or simply a computer or device it controls to conduct its searches. *See Cotterman*, 709 F.3d at 958 (treating government's use of "forensic software that often must run for several hours to examine" files stored on hard drives as a Fourth Amendment "search"); *see also United States v. Crist*, 627 F. Supp. 2d 575, 585 (M.D. Pa. 2008) (government's use of "hash" analysis to review all computer files a Fourth Amendment "search" notwithstanding fact that no human agents looked at any files); *United States v. Saboonchi*, 990 F. Supp. 2d 536, 568 (D. Md. 2014) (similar). For instance, the privacy intrusion caused by surreptitious video recording has never turned on whether a government agent was actually reviewing the footage. *See, e.g.*, *United States v. Taketa*, 923 F.2d 665, 676 (9th Cir. 1991) ("The videotaping was a continuous search of anyone who entered the camera's field of vision."). It is obvious why: a contrary rule would permit the government to collect and retain enormous amounts of private information about Americans who have done nothing wrong, just in case it wished to access that information later.[6]

[6] Elsewhere, the government emphasizes that it is collecting phone numbers, not names, as if this mitigates or even eliminates the privacy intrusion. *See* Gov't Br. 14. But phone numbers are every bit as identifying as names. Indeed, they are more so: while many people in the country may share the same name, no two phone subscribers share the same number. Moreover, it is trivial for the government to obtain a subscriber's name once it has that subscriber's phone number, using publicly available resources or the many subpoena authorities at its disposal. *See*

On the other side of the balance—"the promotion of legitimate governmental interests," *King*, 133 S. Ct. at 1970—the government conflates its interest in combating terrorism, which is substantial, with the incremental benefit (if any) offered by the call-records program. Again, however, the PCLOB, the PRG, and the President have come to the conclusion that the government can accomplish its aims using individualized court orders. Moreover, as Judge Leon observed in *Klayman*, "the Government does *not* cite a single instance in which analysis of the NSA's bulk metadata collection actually stopped an imminent attack, or otherwise aided the Government in achieving any objective that was time-sensitive in nature." 957 F. Supp. 2d at 40 (emphasis in original). Instead, the government asks the Court to defer to its own vague, conclusory, and unsupported claims that the program is "valuable," Gov't Br. 67, and to disregard the substantial evidence that the call-records program is not necessary. *See, e.g.*, PRG Report 118–19; PCLOB Report 146; Pl. Br. 34–35. The government emphasizes that the President intends to "maintain[] th[e] capabilit[ies]" of the program, Gov't Br. 62 (quotation marks omitted), but this is beside the point. The critical point is

---

Felten Decl. (ERII 86) ¶ 19 & n.14. For these reasons, the government itself treats phone numbers as identifying information in, for example, the context of Freedom of Information Act requests. *See, e.g.*, *Moore v. Obama*, No. 09-5072, 2009 WL 2762827, at *1 (D.C. Cir. Aug. 24, 2009) (per curiam) (affirming FBI's withholding of employee phone numbers); *Smith v. Dep't of Labor*, 798 F. Supp. 2d 274, 284 (D.D.C. 2011) ("Generally, personal identifying information such as a person's name, address, phone number, date of birth, criminal history, medical history, and social security number may be protected under Exemption 6.").

that the President, like many others, has concluded that the program's capabilities can be maintained without bulk collection.

The government asserts that it need not adopt the narrowest method available to pursue its interests. The problem here, however, is that the government has chosen to employ the *most*-intrusive means possible. Even if the collection of everyone's information were a "reasonably effective means" for the government to obtain information about its targets, Gov't Br. 67, that is not an answer to the Fourth Amendment question. Reasonableness requires the Court to balance "on the one hand, the degree to which [the surveillance] intrudes upon an individual's privacy and, on the other, the degree to which it is needed for the promotion of legitimate governmental interests.'" *Samson v. California*, 547 U.S. 843, 848 (2006) (quoting *United States v. Knights*, 534 U.S. 112, 119 (2001)).

