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 OPENING 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

Legislative Materials

Other Authorities

INTRODUCTION

Over a decade ago, the government secretly began collecting in bulk the telephone records of millions of innocent Americans. Through this mass surveillance program, which continues today, the government keeps records of who calls whom, when, and for how long. These records, amassed in a government database, supply the government with a rich profile of every citizen as well as a record of citizens' associations with one another. The government knows who is calling which doctor, and when; which family members are in touch with one another, and how often; which pastor or imam or rabbi provides counsel to whom; who is calling the abortion clinic, the alcoholism-support line, the psychiatrist, the ex-girlfriend, the criminal-defense lawyer, the suicide hotline, and the child-services agency. The government knows all of this about millions of Americans—including Anna Smith, a nurse and mother living in Coeur d'Alene, Idaho, who has never been suspected of any involvement whatsoever in criminal activity or terrorism.

The surveillance imposed on Americans by the call-records program is anathema to this country's constitutional tradition, and the privacy intrusions the program works are unprecedented in our history. The government's defense of the program is based almost entirely on a Supreme Court decision from thirty-five years ago—*Smith v. Maryland*, 442 U.S. 735 (1979)—that concerned the

warrantless collection of a suspected criminal's dialing information over a period of three days. But the National Security Agency's call-records program bears no resemblance to the targeted and narrowly circumscribed surveillance that the Supreme Court upheld in *Smith*. Indeed, the idea that *Smith* tacitly authorized the government permanently to impose a system of pervasive and intrusive surveillance on hundreds of millions of innocent Americans is beyond untenable. As the Supreme Court cautioned just months ago, analog-era precedents cannot be extended mechanically to factual contexts far removed from the ones that gave rise to them. *See Riley v. California*, 134 S. Ct. 2473, 2488–89 (2014).

Neither *Smith* nor any other authority grants the government the power to invade without suspicion and without end the privacy rights of Mrs. Smith and millions of other innocent Americans. This Court should reverse the judgment below.

STATEMENT OF JURISDICTION

Plaintiff–Appellant Anna Smith brings a claim under the Fourth Amendment. The district court had subject-matter and personal jurisdiction pursuant to 28 U.S.C. § 1331. On June 3, 2014, the district court granted the government's motion to dismiss and denied Mrs. Smith's motion for a preliminary injunction; the court entered final judgment the same day. *See* Dist. Ct. Op. (ERI

8).[1] On July 1, 2014, Mrs. Smith timely filed her Notice of Appeal (ERII 9–10). This Court has jurisdiction under 28 U.S.C. § 1291.

STATEMENT OF ISSUES

1. Whether the government's bulk collection of phone records violates the Fourth Amendment, such that the district court erred in granting the government's motion to dismiss.

2. Whether the district court erred in denying Mrs. Smith's motion for a preliminary injunction.

STATEMENT OF ADDENDUM

Pursuant to Ninth Circuit Rule 28-2.7, an addendum setting forth "pertinent" constitutional provisions and statutes follows the end of this brief.

STATEMENT OF FACTS

A. Appellant Anna J. Smith.

Anna J. Smith is an ordinary American, living with her family in Kootenai County, Idaho. She is a neonatal intensive care nurse and mother of three children. Like many other Americans, her primary means of communication is her mobile phone. She has been a customer of Verizon Wireless for the past three years and was a customer of AT&T Wireless for four years before that. She uses her phone to communicate with her family, her friends, her employer, her children's teachers,

[1] "ERI" refers to Volume I of the Excerpts of Record filed in connection with this opening brief. "ERII" refers to Volume II of the Excerpts of Record.

her doctors, her legal counsel, and many others. None of her communications relate to international terrorism or clandestine intelligence activities. *See* Amended Compl. ¶¶ 6–8, 18–20 (ERII 123, 125).

B. The NSA's Call-Records Program.

For over a decade, the government has been collecting call records on a daily basis in bulk from major domestic telecommunications companies. The government initiated the call-records program in the weeks after September 11, 2001.[2] For almost five years the government collected Americans' call records on the basis of secret presidential authorizations and without any judicial or congressional authorization.

On May 24, 2006, the government secretly obtained approval from the Foreign Intelligence Surveillance Court ("FISC") to collect call records under 50 U.S.C. § 1861—a provision commonly known as "Section 215 of the Patriot Act."[3]

[2] *See* Public Declaration of James R. Clapper, Director of National Intelligence ("DNI") ¶ 6, *Jewel v. NSA*, No. 08-cv-4373 (N.D. Cal. Dec. 20, 2013) (ECF No. 168); *see also* Office of the Inspector General of the Dep't of Def., *et al*., *Unclassified Report on the President's Surveillance Program* 1, 5–9 (2009), https://www.fas.org/irp/eprint/psp.pdf ("PSP IG Report").

[3] *See* Order, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted]*, No. BR 06-05 (FISC May 24, 2006), http://1.usa.gov/1f28pHg; *see* USA PATRIOT Act of 2001, Pub. L. 107-56.

The program continues under Section 215's authority to this day.[4]

Under the FISC orders that currently authorize the program, the government presents multiple telecommunications carriers with orders requiring them to produce to the National Security Agency ("NSA") "on an ongoing daily basis . . . all call detail records or 'telephony metadata'" relating to every domestic and international call placed on their networks.[5] The orders, which are renewed every ninety days, further specify that the "telephony metadata" sought includes, for each call, the originating and terminating telephone number as well as the call's time and duration. *See* Verizon Secondary Order (ERII 117). Once collected, the bulk telephony metadata is stored in a government database for five years.[6]

---

[4] *See* Primary Order, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from [Redacted]*, No. BR 14-96 (FISC June 19, 2014), http://1.usa.gov/1oLUFtg ("June 19, 2014 Primary Order").

[5] Secondary Order*, In re Application of the FBI for an Order Requiring the Prod. of Tangible Things from Verizon Bus. Network Servs., Inc. on Behalf of MCI Commc'n Servs., Inc. d/b/a Verizon Bus. Servs.*, No. BR 13-80 (FISC Apr. 25, 2013) (ERII 116–19) ("Verizon Secondary Order").

[6] Upon a government application to the FISC demonstrating "reasonable articulable suspicion" that a telephone number is associated with an international terrorist organization, the government may query its database using that number, which is known as the "seed." *See* Order Granting the Government's Motion to Amend the Court's Primary Order Dated January 3, 2014, at 3–4, *In re Application of the FBI for an Order Requiring the Prod. of Tangible Things*, No. BR 14-01 (FISC Feb. 5, 2014), http://1.usa.gov/1l34PSi ("Bulk Call-Records Modification Order"). Each query of the database returns all telephone numbers within two "hops" of the seed—effectively, all telephone numbers "that have been in contact or are connected with the seed," plus all telephone numbers "that have been in contact or are connected with a [telephone number] revealed by the first hop." *Id*. at 3 n.2; *see*

While news reports discussed the existence of the call-records program as early as 2006,[7] the government did not officially acknowledge the program until shortly after June 5, 2013, when *The Guardian* newspaper disclosed a "Secondary Order" that had been issued by the FISC two months earlier to Verizon Business Network Services ("Verizon Business"), a subsidiary of Verizon Communications.[8] After it acknowledged the existence of the program, the government also acknowledged that the Secondary Order was issued as part of a broader effort involving multiple telecommunications providers.[9] The FISC has reauthorized the program many times, most recently on June 19, 2014.[10]

The program is unprecedented in its scale and highly intrusive. As Princeton computer science professor Edward W. Felten explained in a declaration submitted to the district court, the program places in the hands of the government a comprehensive record of Americans' telephonic associations, and this record

---

id. at 4. The government stores the results of its queries in a separate database, to which the government has practically unfettered access and may apply "the full range of SIGINT analytic tradecraft." June 19, 2014 Primary Order at 12 n.15.

