[ORAL ARGUMENT SCHEDULED FOR NOVEMBER 4, 2014]

Nos. 14-5004, 14-5005, 14-5016, 14-5017

IN THE UNITED STATES COURT OF APPEALS
FOR THE DISTRICT OF COLUMBIA CIRCUIT

LARRY ELLIOTT KLAYMAN et al.,

Appellees/Cross-Appellants,

v.

BARACK HUSSEIN OBAMA et al.,

Appellants/Cross-Appellees.

ON APPEAL FROM THE UNITED STATES DISTRICT
COURT FOR THE DISTRICT OF COLUMBIA

RESPONSE AND REPLY BRIEF FOR GOVERNMENT APPELLANTS/CROSS-APPELLEES

JOYCE R. BRANDA
Acting Assistant Attorney General

RONALD C. MACHEN JR.
United States Attorney

DOUGLAS N. LETTER
H. THOMAS BYRON III
HENRY C. WHITAKER
(202) 514-3180
Attorneys, Appellate Staff
Civil Division, Room 7256
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page**

* Authorities upon which we chiefly rely are marked with asterisks.

Constitution

Statutes

Rule

GLOSSARY

App.	Appendix
Add.	Addendum to Government Appellants' Opening Brief

INTRODUCTION

All three branches of government have authorized the operation of a bulk telephony-metadata program under Section 215 of the USA PATRIOT Act. Under this counter-terrorism program, the government acquires from certain telecommunications companies, in bulk, business records that contain telephony metadata reflecting the time, duration, dialing and receiving numbers, and other information about telephone calls, but that do not identify the individuals involved in, or the content of, the calls. Gov't Br. 10-14. Every federal court that has decided the question, other than the district court below, has concluded that this Section 215 program does not violate the Fourth Amendment for the reasons explained by the Supreme Court 35 years ago in *Smith* v. *Maryland*, 442 U.S. 735 (1979). Gov't Br. 44-45.

Plaintiffs defend the district court's decision to enjoin the program as unconstitutional, but concede that the government "may conduct surveillance on persons where there is reasonable suspicion that they are in communication with terrorists or committing crimes." Pl. Br. 1. But that is what the program does. Under the program, the government does not indiscriminately "access[] telephony metadata . . .

of hundreds of millions of Americans," *id.*—the only metadata that is reviewed is the tiny fraction that is within one or two steps of contact of records concerning individuals who are reasonably suspected of association with terrorist activity. *See* Gov't Br. 14-16. For the same reason, the program does not involve generating "intimate portraits of the lives of millions of Americans." EFF Amicus Br. 2. Instead, the government analyzes the tiny fraction of metadata that is reviewed to make connections between persons suspected of association with terrorist organizations and others, which contributes valuable information to counter-terrorism investigations. Understood as it is—rather than as the caricature portrayed by plaintiffs, their amici, and the district court—the Section 215 program, at most, minimally intrudes on constitutional privacy rights and serves the paramount government interest of combating terrorism. The district court's injunction should be reversed.

SUMMARY OF ARGUMENT

I. THE DISTRICT COURT'S PRELIMINARY INJUNCTION SHOULD BE REVERSED.

Plaintiffs have failed to establish that the district court's preliminary injunction of the Section 215 bulk telephony-metadata program was proper.

A. The government's opening brief explained that plaintiffs lack standing because they have not shown that the government has obtained any information about their communications under the program. In response, plaintiffs offer only unsupported speculation that metadata about their calls must have been provided to the government by the telecommunications companies because the government has acknowledged that the program is broad in scope. That argument fails to satisfy plaintiffs' established burden to provide evidence that they have suffered injury before they may seek to enjoin an important government anti-terrorism program.

Plaintiffs also have not demonstrated that their alleged injury—that the government might learn confidential information about their activities—has occurred even if metadata about their calls has been acquired under the Section 215 program (which again there is no

evidence of). Plaintiffs do not dispute that it is entirely speculative whether any metadata about their calls would ever be reviewed by a human being, and do not explain how inert metadata—stored in a database and not reviewed or analyzed by any government personnel—could create their asserted injury.