The question, in other words, is whether the government's unprecedented call-records dragnet is reasonable even though the President himself has acknowledged that it is unnecessary. To ask the question is to answer it. On one side of the constitutional balance, the privacy intrusion is substantial—even, in some respects, unprecedented. On the other, the government has conceded that bulk collection is not needed to maintain its capabilities. It has publicly endorsed pending legislation that would end the current bulk collection program in favor of targeted requests served on the phone companies. If reasonableness forbids

anything, it surely forbids indiscriminate searches where the government itself has conceded that "precise and discriminate" demands for private information would suffice. *Berger v. New York*, 388 U.S. 41, 58 (1967).[7]

II. MRS. SMITH HAS STANDING TO CHALLENGE THE CALL-RECORDS PROGRAM

The district court correctly concluded that Mrs. Smith has standing to bring this challenge. Dist. Ct. Op. 3 n.2 (ERI 3). In fact, this Court in *Jewel v. NSA*, 673 F.3d 902, 909 (9th Cir. 2011), already ruled that another set of plaintiffs had standing to raise a Fourth Amendment claim when considering, in part, the very same mass collection of call records.[8] The *Jewel* court reached its conclusion after finding that the plaintiffs had alleged a concrete and particularized injury, noting:

---

[7] The government has suggested that in the absence of legislation it cannot obtain information with the speed it requires, *see* Gov't Br. 18, but that is not supported by the record. The government already has the ability to serve targeted requests for call records on phone companies using a number of authorities, and to demand prompt compliance, including in emergencies. *See, e.g.*, 50 U.S.C. § 1842 (pen registers in foreign-intelligence investigations); 18 U.S.C. § 2709 (national security letters); 18 U.S.C. §§ 3122, 3125 (pen registers in law-enforcement investigations); 18 U.S.C. § 2703(d) (orders for stored telephone records); Fed. R. Crim. P. 17(c) (subpoena duces tecum).

In any event, the fact that Congress has not yet enacted legislative changes cannot supply a valid reason for upholding a program that is unconstitutional. *Cf. Katz*, 389 U.S. 347 (government compelled to seek new legal authority from Congress after wiretapping scheme ruled unconstitutional); 18 U.S.C. §§ 2510–2522 (Title III).

[8] *See Jewel*, 673 F.3d at 910 (plaintiffs alleged that the government "acquire[s] all or most long-distance domestic and international phone calls to or from AT&T long distance customers, including both the content of those calls and dialing, routing, addressing and/or signaling information").

"Significantly, Jewel alleged with particularity that *her* communications were part of the dragnet." *Id.* at 910. The same is true for Mrs. Smith. *See* Am. Compl. ¶¶ 7–8, 15–17, 22 (ERII 123–25) (alleging that the government is collecting Mrs. Smith's telephone metadata).

Even in the absence of *Jewel*, however, Mrs. Smith would have standing to challenge the call-records program. It is virtually certain that her phone-service provider—Verizon Wireless—has received an order from the FISC because Verizon Wireless is the nation's largest wireless carrier. *See* Kent German, *Quick Guide to Cell Phone Carriers*, CNET (May 27, 2014) http://cnet.co/1w3B9L3; *see also* Pl. Br. 36–38 (describing public statements and reports identifying Verizon Wireless as a participant in the NSA bulk-collection program); *ACLU v. Clapper*, 959 F. Supp. 2d 724, 735 (S.D.N.Y. 2013) ("While the Secondary Order does not cover calls placed on Verizon Wireless's network, the Government acknowledged that it has collected metadata for substantially every telephone call in the United States since May 2006.").

Moreover, even if Verizon Wireless has never received such an order, Mrs. Smith routinely places calls to individuals whose provider is Verizon Business Network Services ("Verizon Business"), which the government concedes has received an order compelling it turn over call records in bulk. Gov't Br. 31; *see also* Am. Compl. ¶ 17 (ERII 125). Indeed, Mrs. Smith is represented by, among

others, attorneys from the ACLU, and Verizon Business is the ACLU's telephone provider. *Clapper*, 959 F. Supp. 2d at 735. Finally, even if Mrs. Smith has not yet proven that her communications were collected, that is not a basis for dismissal, as the government alleges; rather, Mrs. Smith has offered specific, credible allegations that her call records were collected, Am. Compl. ¶¶ 1, 7–8, 16–17, 22 (ERII 123–25), and she should be permitted the opportunity to conduct discovery like any other litigant. *See, e.g.*, *OSU Student Alliance v. Ray*, 699 F.3d 1053, 1078 (9th Cir. 2012).