[7] *See*, *e.g.*, Leslie Cauley, *NSA Has Massive Database of Americans' Phone Calls*, USA Today (May 10, 2006), http://usat.ly/1nKurU9.

[8] *See* Verizon Secondary Order (ERII 116–19).

[9] *See*, *e.g.*, White House, Administration White Paper: *Bulk Collection of Telephony Metadata Under Section 215 of the USA PATRIOT Act* 1 (Aug. 9, 2013), http://bit.ly/15ebL9k ("White Paper"); Decl. of John Giacalone ¶¶ 6, 11, 13, 29 ("Giacalone Decl.") (ERII 67, 69, 70, 76).

[10] *See* June 19, 2014 Primary Order.

reveals a wealth of detail about familial, political, professional, religious, and intimate relationships—the same kind of information that could traditionally be obtained only by examining the contents of communications. *See* Decl. of Professor Edward W. Felten ¶¶ 38–64 ("Felten Decl.") (ERII 92–101). By aggregating metadata across time, the government can learn "when we are awake and asleep; our religion . . . ; our work habits and our social aptitude; the number of friends we have; and even our civil and political affiliations." *Id*. ¶ 46 (ERII 95). It can learn about "the rise and fall of intimate relationships, the diagnosis of a life-threatening disease, the telltale signs of a corporate merger or acquisition, the identity of a prospective government whistleblower, the social dynamics of a group of associates, or even the name of an anonymous litigant." *Id*. ¶ 58 (ERII 99).[11]

Two review groups appointed by President Obama have echoed Professor Felten's observations, and both groups—the Presidential Review Group on Intelligence and Communications Technologies ("PRG") and the Privacy and Civil Liberties Oversight Board ("PCLOB")—roundly condemned the call-records program on legal and policy grounds. The PCLOB explained that because call

[11] *See generally* Privacy and Civil Liberties Oversight Board, 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 12, 156–57 (Jan. 23, 2014), http://bit.ly/1aERqzw ("PCLOB Report"); Presidential Review Group on Intelligence and Communications Technologies, *Liberty and Security in a Changing World*, 110–14, 116–17 (Dec. 12, 2013), http://1.usa.gov/1cBct0k ("PRG Report").

records "can reveal intimate details about a person's life, . . . the government's collection of a person's entire telephone calling history has a significant and detrimental effect on that person's privacy." PCLOB Report 156. Because of this intrusiveness, the PRG wrote, the call-records program is likely to "seriously chill 'associational and expressive freedoms.'" PRG Report 117 (*quoting United States v. Jones*, 132 S. Ct. 945, 956 (2012) (Sotomayor, J., concurring)). "Knowing that the government is one flick of a switch away from such information can profoundly 'alter the relationship between citizen and government in a way that is inimical to society.'" PRG Report 117; *accord* PCLOB Report 161–64.

In addition to raising these privacy concerns, both review groups appointed by President Obama emphatically concluded that the program failed to yield any significant benefit at all to the nation's security. After exhaustive investigations that included access to classified information and interviews with intelligence officials, both review groups confirmed that there was "little evidence that the unique capabilities provided by the NSA's *bulk* collection of telephone records actually have actually yielded material counterterrorism results that could not have been achieved without the NSA's Section 215 program." PCLOB Report 146 (emphasis in original); *see* PRG Report 104. The PCLOB specified: "[W]e have not identified a single instance involving a threat to the United States in which the telephone records program made a concrete difference in the outcome of a

counterterrorism investigation." PCLOB Report 11. The PRG confirmed this conclusion: "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 have been obtained in a timely manner using conventional section 215 orders." PRG Report 104.

C. President Obama Acknowledges that the Government's Investigative Interest Can Be Accommodated Without Bulk Collection of Call Records.

On January 17, 2014, President Obama delivered a national address about the government's ongoing review of its signals-intelligence programs. During the address, the President announced immediate revisions to the call-records program.[12] He first acknowledged that the program "could be used to yield more information about our private lives, and open the door to more intrusive bulk collection programs in the future." President's Statement. Conceding that the government could achieve its investigative aims without bulk collection of call records, he announced that his administration would seek certain limited modifications of the FISC orders that governed the program and, separately, would pursue legislation to effectively end the program in favor of more targeted collection. *Id*. The FISC later adopted the President's proposed modifications relating to the use and retention of call records, *see* Bulk Call-Records

[12] *See* President Barack Obama, Remarks by the President on Review of Signals Intelligence (Jan. 17, 2014), http://1.usa.gov/1l2zOBS ("President's Statement").

Modification Order, but the government's bulk *collection* of Americans' call records continues.[13]

PROCEDURAL HISTORY

A. Litigation Challenging the Call-Records Program.

The Guardian's publication of the Secondary Order directed at Verizon Business prompted the filing of several lawsuits challenging the government's call-records program, including this one. *See* Compl. (June 12, 2013) (ECF No. 1); *Klayman v. Obama*, No. 13-cv-851 (D.D.C. June 6, 2013); *ACLU v. Clapper*, No. 13 Civ. 3994 (S.D.N.Y. June 11, 2013); *First Unitarian Church of L.A. v. NSA*, No. 13-cv-3287 (N.D. Cal. July 16, 2013).

In December 2013, two of these cases proceeded to judgment. First, on December 16, 2013, Judge Richard Leon of the District of D.C. preliminarily enjoined the collection as a violation of the Fourth Amendment, sharply noting: "I cannot imagine a more 'indiscriminate' and 'arbitrary invasion' than this

[13] In particular, the modifications (i) "generally preclude the government from querying the telephony metadata without first having obtained, by motion, a determination by [the FISC] that each selection term to be used satisfies [a 'reasonable articulable suspicion'] standard," and (ii) "limit the results of each query to metadata associated with identifiers that are within two, rather than three, 'hops' of the approved seed used to conduct the query." Bulk Call-Records Modification Order at 4. These changes do not affect Mrs. Smith's claims in this lawsuit, because the claims relate principally to the collection of Mrs. Smith's call records, and only secondarily to the government's use of the records once collected.

systematic and high-tech collection and retention of personal data on virtually every single citizen." *See Klayman v. Obama*, 957 F. Supp. 2d 1, 42 (D.D.C. 2013). Less than two weeks later, Judge William Pauley of the Southern District of New York arrived at the opposite conclusion, holding that the Supreme Court's decision in *Smith v. Maryland*, 442 U.S. 735 (1979), "control[led]" the Fourth Amendment analysis. *ACLU v. Clapper*, 959 F. Supp. 2d 724, 752 (S.D.N.Y. 2013). Both cases are now pending before the Courts of Appeals. *See Klayman v. Obama*, No. 14-5004 (D.C. Cir. 2014) (oral argument scheduled Nov. 4, 2014); *ACLU v. Clapper*, No. 14-42 (2d Cir. 2014) (oral argument held Sept. 2, 2014).

B. This Lawsuit.

Days after the public revelation that the government was engaging in the bulk collection of call records from Verizon Business, Mrs. Smith filed this lawsuit. *See* Compl. (June 12, 2013) (ECF No. 1). Mrs. Smith, a Verizon Wireless customer, alleged that the government was collecting her call records and that the program violated her Fourth Amendment rights. *See* Amended Compl. ¶¶ 15–24, 27 (ERII 124–26).[14] Mrs. Smith requested the government end its collection of her call records and purge any of her call records already collected under the program. *See* Amended Compl. at 5 (ERII 126). On December 20, 2013, Mrs. Smith moved

[14] Mrs. Smith further alleged that the call-records program violated Section 215 and the First Amendment, but she later withdrew those claims. *See* Amended Compl. ¶¶ 25–26 (ERII 126); Dist. Ct. Op. 3 n.1 (ERI 3).

for a preliminary injunction. *See* Pl.'s PI Mot. (Dec. 20, 2013) (ECF No. 8).