B. Plaintiffs err in defending the district court's conclusion that they are likely to succeed in their contention that the Section 215 program violates the Fourth Amendment. Plaintiffs in essence ask this Court to disregard *Smith* v. *Maryland*, 442 U.S. 735 (1979), which holds that individuals lack a Fourth Amendment privacy interest in telephony metadata provided to telecommunications companies by subscribers. The same kind of information is at issue here. Contrary to plaintiffs' contentions, the force and controlling precedential effect of *Smith* has not been altered by changes in technology or the Supreme Court's decision in *Riley* v. *California*, 134 S. Ct. 2473 (2014), which involved unrestricted police inspection of private information on cellular telephones incident to arrests. This case, by contrast, involves the acquisition of business records of telecommunications companies containing metadata that individuals have conveyed to those

companies, which are accessible to government personnel only under highly restricted, judicially supervised conditions.

Plaintiffs also cannot overcome the conclusion that, even if the program could be viewed as effecting a Fourth Amendment search, it would be permissible under the "special needs" doctrine. They agree that the prevention of terrorist attacks is a governmental need of overriding and compelling importance. But plaintiffs repeat the error of the district court in demanding that the government produce evidence that the program is responsible for preventing specified terrorist attacks. There is no such requirement. Nor is there any basis for plaintiffs' (and the district court's) efforts to substitute their judgment for the judgment of government officials that the Section 215 program contributes meaningfully to efforts to counter the continuing terrorist threat. That contribution, when coupled with the program's carefully crafted safeguards providing for significant judicial involvement and oversight, and minimizing any intrusion on legitimate privacy interests, makes the program reasonable under the Fourth Amendment.

II. THERE IS NO BASIS FOR BROADENING THE DISTRICT COURT'S INJUNCTION.

In their cross-appeal, plaintiffs seek to broaden the district court's injunction by reviving their challenge to government anti-terrorism programs that involve the acquisition of content and Internet metadata.

Plaintiffs lack standing to assert that challenge. Plaintiffs' claims appear to concern Section 702 of the Foreign Intelligence Surveillance Act, which involves surveillance targeted at non-U.S. persons located outside the United States. The district court correctly concluded that plaintiffs lack standing under the Supreme Court's decision in *Clapper* v. *Amnesty International USA*, 133 S. Ct. 1138 (2013), to mount such a challenge because plaintiffs can only speculate whether any of their communications has ever been targeted or acquired under Section 702.

Plaintiffs also lack standing to challenge the bulk acquisition of Internet metadata records under Section 402 of the Foreign Intelligence Surveillance Act. That program ended in 2011, years before plaintiff filed this lawsuit, and the bulk data acquired under it was destroyed. Plaintiffs do not have a right to injunctive relief against a program that does not exist.

ARGUMENT

I. THE DISTRICT COURT ERRED IN ENTERING A PRELIMINARY INJUNCTION AGAINST THE SECTION 215 BULK TELEPHONY-METADATA PROGRAM.

A. Plaintiffs Lack Standing To Challenge The Program.

The government's opening brief demonstrated that plaintiffs lack standing because they have provided no evidence, although it is their burden to do so, that the government has ever under the Section 215 program acquired business records containing telephony metadata about their calls. Gov't Br. 38-39.

In response, plaintiffs repeat the district court's logic that they have standing because some of them are subscribers of Verizon Wireless cellular telephone service. Pl. Br. 26-28. But plaintiffs make no effort to remedy the defect in that assertion—there is no evidence that the government has collected telephony metadata from Verizon Wireless. *See* Gov't Br. 38-39. Plaintiffs note that the government has acknowledged that "for several months in 2013" it acquired metadata from "Verizon Business Network Services," Pl. Br. 27, but plaintiffs do

not dispute that Verizon Business Network Services is not the same business entity as Verizon Wireless.[1]

Plaintiffs' claim to standing thus stands or falls on the strength of their (and the district court's) speculation that the government must have acquired metadata from Verizon Wireless because the Section 215 program "creates a historical repository that permits retrospective analysis of terrorist-related communications *across multiple telecommunications networks*." Pl. Br. 28. The conclusion does not follow from the premise. That the program is broad does not mean it is—or need be to serve what plaintiffs perceive to be its "function," Pl. Br. 28—all encompassing. And as a matter of fact, the program has never encompassed all, or even virtually all, call records and does not do so today. *See* Add. 101. There is no evidence that Verizon Wireless