In an effort to shield its surveillance activities from judicial review, the government contends that the call-records program does not entail the collection of every call record. Gov't Br. 32–33. In explaining the program to Congress and the public, however, the government has emphasized not only that the program is comprehensive, but that this comprehensiveness is the key to its utility. Thus, Robert Litt, General Counsel of the Office of the Director of National Intelligence testified before Congress that: "In order to find the needle that matched up against that number, we needed the haystack, right. That's what the premise is in this case."[9] Similarly, NSA Deputy Director John Inglis defended the program by saying: "If you're looking for a needle in the haystack you need the haystack. So

[9] *Strengthening Privacy Rights and National Security: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (July 31, 2013), http://bit.ly/ZFmRov.

you wouldn't want to check a database that only has one third of the data, and say there's a one third chance that I know about a terrorist plot, there's a two thirds chance I missed it because I don't have that data."[10]

The government appears to be asking this Court to believe that the call-records program is comprehensive enough to be very effective but not so comprehensive that Mrs. Smith should be permitted to challenge its constitutionality. This proposition is not just self-serving but implausible. Faced with the same argument from the government, the district court in *Klayman* observed: "[T]he Government asks me to find that plaintiffs lack standing based on the theoretical possibility that the NSA has collected a universe of metadata so incomplete that the program could not possibly serve its putative function. Candor of this type defies common sense and does not exactly inspire confidence." *Klayman*, 957 F. Supp. 2d at 27.

The government's argument that Mrs. Smith lacks standing because she cannot show that the government has reviewed the call records it has collected, Gov't Br. 34, is misguided. Mrs. Smith complained not only about the government's review of her records but about its acquisition of her records in the first instance. *See, e.g.*, Am. Compl. ¶ 1 (ERII 123). Though the government's

[10] Transcript: NSA Deputy Dir. John Inglis, NPR (Jan. 10, 2014, 6:19 AM), http://n.pr/1bZ9Rc3.

subsequent use of Mrs. Smith's records aggravates her injuries, Mrs. Smith need not establish anything about the government's subsequent use of her records in order to challenge the government's initial collection of them. The government's collection of Mrs. Smith's call records inflicts an injury sufficient by itself to support standing.[11]

In fact, the government's argument that there is no case or controversy until an analyst reviews the information the government has collected is not simply wrong but radically so. Consider the implications: If the collection of information could not give rise to a case or controversy, the Constitution would permit the government to copy every email, record every phone call, and make a permanent record of every person's physical movements—all without ever having to justify its actions to any court. The Constitution would be engaged, if at all, only when the government decided to review the data it had collected. The government supplies no authority for the proposition that the Constitution is indifferent to the government's accumulation of vast quantities of sensitive information about

[11] In any event, even if the relevant question were whether the NSA had reviewed Mrs. Smith's records, the government has effectively acknowledged that it has done so. *Klayman*, 957 F. Supp. 2d at 28 & n.38 ("When the NSA runs such a query [on a foreign phone number], its system must necessarily analyze *every* phone number in the database by comparing the foreign target number against *all* of the stored call records to determine which U.S. phones, if any, have interacted with the targeted number.") (emphasis in original).

Americans' lives—let alone for the proposition that such surveillance does not even trigger Article III.

The government's reliance on *Clapper v. Amnesty International USA*, 133 S. Ct. 1138 (2013), and *Laird v. Tatum*, 408 U.S. 1 (1972), is also misplaced. The *Clapper* Court concluded that the plaintiffs lacked standing not because the plaintiffs failed to demonstrate that their communications had been "retrieved" from government databases but because the plaintiffs failed to demonstrate even a "substantial risk" that their communications would be collected in the future. *Amnesty*, 133 S. Ct. at 1150 n.5. Similarly, in *Laird*, the plaintiffs complained not about the collection of their information but about the possibility that the information collected would be misused in the future. *See Laird*, 408 U.S. at 13.

Finally, the government suggests that the NSA's automated searches of phone records are like dog sniffs for contraband and thus do not implicate the privacy of those whose records are not responsive to the queries. Gov't Br. 24–25, 36. That argument reflects a deep misunderstanding of the contraband doctrine. The doctrine does not turn on the fact that a dog is conducting the search—after all, the dog is acting as an instrument of the government. *See United States v. Place*, 462 U.S. 696, 706 (1983). The doctrine turns, instead, on the fact that the search turns up only *contraband*, in which there is no reasonable expectation of privacy. *See, e.g.*, *id.* at 707 ("A 'canine sniff' by a well-trained narcotics detection

dog, however, . . . does not expose noncontraband items that otherwise would remain hidden from public view . . . ."); *Illinois v. Caballes*, 543 U.S. 405, 410 (2005) ("The legitimate expectation that information about perfectly lawful activity will remain private is categorically distinguishable from respondent's hopes or expectations concerning the nondetection of contraband in the trunk of his car."); *see also United States v. Young*, 573 F.3d 711, 720–21 (9th Cir. 2009). Here, however, the government is collecting not contraband but information relating to constitutionally protected associations.