On January 24, 2014, the government filed an opposition to Mrs. Smith's motion for a preliminary injunction and moved to dismiss the complaint. *See* Gov't Mot. to Dismiss (Jan. 24, 2014) (ECF No. 15). The government argued Mrs. Smith had no standing to bring the lawsuit. Even if she did have standing, the government argued, the collection of call records under Section 215 was not inconsistent with the Fourth Amendment. *See, e.g.*, Oral Arg. Tr. 43 (ERII 54).

On June 6, 2014, the district court entered judgment for the government on both parties' motions. The court rejected the government's argument that Mrs. Smith lacked standing, noting that she was a "Verizon customer" and quoting Judge Leon's conclusion in *Klayman* that there was "strong evidence" that the NSA had collected and queried Verizon Wireless metadata. Dist. Ct. Op. 2 n.2 (ERI 3) (quoting *Klayman*, 957 F. Supp. 2d at 26–28). The court felt "constrain[ed]," however, to dismiss Mrs. Smith's complaint because of *Smith v. Maryland* and its progeny. Dist. Ct. Op. 8 (ERI 8). It acknowledged that the "data collected by the NSA . . . reaches into [Mrs. Smith's] personal information," and that the call-records program is "revealing" of personal details and information people would likely keep private. *Id*. at 3–4 (ERI 3–4).[15] The court also recognized

[15] The district court expressed concern that the government is collecting information about Americans' locations under the call-records program. *See* Dist. Ct. Op. 4–7 (ERI 4–7). Mrs. Smith did not advance that argument below and does

the "gulf" between the privacy intrusions in *Smith* and those caused by the call-records program. *See id*. at 5 (ERI 5). It concluded, however, that *Smith* controlled. *See id.* at 8 (ERI 8).

The court denied Mrs. Smith's motion for preliminary relief and granted the government's motion to dismiss. *See id.* (ERI 8).

SUMMARY OF ARGUMENT

The district court erred in granting the government's motion to dismiss and denying Mrs. Smith's motion for a preliminary injunction. Phone records reveal personal details and relationships that most people customarily and justifiably regard as private. The government's long-term collection and aggregation of this information invades a reasonable expectation of privacy and constitutes a search. This search violates the Fourth Amendment because it is conducted without a warrant or probable cause and because it is far more intrusive than can be justified by any legitimate government interest.

Mrs. Smith is entitled to a preliminary injunction prohibiting the government from collecting her call records under this program, and requiring it to purge those records it has already collected. The government has no legitimate interest in conducting unlawful surveillance. Further—as multiple independent reviews have

---

not do so on appeal, and the district court ultimately disavowed consideration of the possibility in its opinion. *See id*. at 7 (ERI 7).

found, and as the president himself has acknowledged—the government's legitimate goal of tracking suspected terrorists' associations can be accomplished through far less-intrusive means.

STANDARD OF REVIEW

The Court reviews *de novo* a district court's dismissal of a complaint pursuant to Federal Rule of Civil Procedure 12(b)(1) or (b)(6), accepting as true all material factual allegations in the complaint and construing the pleadings in the light most favorable to the plaintiff. *See Von Saher v. Norton Simon Museum of Art at Pasadena*, 754 F.3d 712, 719 (9th Cir. 2014). When reviewing a court's denial of a preliminary injunction, this Court reviews the district court's legal conclusions *de novo*, its findings of fact for clear error, and its ultimate decision for abuse of discretion. *See Alliance for Wild Rockies v. Cottrell*, 632 F.3d 1127, 1131 (9th Cir. 2011).

ARGUMENT

I. THE CALL-RECORDS PROGRAM VIOLATES THE FOURTH AMENDMENT.

A. The Government's Long-Term Collection and Aggregation of Call Records Constitutes a Search.

The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated." U.S. Const., amend. IV. A "search" under the

Fourth Amendment occurs "when the government violates a subjective expectation of privacy that society recognizes as reasonable." *Kyllo v. United States*, 533 U.S. 27, 33 (2001); *see Katz v. United States*, 389 U.S. 347, 361 (1967) (Harlan, J., concurring). The government's long-term collection and aggregation of Americans' call records, including Mrs. Smith's call records, invades a reasonable expectation of privacy. As a result, the long-term collection and aggregation of this sensitive information is, by itself, a search under the Fourth Amendment.[16]

1. Neither *Smith* nor any other precedent authorizes the suspicionless collection of call records in bulk.

Given the great differences between the facts of *Smith* and the NSA's call-records program, *Smith* simply cannot bear the weight the government seeks to place on it.

In *Smith*, the Baltimore police suspected that Michael Smith was making threatening and obscene phone calls to a woman he had robbed days earlier. To confirm their suspicions, they asked his telephone company to install a "pen register" on his line to record the numbers he dialed. 442 U.S. at 737. After just

[16] For similar reasons, the collection of Mrs. Smith's call records is also a "seizure" for Fourth Amendment purposes. *See United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1171–72, 1176 (9th Cir. 2010) (en banc) (per curiam) (describing the government's copying of electronic data as a seizure); *Katz*, 389 U.S. at 354 (describing the government's recording of a phone call as a "search and seizure"); *United States v. Ganias*, 755 F.3d 125, 137 (2d Cir. 2014) (the government's denial "of exclusive control over" copies of digital files constituted "a meaningful interference with . . . possessory rights in those files and constituted a seizure within the meaning of the Fourth Amendment").

three days, the pen register confirmed that Mr. Smith was the culprit. *Id.* The Supreme Court upheld the warrantless installation of the pen register, but the stakes were small. The pen register was very primitive—it tracked the numbers being dialed, but it did not indicate which calls were completed, let alone the duration of those calls. *Id.* at 741. It was in place for only three days, and it was directed at a single criminal suspect. *Id.* at 737. Moreover, the information it yielded was not aggregated with information from other pen registers, let alone with information relating to hundreds of millions of other people. *Id.*

The differences between the government's call-records program and the pen register in *Smith* are obvious. The surveillance in *Smith* continued for three days, but the surveillance at issue here is effectively permanent. The surveillance in *Smith* was primitive and narrow, involving only the numbers dialed, but the surveillance at issue here is much broader, encompassing (among other things) the duration of calls. The surveillance in *Smith* was directed at a single criminal suspect, but the surveillance at issue here reaches hundreds of millions of people, most of them—like Mrs. Smith—not connected even remotely with the activity the government is investigating. Moreover, unlike in *Smith*, the government here is concededly aggregating the records of all of these people in a massive database. This aggregation compounds the invasiveness of the surveillance, because the government acquires more information about any given individual by monitoring

the call-records of that individual's contacts—and by monitoring the call-records of those *contacts'* contacts.

Smith did not involve long-term and profoundly intrusive surveillance of hundreds of millions of people, and accordingly *Smith* does not control this case. *See Klayman*, 957 F. Supp. 2d at 31.

The court below pointed to post-*Smith* decisions, including decisions of this Court, that applied *Smith* to other contexts. *See* Dist. Ct. Op. 5 (ERI 5). These cases, too, however, involved targeted, short-term surveillance of individual criminal suspects. None of them addressed the kind of bulk collection at issue here. For example, *United States v. Forrester*, 512 F.3d 500 (9th Cir. 2008), extended *Smith* to reach the use of a pen register to capture internet metadata of a single criminal suspect for discrete periods of time. *See id.* at 505, 509-511. This Court specifically noted, however, that its holding did not extend to "more intrusive" surveillance methods or to those that would reveal more sensitive information, like data that could be similar to the "content" of a communication. *Id.* at 511. The other cases cited by the district court involved only individualized collection of customer records based on individualized suspicion of criminal activity. *See United States v. Reed*, 575 F.3d 900, 906, 914 (9th Cir. 2009); *United States v. Golden Valley Elec. Ass'n*, 689 F.3d 1108, 1111, 1116 (9th Cir. 2012).