[1] Plaintiffs point to a district court decision concluding that the plaintiffs in *ACLU* v. *Clapper* had alleged standing to challenge the Section 215 bulk telephony-metadata program. Pl. Br. 28-29. The plaintiffs in that case, however, alleged they were subscribers of Verizon Business Network Services. *See* Compl. at ¶ 28, *ACLU* v. *Clapper*, Doc. 1, No. 1:13cv3994 (S.D.N.Y. June 11, 2013). The government did not contend in *ACLU* that the plaintiffs lacked standing based on a lack of evidence about whether those plaintiffs' call records had been acquired under the Section 215 program (though the government did dispute standing on other grounds).

participates in the program—indeed, there is no evidence about the identity of any carrier beyond the fact that Verizon Business Network Services participated for a few months last year.

Plaintiffs complain that they have been unable to establish their standing only because the identities of the carriers that participate in the Section 215 program are classified. Pl. Br. 24-25. But it is plaintiffs' burden to demonstrate standing to sue. *See, e.g.*, *Lujan* v. *Defenders of Wildlife*, 504 U.S. 555, 561 (1992). The Supreme Court made clear in *Clapper* v. *Amnesty International USA*, 133 S. Ct. 1138, 1149 n.4 (2013), that plaintiffs' burden is not eliminated where the government continues to preserve the secrecy of highly sensitive and classified information concerning an intelligence-gathering anti-terrorism program.

The government's opening brief also demonstrated that plaintiffs lack standing for another reason. Plaintiffs assert that the government may learn confidential information about them and "use" that information against them in some unspecified way, App. 100, but that injury could arise only if government analysts actually were to review metadata about plaintiffs' calls, Gov't Br. 39-44.

Plaintiffs do not dispute that the prospect of any government analyst reviewing such metadata is entirely speculative, given that metadata under the program may be accessed only under the highly restricted querying process. *See* Gov't Br. 14-16, 40. Instead, plaintiffs assert that they suffer a cognizable injury from the government's mere possession of metadata that may languish unreviewed in the government's possession. Pl. Br. 30-32. Those conclusory assertions are divorced from the claims to injury that appear in plaintiffs' pleadings, which rest not on the mere presence of inert metadata sitting in a government database, but rather on the anxiety that plaintiffs purport to experience from the prospect that a human being might learn something personal about them from metadata about their calls. *See* App. 100, 102-04. That could happen only if metadata about plaintiffs' calls is responsive to a query. And that prospect is speculative.

Plaintiffs claim to suffer an injury whenever the government conducts a query of the metadata, even if metadata about their calls is never responsive to a query. Pl. Br. 30-31. But the querying process, contrary to plaintiffs' assertions, is not like a government official peering into a person's luggage, or scanning a home using a thermal

imager. Pl. Br. 32. In those instances, government personnel are actually reviewing private information about individuals' homes and personal effects. Here, by contrast, a person reviews only metadata that is responsive to a query; no person reviews nonresponsive information. The better comparison is to a dog sniff, which, as the Supreme Court has made clear, does not invade a protected Fourth Amendment interest simply because government personnel use it to rule out particular items as nonresponsive to an investigation. *See, e.g.*, *United States* v. *Place*, 462 U.S. 696, 707 (1983); *see also Illinois* v. *Caballes*, 543 U.S. 405, 409 (2005); *United States* v. *Jacobson*, 466 U.S. 109, 123-24 (1984). So too here, there is no invasion of a legally cognizable privacy interest merely because the government may run queries that rule out metadata about plaintiffs' calls as responsive (assuming *arguendo* the government acquired any under the program in the first place).