III. THE DISTRICT COURT ERRED IN DENYING MRS. SMITH'S MOTION FOR A PRELIMINARY INJUNCTION

For the reasons above, Mrs. Smith is likely to succeed on the merits of her claim. She will also suffer irreparable harm if a preliminary injunction is not granted: the NSA's daily collection of her phone records infringes her privacy and Fourth Amendment right to be free of unreasonable searches and seizures. Indeed, given that the alleged infringement is a constitutional one, under this Court's case law the Court is entitled to *presume* irreparable harm. *See* Pl. Br. 38–39.

The balance of hardships and the public interest also counsel in favor of granting preliminary relief. Each day brings new incursions into Mrs. Smith's constitutionally protected privacy rights, as the NSA collects a new set of her call records. The preliminary relief she seeks would not prejudice the government because, as discussed above, the government need not collect Mrs. Smith's records

in order to obtain the call records of suspected terrorists and their contacts. *See, e.g.*, PCLOB Report at 146 (stating that there is "little evidence that the unique capabilities provided by the NSA's *bulk* collection of telephone records actually have yielded material counterterrorism results that could not have been achieved without the NSA's Section 215 program") (emphasis in original); PRG Report at 104 ("Our review suggests that the information contributed to terrorist investigations by the use of section 215 telephony meta-data was not essential to preventing attacks and could readily have been obtained in a timely manner using conventional section 215 orders."). Indeed, it is "most unlikely" that such a preliminary injunction would interfere with the government's investigations because, as the government states, "the program is directed at identifying terrorist connections, and there is no allegation or evidence that metadata about [Mrs. Smith's] calls" has ever contributed to such an investigation through a call-records query. *Compare* Gov't Br. 55, *with id.* at 70 (claiming, without evidence, that Mrs. Smith's call records could "reveal connections between individuals associated with terrorist activity").

Finally, the government dramatically overstates the difficulty of implementing the requested injunction. *See* Gov't Br. 69–70. The government appears to have already developed—and used for years—methods that allow it to isolate and exclude particular numbers from queries of the call-records database.

See, e.g., David S. Kris, *On the Bulk Collection of Tangible Things* 13–14, 1 Lawfare Research Paper Series No. 4 (Sept. 29, 2013) ("NSA technicians may access the metadata to make the data more useable—*e.g.*, to create a 'defeat list' to block contact chaining through 'high volume identifiers' presumably associated with telemarketing or similar activity." (quoting orders of the Foreign Intelligence Surveillance Court)); *see also* Memorandum for Staff Dir., H. Permanent Select Comm. on Intel. (June 29, 2009) http://goo.gl/Fl7OXw (describing NSA's use of a master "defeat" list in another bulk metadata program). Against this background, the government's complaint that a preliminary injunction would be "extraordinarily burdensome," Shea Decl. ¶ 68 (SER 27), is not credible. Both the balance of hardships and the public interest weigh in favor of Mrs. Smith.

CONCLUSION

For the reasons stated above, this Court should reverse the judgment below and remand for entry of a preliminary injunction.

DATED: October 16, 2014 Respectfully submitted,

By: */s/ Peter Smith*
Peter J. Smith IV
LUKINS & ANNIS, P.S.
601 E. Front Avenue, Suite 502
Coeur d'Alene, ID 83814

Lucas T. Malek
LUKE MALEK, ATTORNEY AT LAW, PLLC
721 N 8th Street
Coeur d'Alene, ID 83814

Cindy Cohn
David Greene
Hanni Fakhoury
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109

Jameel Jaffer
Alex Abdo
Patrick Toomey
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad St., 18th Floor
New York, NY 10004

Richard Alan Eppink
AMERICAN CIVIL LIBERTIES UNION OF IDAHO FOUNDATION
P.O. Box 1897
Boise, ID 83701

Counsel for Plaintiff-Appellant ANNA J. SMITH

**CERTIFICATE OF COMPLIANCE
WITH TYPE-VOLUME LIMITATION,
TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS
PURSUANT TO FED. R. APP. P. 32(a)(7)(C)**

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. Appellees' Reply Brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 6,697 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

DATED: October 16, 2014

Respectfully submitted,

By: */s/ Peter Smith*
Peter J. Smith IV
LUKINS & ANNIS, P.S.

Counsel for Plaintiff-Appellant ANNA J. SMITH

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on October 16, 2014.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

DATED: October 16, 2014

Respectfully submitted,

By: */s/ Peter Smith*
Peter J. Smith IV
LUKINS & ANNIS, P.S.

Counsel for Plaintiff-Appellant ANNA J. SMITH