The Supreme Court has long recognized that dragnet or bulk surveillance raises distinct constitutional concerns. Indeed, the Court made this explicit just four years after it decided S*mith*, when it considered the government's warrantless use of a beeper to track the car of a suspected manufacturer of narcotics. *See United States v. Knotts*, 460 U.S. 276 (1983). While the Court found the defendant lacked a reasonable expectation of privacy in his public movements in the circumstances of that case, it cautioned that *Smith* could not be read to justify "twenty-four hour surveillance of any citizen of this country." *Id.* at 283 (quotation marks omitted). "Dragnet type law enforcement practices," the Court wrote, would present a different constitutional question. *Id.* at 284; *see also United States v. Pineda-Moreno*, 591 F.3d 1212, 1216 n. 2 (9th Cir. 2010) (reserving right to consider "programs of mass surveillance") (quotation marks and citation omitted), *vacated* 132 S. Ct. 1533 (2012).

The D.C. Circuit addressed that distinct constitutional question in *United States v. Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd sub nom*. *United States v. Jones*, 132 S. Ct. 945 (2012), holding that the government's thirty-day tracking of an individual's movements amounted to a search for Fourth Amendment purposes. The D.C. Circuit rejected the government's invitation to read *Knotts*—a case that, again, involved targeted surveillance—to authorize long-term surveillance. *Knotts* did not hold, the D.C. Circuit wrote, that an individual "has no reasonable

expectation of privacy in his movements whatsoever, world without end, as the Government would have it." 615 F.3d at 557.

Unanimously affirming *Maynard* in *Jones*, all nine justices of the Supreme Court agreed with the D.C. Circuit's conclusion that long-term location surveillance raises distinct and novel questions not controlled by prior precedent. The plurality opinion for the Court noted: "[I]t may be that achieving [long-term location tracking] through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question." *Jones*, 132 S. Ct. at 954.

The Supreme Court ultimately decided *Jones* on trespass grounds, not on the basis of the expectation-of-privacy analysis relied on by the D.C. Circuit in *Maynard*. Five of the Justices in *Jones*, however, made clear that they would resolve the reasonable-expectation-of-privacy question as had the appellate court below. Justice Alito concluded that "the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment" *id.* at 964 (Alito, J., concurring). Justice Sotomayor concurred: "at the very least, 'longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.'" *Id.* at 955 (Sotomayor, J., concurring).

The full Court addressed a related point two years later in *Riley* in the context of cell phones, noting: "[T]here is an element of pervasiveness that

characterizes cell phones but not physical records . . . . Although the data stored on a cell phone is distinguished from physical records by quantity alone, certain types of data are also qualitatively different." *Riley*, 134 S. Ct. at 2490, (citing *Jones*, 132 S. Ct. at 955 (Sotomayor, J., concurring)); *id.* at 2489. The Court's elaboration focused on smartphone technologies, but its observation applies equally to call records, where new technology "allows even just one type of information to convey far more than previously possible." *Id.* at 2489. Notably, the Court in *Riley* specifically observed that thousands of photos could reconstruct the "sum of an individual's private life" in a way that just one or two photos could not. *Id.*

Riley thus confirms the obvious: analog-era precedents cannot be extended mechanically to factual contexts dramatically different from those that gave rise to them. Thus, the Supreme Court in *Riley* unanimously rejected the government's "strained" attempt to analogize cell-phone searches to the searches of physical items—like packs of cigarettes—that the Court had approved decades earlier. *See id*. at 2491; *id.* at 2484–89 (discussing *Chimel v. California*, 395 U.S. 752 (1969)); *United States v. Robinson*, 414 U.S. 218 (1973). As this Court has recognized, in assessing the intrusiveness and ultimately the reasonableness of government action, "technology matters." *United States v. Cotterman*, 709 F.3d 952, 965 (9th Cir. 2013) (holding that Supreme Court case authorizing a suspicionless border search of a car did not authorize a suspicionless comprehensive search of the

digital contents of an electronic device). Automatically extending cases from a different era involving primitive—and thus less intrusive and revealing—technologies to novel contexts in the digital age ignores the "power of technology to shrink the realm of guaranteed privacy." *Kyllo*, 533 U.S. at 34. Instead, courts must confront the technology before them, "take the long view, from the original meaning of the Fourth Amendment forward," and avoid the temptation to simply analogize from cases involving more limited, less intrusive, and less revealing surveillance. *Id.* at 40.

In *Klayman*, Judge Leon appropriately applied this logic to the question of *Smith*'s relevance to the call-records program: "In sum, the *Smith* pen register and the ongoing NSA Bulk Telephony Metadata Program have so many significant distinctions between them that I cannot possibly navigate these uncharted Fourth Amendment waters using as my North Star a case that predates the rise of cell phones." 957 F. Supp. 2d at 37. This Court should do the same here, and tackle the call-records program for what it is—a novel and unprecedented intrusion into the privacy of millions of innocent Americans, including Mrs. Smith.

2. The long-term collection and aggregation of call records intrudes on a reasonable expectation of privacy.

Because *Smith* does not control this case, the Court must analyze Mrs. Smith's Fourth Amendment claim by applying the familiar test described by Justice Harlan in *Katz*—that is, by asking whether individuals have a reasonable

expectation of privacy in the information the government seeks. *Katz*, 389 U.S. at 360-61 (Harlan, J., concurring). In the district court, the government did not dispute that Mrs. Smith has a subjective expectation of privacy in the personal information revealed in the many years' worth of her call records that the government has collected. *See United States v. Nerber*, 222 F.3d 597, 599 (9th Cir. 2000) (Fourth Amendment requires person have "expectation that his activities would be private").[17]

Mrs. Smith's expectation of privacy is also objectively reasonable.

The sensitivity of Americans' call records—when collected over time and aggregated with the records of millions of others—is widely recognized. Professor Felten, as well as the presidentially appointed PRG and PCLOB, have all explained how the government's collection of a comprehensive record of Americans' telephone calls exposes an astonishing amount about each of us. *See supra* at 6–8. It reveals our religious, familial, political, and intimate relationships; our sleeping, sexual, and work habits; our health problems, our closest friendships, and our business plans. *See* Felten Decl. ¶¶ 38–64 (ERII 92–101); *see also* PCLOB Report 12, 156–57; PRG Report 110–14, 116–17. In other words, one's call records are, when collected over time and aggregated with those of others, a proxy for content.

[17] Similarly, the district court did not question whether Mrs. Smith maintains a subjective expectation of privacy in her phone records. *See* Decl. of Anna Smith ¶¶ 5–10 (ERII 120); *see also* PCLOB Report 156–58; PRG Report 110–17.

It was for precisely this reason that a majority of the Supreme Court in *Jones* recognized that the long-term collection of personal data concerning even one individual can intrude upon a reasonable expectation of privacy where more limited surveillance might not. *See Jones*, 132 S. Ct. at 964 (Alito, J., concurring); *id.* at 955 (Sotomayor, J., concurring). As Justice Sotomayor recognized, long-term location tracking "enables the Government to ascertain, more or less at will, [every person's] political and religious beliefs, sexual habits, and so on." *Id.* at 956 (Sotomayor, J., concurring); *id*. at 955–56 ("GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations. The Government can store such records and efficiently mine them for information years into the future. And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility." (quotation marks and citations omitted)).

What the Supreme Court observed of long-term monitoring in *Jones* is equally true of the bulk collection of Americans' telephone records here. *See* Felten Decl. ¶¶ 38–64 (ERII 92–101); PCLOB Report 156–58; *cf. Klayman* ("Admittedly, what metadata *is* has not changed over time. . . . But the ubiquity of

phones has dramatically altered the *quantity* of information that is now available and, *more importantly,* what that information can tell the Government about people's lives. . . . I think it is . . . likely that these trends have resulted in a *greater* expectation of privacy and a recognition that society views that expectation as reasonable.").