B. Plaintiffs Are Not Likely To Succeed On Their Claim That The Section 215 Program Violates The Fourth Amendment.

1. Plaintiffs Have No Fourth Amendment Privacy Interest In Business Records Containing Telephony Metadata.

The government's opening brief showed that the Fourth Amendment issue in this case is squarely controlled by *Smith* v. *Maryland*, 442 U.S. 735 (1979). *Smith* holds that an individual has no Fourth Amendment privacy interest in telephony metadata voluntarily conveyed by an individual to a telecommunications provider. *Id.* at 743-44. And every court that has decided the matter, other than the district court below, has agreed with that reading of *Smith*, which compels reversal of the district court's injunction. Gov't Br. 44-45.

The government's opening brief explained why the district court's efforts to distinguish *Smith* from this case do not succeed. Gov't Br. 48-60. Instead of engaging with the government's analysis, plaintiffs, joined by amicus curiae Electronic Frontier Foundation, do little more than repeat the district court's flawed reasoning. Pl. Br. 38-45; EFF Amicus Br. 16-20.

Like the district court, plaintiffs and their amicus principally seize on the fact that under the Section 215 program, as compared to the pen register at issue in *Smith*, the government acquires a larger scope of business records containing telephony metadata, and retains them over a longer period of time. Pl. Br. 41-44; EFF Amicus Br. 18-19. The government's opening brief explained, however, that those distinctions make no difference: *Smith* held that individuals lack a privacy interest in *any* of the telephony metadata voluntarily transmitted to a telephone company because they "voluntarily convey[] those numbers to the telephone company" and because "'a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'" *California* v. *Greenwood*, 486 U.S. 35, 41 (1988) (quoting *Smith*, 442 U.S. at 743-44). *See* Gov't Br. 48-53. That expectation does not become legitimate simply because telephone use is more pervasive now than it was in 1979, Pl. Br. 37-39; *see* EFF Amicus Br. 18-19, or because the Section 215 program collects additional forms of telephony metadata than were specifically at issue in *Smith*, *see* EFF Amicus Br. 19. As the Foreign Intelligence Surveillance Court has explained, the greater volume of call records at issue here is of no constitutional

moment because Fourth Amendment rights are personal in nature. *See* Add. 86 (citing *Rakas* v. *Illinois*, 439 U.S. 128, 133-34 (1978)); App. 136-37 (same); *see also United States* v. *Dionisio*, 410 U.S. 1, 13 (1973) ("It does not follow that each witness may resist a subpoena on the ground that too many witnesses have been called.") Indeed, if anything, the manner in which the Section 215 program acquires telephony metadata is less intrusive than was true in *Smith*, in which telephony metadata about a particular, known individual was acquired using a pen register (rather than from the company's business records) and used to arrest and prosecute him, and in which there were no restrictions whatsoever on what the police could do with the information it acquired. *See* 442 U.S. at 737, 741-42.

Plaintiffs, and amicus with even greater insistence, also object that the telephony metadata acquired and used in the Section 215 program could reveal information about an individual. Pl. Br. 43; EFF Amicus Br. 3-14. As explained above, however, it is entirely speculative whether the Section 215 program has "revealed" anything about *plaintiffs*, because there is no indication that metadata about their calls, even if the government acquired that information, has been

among the tiny fraction of metadata reviewed by government personnel after querying. That alone means that no Fourth Amendment "search" demonstrably happened here, and plaintiffs cannot assert the Fourth Amendment privacy interests of others. *See, e.g.*, *Minnesota* v. *Carter*, 525 U.S. 83, 88 (1998); *Place*, 462 U.S. at 707.

In any event, it is true enough, but beside the point, that telephony metadata could be revealing—indeed, the Section 215 program is important precisely because targeted and limited queries of telephony metadata collected in bulk shed light on connections between individuals suspected of association with terrorism and other known and unknown persons. But other business records also can reveal personal information: records of dialed telephone numbers can prove that an individual has been making obscene and harassing phone calls, *see Smith*, 442 U.S. at 737, and checks, deposit slips, and other customer bank records can show significant commercial and personal transactions, *see United States* v. *Miller*, 425 U.S. 435, 442-44 (1976). Similarly, confessions made to a government informant can provide important information about criminal activity. *See Lopez* v. *United States*, 373 U.S. 427, 438 (1963). Yet there is no Fourth Amendment