These features of the call-records program—features that the government has never disputed—dictate the conclusion that the government intrudes on a reasonable expectation of privacy when it collects Mrs. Smith's telephony metadata.

To support its argument below, the government invoked the so-called "third-party" rule, which holds, in the government' view, that an individual surrenders her constitutional privacy interest in information if she entrusts that information to a third party. But the "third-party" rule does not operate like an on-off switch even outside the digital context. Thus, in *Ferguson v City of Charleston*, 532 U.S. 67, 78 (2001), the Supreme Court found that a "reasonable expectation of privacy enjoyed by the typical patient undergoing diagnostic tests in a hospital is that the results of those tests will not be shared with nonmedical personnel without her consent." In *Stoner v. California*, 376 U.S. 483, 489–90 (1964), the Supreme Court protected a hotel guest against police entry even after finding that he "gives 'implied or express permission' to such persons as maids, janitors or repairmen' to enter his

room 'in the performance of their duties.'" *See also Chapman v. United States*, 365 U.S. 610, 616 (1961) (holding that police intrusion onto premises is subject to the Fourth Amendment even if landlord may enter for limited purpose); *Bond v. United States*, 529 U.S. 334, 338–39 (2000) (expectation of privacy in personal luggage in overhead bin on bus); *United States v. Young*, 573 F.3d 711, 716-17 (9th Cir. 2009) (expectation of privacy in hotel room and luggage left in room).

The same approach applies in the digital world, with courts recognizing that the mere fact that a person entrusts information to a third party does not necessarily mean that she has surrendered her constitutional right to privacy in the information. For example, a person sending an email "voluntarily discloses" the electronic contents of the email to the email provider so that the email may be transmitted, just as a person making a phone call "voluntarily discloses" the number she dials so that the call may be completed. Yet the email sender nonetheless retains a reasonable expectation of privacy in the email she has disclosed to her email provider. *See United States v. Warshak*, 631 F.3d 266, 286–87 (6th Cir. 2010) (expectation of privacy in emails stored online). In *Cotterman*, this Court recognized that emails "are expected to be kept private and this expectation is 'one that society is prepared to recognize as reasonable.'" 709 F.3d at 964 (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)). Very recently, the Eleventh Circuit found a reasonable expectation of privacy in cell-phone location records stored by

a cell phone provider. *United States v. Davis*, 754 F.3d 1205, 1217 (11th Cir. 2014).

In sum, the third-party rule has never been an all or nothing proposition. For these reasons, Mrs. Smith has a reasonable expectation of privacy in the information revealed by her aggregated phone records. Accordingly, the government's collection of this information constitutes a search.[18]

B. The Government's Long-Term Collection and Aggregation of Call Records Violates the Fourth Amendment.

1. The government's long-term collection and aggregation of call records is unconstitutional because it is warrantless and lacks probable cause.

Because the call-records program invades Americans' privacy without a warrant drawn with particularity and supported by probable cause, it violates the Fourth Amendment. Warrantless searches are "per se unreasonable," subject only to a few "jealously and carefully drawn" exceptions. *Coolidge v. New Hampshire*, 403 US 443, 454–55 (1971) (quotations omitted). Because none of these "well-delineated exceptions" applies, no further analysis is necessary. *See Al Haramain Islamic Found., Inc. v. U.S. Dep't of Treasury*, 686 F.3d 965, 990 (9th Cir. 2011)

[18] When the government queries the database in which it amasses these call records, *see supra* n.6, it engages in a separate and further search under the Fourth Amendment. Each of those queries involves an examination of Mrs. Smith's call records for the purpose of determining whether she has communicated with an NSA target, or with someone else who has communicated with an NSA target. *See id.*

(quoting *Katz*, 389 U.S. at 357).

The Fourth Amendment's warrant and particularity requirements prohibit general searches by interposing a judge between the citizen and the state, leaving the government with no discretion as to what it can take. *See Stanford v. Texas*, 379 U.S. 476, 485 (1964); *Warden v. Hayden*, 387 U.S. 294, 301 (1967). The search of Mrs. Smith's highly personal information here is a general search predicated on a general warrant, which renders the search *per se* unconstitutional. *See Berger v. New York*, 388 U.S. 41, 59 (1967).

The "reviled" general warrant, "which allowed British officers to rummage through homes in an unrestrained search," was one of the causes of the American Revolution itself, and the primary motivation for adoption of the Fourth Amendment. *Riley*, 134 S. Ct. at 2494. In *Stanford*, the Supreme Court explained that writs of assistance gave "customs officials blanket authority to search where they pleased for goods imported in violation of the British tax laws." 379 U.S. at 481. The Founders objected because general warrants permitted the government to engage in "exploratory rummaging" absent any individualized suspicion. *Andresen v. Maryland*, 427 U.S. 463, 480 (1976); *see Riley*, 134 S. Ct. at 2494.

"The wholesale seizure for later detailed examination of records not described in a warrant" is "the kind of investigatory dragnet" the Fourth Amendment prohibits. *United States v. Tamura*, 694 F.2d 591, 595 (9th Cir. 1982)

(quoting *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980) (quotation marks omitted)). Thus, in *United States v. Kow*, 58 F.3d 423 (9th Cir. 1995), this Circuit found that a search warrant that "contained no limitations on which documents . . . could be seized or suggested how they related to specific criminal activity" failed the particularity requirement. 58 F.3d at 427. The Court held that "generalized seizure" of a large collection of documents may be justified only on a showing of probable cause that the entire collection was likely to show evidence of criminal activity. *Id.*

The call-records program fails all of these requirements. It is wholesale and unlimited, because the government acquires the complete call records of Mrs. Smith and millions of others—and, therefore, the highly detailed personal information revealed by those records, especially when aggregated. There is no particularity to the government's demand for call records; nor is there *any* showing that a given person's call records contain information about terrorist or criminal activity, much less any showing that would amount to individualized suspicion. Thus, like a general search, the program involves searches not predicated upon "an oath or information supplying cause." Morgan Cloud, *Searching Through History; Searching For History*, 63 U. Chi. L. Rev. 1707, 1738 (1996); *accord Stanford*, 379 U.S. at 481; *see* 50 U.S.C. § 1861(b)(2)(a) (requiring only a "showing that there are reasonable grounds to believe that the tangible things sought are relevant

to an authorized [foreign-intelligence] investigation."). It is "not restricted to searches of specific places or to seizures of specific goods." Cloud, 63 U. Chi. L. Rev. at 1738; *see also Berger*, 388 U.S. at 59 (striking down electronic-surveillance statute that, like "general warrants," left "too much to the discretion of the officer executing the order" and gave the government "a roving commission to seize any and all conversations" (quotation marks omitted)).

2. No exception to the warrant and probable cause requirement applies.

Below, the government argued that the warrant requirement does not apply because the call-records program serves special government needs. *See, e.g.*, Oral Arg. Tr. 43 (ERII 54). But the "special needs" doctrine applies "[o]nly in those exceptional circumstances in which special needs, beyond the normal need for law enforcement, make the warrant and probable-cause requirement impracticable." *New Jersey v. T.L.O.*, 469 U.S. 325, 351 (1985) (Blackmun, J., concurring); *see Ferguson*, 532 U.S. at 81–86; *City of Indianapolis v. Edmond*, 531 U.S. 32, 41–47 (2000).

Here, application of the warrant and individualized-suspicion requirements would not compromise the government's asserted interest in determining which individuals were in contact with phone numbers associated with suspected terrorists. *See infra* Part I.B.3. To the contrary, the PCLOB, the PRG, and the President himself have determined that the government can accomplish its aims

using individualized court orders and without collecting or aggregating hundreds of millions of individuals' call records. *See* PCLOB Report 146; PRG Report 118–19; White House, Office of the Press Secretary, *The Administration's Proposal for Ending the Section 215 Bulk Telephony Metadata Program* (Mar. 27, 2014), http://1.usa.gov/1gS2HK0. Even if one assumes that the call-records program allows the government to learn terrorists' associations *more rapidly* than it would otherwise be able to do, the Supreme Court has never dispensed with the Fourth Amendment's core constraints based on simple expedience. *See, e.g.*, *Carroll v. United States*, 267 U.S. 132, 153–54 (1925); *United States v. Barbera*, 514 F.2d 294, 301–02 (2d Cir. 1975). Moreover, in any true emergency the government could satisfy the exigent-circumstances exception to the warrant requirement, an exception it does not assert applies to the mass collection generally. *See Riley*, 134 S. Ct. at 2494; *Missouri v. McNeely*, 133 S. Ct. 1552, 1570 (2013).

3. The government's long-term collection and aggregation of call records is unconstitutional because it is unreasonable.

Even if an exception to the warrant and probable-cause requirements applies, such as the special needs exception, the call-records program is unconstitutional because it is unreasonable under the Fourth Amendment. Special needs searches are a "closely guarded category." *Chandler v. Miller*, 520 U.S. 305, 309 (1997). They are permitted only "[i]n limited circumstances, 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, a search may be reasonable despite the absence of [individualized] suspicion." *Id.* at 314 (quoting *Skinner v. Ry. Labor Executives Assoc.*, 489 U.S. 602, 624 (1989)).

Reasonableness is determined by examining the "totality of circumstances" to "assess[], on the one hand, the degree to which [government conduct] 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) (quotation marks omitted); *see also Virginia v. Moore*, 553 U.S. 164, 169 (2008). In the context of government surveillance, this test demands that statutes be "precise and discriminate" and that the government's surveillance authority be "carefully circumscribed so as to prevent unauthorized invasions" of privacy. *Berger*, 388 U.S. at 58. The call-records program—in which the government has employed the most indiscriminate means possible to pursue its limited goal of tracking the associations of a discrete number of suspected terrorists—cannot meet this burden.

As an initial matter, the intrusion here cannot by any stretch of the imagination be described as "minimal." The government is permanently tracking the phone calls of millions of innocent people, and the records the government is collecting contain a wealth of information that can be every bit as revealing as the

content of calls. *See* Felten Decl. ¶¶ 38–64 (ERII 92–101); PCLOB Report 12, 156–58; PRG Report 110–14, 116–17; *see also Klayman*, 957 F. Supp. 2d at 33–37, 39. Mrs. Smith's privacy interest in the intimate details of her personal life revealed by her phone records, far from being "minimal," lies at the heart of the Fourth Amendment. As previously described, a person's phone records reveal a vast array of intimate details about that person's private life, including medical, religious, romantic, family and political information. *See supra* Part I.A.2.

The program also lacks any of the traditional indicia of reasonableness. The government is collecting all of these records without individualized suspicion, without temporal limit, and without limitation as to the individuals or phone calls swept up in the collection. *See, e.g.*, *Berger*, 388 U.S. at 55–56, 59–60 (invalidating surveillance statute due to the breadth, lack of particularity, and indefinite duration of the surveillance it authorized); *Chandler*, 520 U.S. at 313 ("To be reasonable under the Fourth Amendment, a search ordinarily must be based on individualized suspicion of wrongdoing."); *United States v. Duggan*, 743 F.2d 59, 73 (2d Cir. 1984) (FISA's requirement of individualized suspicion that the government's target is an "agent of a foreign power" is part of what makes it "reasonable."); *United States v. Tortorello*, 480 F.2d 764, 773–74 (2d Cir. 1973) (Title III provides for "particularity in the application and order" and "clearly circumscribe[s] the discretion" of the government "as to when the surveillance

should end."); *United States v. Cafero*, 473 F.2d 489, 498 (3d Cir. 1973) (similar); *In re Sealed Case*, 310 F.3d 717, 739–40 (FISCR 2002) (describing "constitutionally significant" limitations on the government's search powers).

The program also sweeps far more broadly than necessary to achieve the government's goals. The government's stated interest is in identifying unknown terrorist operatives and thereby preventing terrorist attacks. *See, e.g.*, Oral Arg. Tr. 43 (ERII 54). But the record makes clear that the call-records program has not achieved this goal. The record also makes clear, perhaps even more significantly, that the government could achieve its goal without collecting the phone records of millions of innocent Americans.[19]

The program's ineffectiveness has now been confirmed by multiple sources that have had broad access to the government's secret programs. Judge Leon noted: "[T]he 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." *Klayman*, 957 F. Supp. 2d at 40. Senator Wyden, who sits on the Senate Intelligence Committee, agrees: "I have seen absolutely zero evidence that the bulk

[19] *See* Jennifer Valentino-Devries & Siobhan Gorman, *Secret Court's Redefinition of 'Relevant' Empowered Vast NSA Data-Gathering*, Wall St. J., (July 8, 2013) http://on.wsj.com/14N9j6j (quoting Rep. Jim Sensenbrenner) ("It's like scooping up the entire ocean to . . . catch a fish.").

collection of Americans' phone records under Section 215 of the PATRIOT Act has provided any unique value to intelligence gathering or actually made Americans any safer . . . ."[20] As explained above, the President's Review Group also concluded 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."[21] This conclusion was echoed by the Privacy and Civil Liberties Oversight Board: "[W]e have seen little indication that the same result could not have been obtained through traditional, targeted collection of telephone records."[22]

The government itself has effectively conceded that the bulk collection of call records is unnecessary. For instance, the government has stated that it queried the phone-records database fewer than 300 times in 2012, *see* White Paper 4—but this merely confirms that the government could achieve its goals with targeted surveillance (such as serving the phone companies with demands for records relating to particular terrorism suspects).[23] The evolution of the government's

---

[20] Press Release, Sen. Ron Wyden, Wyden Statement on President Obama's Proposed Reforms to the FISC and PATRIOT Act (Aug. 9, 2013), http://1.usa.gov/1bBEyWb.

[21] PRG Report 118–19.

[22] PCLOB Report 146.

[23] Multiple statutes permit the government to make such demands. *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-

arguments in defense of the program is also revealing. Although the government told the FISC in 2008 that bulk collection was the "only effective means" of tracking the associations of suspected terrorists, Order at 1–2, *In re Prod. of Tangible Things from [Redacted]*, No. BR 08-13 (FISC Mar. 2, 2009), the government has conspicuously avoided that representation in this litigation, *see, e.g.*, Giacalone Decl. ¶ 30 (ERII 77) (asserting that "NSA's analysis of bulk telephony metadata . . . provides the Government with *one means* of discovering communications involving unknown terrorist operatives" (emphasis added)). And earlier this year, then-NSA Director Keith Alexander conceded publicly that the dragnet surveillance of Americans' call records is simply unnecessary to acquiring "the information the NSA needs about terrorist connections."[24]

Given the admitted alternatives to the call-records program, the government cannot justify its massive intrusion into the privacy of Mrs. Smith and millions of other Americans. Although "the government's interest in preventing terrorism . . . is extremely high," the importance of that interest "is no excuse for the dispensing altogether with domestic persons' constitutional rights." *Al Haramain Islamic*

---

enforcement investigations); 18 U.S.C. § 2703(d) (orders for stored telephone records); Fed. R. Crim. P. 17(c) (subpoena duces tecum).

[24] Siobhan Gorman, *NSA Chief Opens Door to Narrower Data Collection*, Wall St. J. (Feb. 27, 2014), http://on.wsj.com/1cA6SIr ("But Gen. Alexander instead signaled that the information the NSA needs about terrorist connections might be obtainable without first collecting what officials have termed 'the whole haystack' of U.S. phone data.").

Foundation, 686 F.3d at 993; *see also United States v. U.S. District Court (Keith)*, 407 U.S. 297, 316-21 (1972) (rejecting government's argument that national security required dispensing with the warrant requirement in domestic security surveillance cases). "Emergency does not create power. Emergency does not increase granted power or remove or diminish the restrictions imposed upon power granted or reserved. . . . [¶] . . . [E]ven the war power does not remove constitutional limitations safeguarding essential liberties." *Home Bldg. & Loan Ass'n v. Blaisdell*, 290 U.S. 398, 425-26 (1934). Allowing even legitimate national security concerns to override the most fundamental of Fourth Amendment protections—the prohibition on the modern-day equivalent of the despised "general warrant"—would turn the Constitution on its head and destroy the basic civil liberties that the Founders fought to protect.

The totality of the circumstances demonstrates that the call-records program is unreasonable.

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

The district court below found that Mrs. Smith has standing to challenge the call-records program. ERI 3 (Dist. Ct. Op. 3 n.2). Because of the breadth of the program, there is no serious question that the government has collected records relating to Mrs. Smith's telephone calls—either because it has collected Mrs. Smith's call records from Verizon Wireless or because it has collected the

call records of Verizon Business subscribers with whom Mrs. Smith has been in contact. ER 123–25 (Amended Compl. ¶¶ 7–8, 15–17). That conclusion is consistent with the *Klayman* court's ruling that another Verizon Wireless subscriber had standing to sue. *See* 957 F. Supp. 2d at 26–28. The government has repeatedly claimed that the program's effectiveness depends on its comprehensiveness and, in particular, on the NSA's collection of call records from multiple providers. *See, e.g.*, White Paper 13 ("Unless the data is aggregated, it may not be feasible to identify chains of communications that cross different telecommunications networks."); Giacalone Decl. ¶ 29 (ERII 76) ("[A]ggregating the NSA telephony metadata from different telecommunications providers enhances and expedites the ability to identify chains of communications across multiple providers."). Both news reports and a statement by a member of the President's Review Group leave little doubt that Verizon Wireless—which has nearly 100 million cell-phone subscribers in the United States—is a participant in the program. *See, e.g.*, Siobhan Gorman, *et al.*, *U.S. Collects Vast Data Trove*, Wall St. J., June 7, 2013, http://on.wsj.com/1q5Jrkf ("The arrangement with Verizon, AT&T and Sprint, the country's three largest phone companies means, that every time the majority of Americans makes a call, NSA gets a record . . . ."); Geoffrey Stone, *Understanding Obama's NSA Proposals*, Daily Beast (Mar. 27, 2014), http://thebea.st/1nEh0oG ("Under the telephone metadata program, which

was created in 2006, telephone companies like Sprint, Verizon, and AT&T are required to turn over to the NSA, on an ongoing daily basis, huge quantities of telephone metadata involving the phone records of millions of Americans . . . .").

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

The Supreme Court has explained that "[a] plaintiff seeking a preliminary injunction must establish that he is likely to succeed on the merits, that he is likely to suffer irreparable harm in the absence of preliminary relief, that the balance of equities tips in his favor, and that an injunction is in the public interest." *Winter v. Natural Res. Def. Council,* 555 U.S. 7, 20 (2008).

For the reasons given above, Mrs. Smith is likely to succeed on the merits of her Fourth Amendment claim.[25] She is also likely to suffer irreparable injury if preliminary relief is not granted. In this Circuit, "[a]n alleged constitutional infringement will often alone constitute irreparable harm." *Goldie's Bookstore, Inc. v. Superior Court*, 739 F.2d 466, 472 (9th Cir. 1984); *see Assoc'd Gen. Contractors of Cal., Inc. v. Coal. for Econ. Equality*, 950 F.2d 1401, 1412 (9th Cir.

[25] Even if Mrs. Smith had not shown a likelihood of success on the merits, this Circuit has held that where the "hardship balance . . . tips sharply toward the plaintiff"—as it does here, *see infra*—a plaintiff need only demonstrate that there are "serious questions going to the merits" to support an injunction (rather than a likelihood of success), "so long as the plaintiff also shows that there is a likelihood of irreparable injury and that the injunction is in the public interest." *Alliance for Wild Rockies v. Cottrell*, 632 F.3d, 1127, 1135 (9th Cir. 2011). That this case presents "serious" legal questions is not in doubt.

1991). But even if this presumption did not apply, Mrs. Smith would satisfy the irreparable-harm standard. The continuation of the surveillance at issue means the continuation of the government's intrusion into Mrs. Smith's sensitive associations and communications. When the government takes this private information for its own purposes, the injury is immediate—it is complete as soon as the government interjects itself into the zone of privacy. *See United States v. Verdugo-Urquidez*, 494 U.S. 259, 264 (1990); *United States v. Balsys*, 524 U.S. 666, 692 (1998). The resulting invasion of privacy is an injury that cannot be undone. Indeed, it has long been established that the loss of constitutional freedoms, "for even minimal periods of time, unquestionably constitutes irreparable injury." *Elrod v. Burns*, 427 U.S. 347, 373 (1976).

Though the district court did not have occasion to address the balance of equities or whether an injunction would be in the public interest, both elements favor Mrs. Smith. On the one hand, each day brings new intrusions into Mrs. Smith's and millions of Americans' constitutionally protected privacy rights. *See Melendres v. Arpaio*, 695 F.3d 990, 1102 (9th Cir. 2012) ("[I]t is always in the public interest to prevent the violation of a party's constitutional rights."); *Sammartano v. First Judicial District Court*, 303 F.3d 959, 974 (9th Cir. 2002). On the other, the government has no legitimate interest in conducting surveillance that violates the Constitution. *See Sanders Cnty. Republican Cent. Comm. v. Bullock*,

698 F.3d 741, 749 (9th Cir. 2012) (the government receives "no legally cognizable benefit from being permitted to further enforce" an unconstitutional law); *Memphis Planned Parenthood, Inc. v. Sundquist*, 175 F.3d 456, 495 (6th Cir. 1999) ("[T]he public is certainly interested in preventing the enforcement of unconstitutional statutes and rules; therefore, no harm to the public will result from the issuance of the injunction here."). Moreover, the preliminary relief Mrs. Smith seeks would not prejudice the government because the call-records program as constituted is not necessary to achieve the government's aims. *See supra* Part I.B.3. Both the balance of hardships and the public interest weigh in favor of Mrs. Smith here.

CONCLUSION

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

DATED: September 2, 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

STATEMENT OF RELATED CASES

Undersigned counsel is aware of the following related case pending before this Court:

United States v. Moalin, No. 13-50572 (9th Cir. 2013).

DATED: September 2, 2014

Respectfully submitted,

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

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' Opening Brief complies with the type-volume limitation of Fed. R. App. P. 32(a)(7)(B) because this brief contains 9,576 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: September 2, 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 September 2, 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: September 2, 2014

Respectfully submitted,

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

Counsel for Plaintiff-Appellant ANNA J. SMITH

This page intentionally left blank.

ADDENDUM

TABLE OF CONTENTS

ADDENDUM

U.S. Const., Amend. IV

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

50 U.S.C.A. § 1861 (West)

(a)(1) Subject to paragraph (3), the Director of the Federal Bureau of Investigation or a designee of the Director (whose rank shall be no lower than Assistant Special Agent in Charge) may make an application for an order requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, provided that such investigation of a United States person is not conducted solely upon the basis of activities protected by the first amendment to the Constitution.

(2) An investigation conducted under this section shall

(A) be conducted under guidelines approved by the Attorney General under Executive Order 12333 (or a successor order); and

(B) not be conducted of a United States person solely upon the basis of activities protected by the first amendment to the Constitution of the United States.

(3) In the case of an application for an order requiring the production of library circulation records, library patron lists, book sales records, book customer lists, firearms sales records, tax return records, educational records, or medical records containing information that would identify a person, the Director of the Federal Bureau of Investigation may delegate the authority to make such application to either the Deputy Director of the Federal Bureau of Investigation or the Executive Assistant Director for National Security (or any successor position). The Deputy Director or the Executive Assistant Director may not further delegate such authority.

(b) Each application under this section

(1) shall be made to—

(A) a judge of the court established by section 1803(a) of this title; or

(B) a United States Magistrate Judge under chapter 43 of Title 28, who is publicly designated by the Chief Justice of the United States to have the power to hear applications and grant orders for the production of tangible things under this section on behalf of a judge of that court; and

(2) shall include—

(A) a statement of facts showing that there are reasonable grounds to believe that the tangible things sought are relevant to an authorized investigation (other than a threat assessment) conducted in accordance with subsection (a)(2) of this section to obtain foreign intelligence information not concerning a United States person or to protect against international terrorism or clandestine intelligence activities, such things being presumptively relevant to an authorized investigation if the applicant shows in the statement of the facts that they pertain to—

(i) a foreign power or an agent of a foreign power;

(ii) the activities of a suspected agent of a foreign power who is the subject of such authorized investigation; or

(iii) an individual in contact with, or known to, a suspected agent of a foreign power who is the subject of such authorized investigation; and

(B) an enumeration of the minimization procedures adopted by the Attorney General under subsection (g) of this section that are applicable to the retention and dissemination by the Federal Bureau of Investigation of any tangible things to be made available to the Federal Bureau of Investigation based on the order requested in such application.

(c)(1) Upon an application made pursuant to this section, if the judge finds that the application meets the requirements of subsections (a) and (b) of this section, the judge shall enter an ex parte order as requested, or as modified, approving the release of tangible things. Such order shall direct that minimization procedures adopted pursuant to subsection (g) of this section be followed.

(2) An order under this subsection—

(A) shall describe the tangible things that are ordered to be produced with sufficient particularity to permit them to be fairly identified;

(B) shall include the date on which the tangible things must be provided, which shall allow a reasonable period of time within which the tangible things can be assembled and made available;

(C) shall provide clear and conspicuous notice of the principles and procedures described in subsection (d) of this section;

(D) may only require the production of a tangible thing if such thing can be obtained with a subpoena duces tecum issued by a court of the United States in aid of a grand jury investigation or with any other order issued by a court of the United States directing the production of records or tangible things; and

(E) shall not disclose that such order is issued for purposes of an investigation described in subsection (a) of this section.

(d)(1) No person shall disclose to any other person that the Federal bureau of investigation has sought or obtained tangible things pursuant to an order under this section, other than to

(A) those persons to whom disclosure is necessary to comply with such order;

(B) an attorney to obtain legal advice or assistance with respect to the production of things in response to the order; or

(C) other persons as permitted by the Director of the Federal Bureau of Investigation or the designee of the Director.

(2)(A) A person to whom disclosure is made pursuant to paragraph (1) shall be subject to the nondisclosure requirements applicable to a person to whom an order is directed under this section in the same manner as such person.

(B) Any person who discloses to a person described in subparagraph (A), (B), or (C) of paragraph (1) that the Federal Bureau of Investigation has sought or obtained tangible things pursuant to an order under this section shall notify such person of the nondisclosure requirements of this subsection.

(C) At the request of the Director of the Federal Bureau of Investigation or the designee of the Director, any person making or intending to make a disclosure under subparagraph (A) or (C) of paragraph (1) shall identify to the Director or such designee the person to whom such disclosure will be made or to whom such disclosure was made prior to the request.

(e) A person who, in good faith, produces tangible things under an order pursuant to this section shall not be liable to any other person for such production. Such production shall not be deemed to constitute a waiver of any privilege in any other proceeding or context.

(f)(1) In this subsection—

(A) the term "production order" means an order to produce any tangible thing under this section; and

(B) the term "nondisclosure order" means an order imposed under subsection (d) of this section.

(2)(A)(i) A person receiving a production order may challenge the legality of that order by filing a petition with the pool established by section 1803(e)(1) of this title. Not less than 1 year after the date of the issuance of the production order, the recipient of a production order may challenge the nondisclosure order imposed in connection with such production order by filing a petition to modify or set aside such nondisclosure order, consistent with the requirements of subparagraph (C), with the pool established by section 1803(e)(1) of this title.

(ii) The presiding judge shall immediately assign a petition under clause (i) to 1 of the judges serving in the pool established by section 1803(e)(1) of this title. Not later than 72 hours after the assignment of such petition, the assigned judge shall conduct an initial review of the petition. If the assigned judge determines that the petition is frivolous, the assigned judge shall immediately deny the petition and affirm the production order or nondisclosure order. If the assigned judge determines the petition is not frivolous, the assigned judge shall

promptly consider the petition in accordance with the procedures established under section 1803(e)(2) of this title.

(iii) The assigned judge shall promptly provide a written statement for the record of the reasons for any determination under this subsection. Upon the request of the Government, any order setting aside a nondisclosure order shall be stayed pending review pursuant to paragraph (3).

(B) A judge considering a petition to modify or set aside a production order may grant such petition only if the judge finds that such order does not meet the requirements of this section or is otherwise unlawful. If the judge does not modify or set aside the production order, the judge shall immediately affirm such order, and order the recipient to comply therewith.

(C)(i) A judge considering a petition to modify or set aside a nondisclosure order may grant such petition only if the judge finds that there is no reason to believe that disclosure may endanger the national security of the United States, interfere with a criminal, counterterrorism, or counterintelligence investigation, interfere with diplomatic relations, or endanger the life or physical safety of any person.

(ii) If, upon filing of such a petition, the Attorney General, Deputy Attorney General, an Assistant Attorney General, or the Director of

the Federal Bureau of Investigation certifies that disclosure may endanger the national security of the United States or interfere with diplomatic relations, such certification shall be treated as conclusive, unless the judge finds that the certification was made in bad faith.

(iii) If the judge denies a petition to modify or set aside a nondisclosure order, the recipient of such order shall be precluded for a period of 1 year from filing another such petition with respect to such nondisclosure order.

(D) Any production or nondisclosure order not explicitly modified or set aside consistent with this subsection shall remain in full effect.

(3) A petition for review of a decision under paragraph (2) to affirm, modify, or set aside an order by the Government or any person receiving such order shall be made to the court of review established under section 1803(b) of this title, which shall have jurisdiction to consider such petitions. The court of review shall provide for the record a written statement of the reasons for its decision and, on petition by the Government or any person receiving such order for writ of certiorari, the record shall be transmitted under seal to the Supreme Court of the United States, which shall have jurisdiction to review such decision.

(4) Judicial proceedings under this subsection shall be concluded as expeditiously as possible. The record of proceedings, including petitions filed, orders granted, and statements of reasons for decision, shall be maintained under security measures established by the Chief Justice of the United States, in consultation with the Attorney General and the Director of National Intelligence.

(5) All petitions under this subsection shall be filed under seal. In any proceedings under this subsection, the court shall, upon request of the Government, review ex parte and in camera any Government submission, or portions thereof, which may include classified information.

(g) Minimization procedures

(1) In general

Not later than 180 days after March 9, 2006, the Attorney General shall adopt specific minimization procedures governing the retention and dissemination by the Federal Bureau of Investigation of any tangible things, or information therein, received by the Federal Bureau of Investigation in response to an order under this subchapter.

(2) Defined

In this section, the term "minimization procedures" means—

(A) specific procedures that are reasonably designed in light of the purpose and technique of an order for the production of tangible things, to minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 1801(e)(1) of this title, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand foreign intelligence information or assess its importance; and

(C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes.

(h) Use of information

Information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this subchapter concerning any United States person may be used and disclosed by Federal officers and employees

without the consent of the United States person only in accordance with the minimization procedures adopted pursuant to subsection (g) of this section. No otherwise privileged information acquired from tangible things received by the Federal Bureau of Investigation in accordance with the provisions of this subchapter shall lose its privileged character. No information acquired from tangible things received by the Federal Bureau of Investigation in response to an order under this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.