privacy interest in any such information when conveyed voluntarily to a third party. Amicus believes the notion that the Fourth Amendment would permit acquisition of revealing metadata was "unimaginable when *Smith* was decided and certainly not considered by the Court" EFF Amicus Br. 19, but *Smith* reached its holding over dissents noting precisely that. *See Smith*, 442 U.S. at 747-48 (Stewart, J., dissenting); *id.* at 750 (Brennan, J., dissenting); *see also Miller*, 425 U.S. at 451 (Brennan, J., dissenting). The question is not whether metadata is revealing, but whether it is reasonable to expect that routing information about phone calls will be kept private, even after a customer conveys that information to a telephone company for incorporation into that company's business records and for use by that company to advance its own business purposes. Under *Smith*, the answer to that question is no.[2]

---

[2] *Smith* distinguished the lack of a reasonable expectation of privacy in telephony metadata conveyed to a telephone company from the expectation of privacy in "the *contents* of communications." 442 U.S. at 741 (emphasis the Court's). The same distinction between metadata and content underlies Supreme Court case law holding that observation of the contents of sealed mail is a search, but viewing the routing information on the outside of mail is not. *See United States* v. *Jacobsen*, 466 U.S. 109, 114 (1984); *Reporters Comm. for Freedom of the Press* v.

Continued on next page.

Plaintiffs' and amicus' heavy reliance on the potentially revealing nature of metadata is doubly misplaced given the strict and carefully crafted safeguards imposed by the Foreign Intelligence Surveillance Court. That court's orders permit analysis only of metadata that is within two steps of a selector for which there is reasonable, articulable suspicion (now founded on a prior judicial determination) of association with a terrorist organization. Add. 43-44, 48. Whatever concerns might be posed by a hypothetical government program that permitted the indiscriminate use of telephony metadata to "determine the membership, structure, or participants in organizations and movements like the NAACP, the Tea Party, or Occupy Wall Street," EFF Amicus Br. 10, are concerns that do not apply to the Section 215 program, which is far more limited.

In an attempt to avoid the controlling precedential effect of *Smith*, plaintiffs repeatedly claim that the Supreme Court "invalidate[d]" or "eliminated" *Smith* in its recent decision in *Riley* v. *California*, 134 S.

AT&T, 593 F.2d 1030, 1056-57 (D.C. Cir. 1978). Because the government does not acquire content under the Section 215 program, this case does not present the question whether the contents of communications voluntarily transmitted to third parties would be accompanied by a reasonable expectation of privacy.

Ct. 2473 (2014). Pl. Br. 2, 19, 34. Plaintiffs fundamentally misunderstand the basis and scope of *Riley*. As we explained, Gov't Br. 54-55 & n.17, *Riley* did not involve the question whether government action was a Fourth Amendment "search," which is the question in this case. The issue in *Riley* was whether police needed a warrant to search the data on a cell phone incident to arrest. *See* 134 S. Ct. at 2489-93. The Supreme Court could not have been more explicit that, because *Riley* involved "*searches* incident to an arrest," the case did "not implicate the question whether the collection or inspection of aggregated digital information amounts to a search under other circumstances." *Id.* at 2489 n.1 (emphasis the Court's). Far from "eliminating" *Smith*, the Court cited *Smith*, observing that it involved a different question. *Id.* at 2492.

The Supreme Court in *Riley* addressed questions raised by searches of cell-phone devices, but those concerns are not present in this case. The information subject to search in *Riley* went far beyond metadata and included sensitive content, such as photographs, voicemails, and text messages—a veritable "cache of sensitive personal information" that is private. 134 S. Ct. at 2490. The telephony

metadata at issue here, by contrast, contains no content; has been voluntarily disclosed by subscribers to their telephone companies, and then integrated into those companies' business records; and may be used or analyzed only under carefully restricted and judicially supervised circumstances. This case does not implicate the privacy concerns raised by a search of the contents of a cell phone incident to an arrest.

Amicus Electronic Frontier Foundation makes much of *United States* v. *Jones*, 132 S. Ct. 945 (2012), and *United States* v. *Maynard*, 615 F.3d 544 (D.C. Cir. 2010), *aff'd on other grounds sub nom. Jones*, 132 S. Ct. at 945. EFF Amicus Br. 22-25. *Jones* and *Maynard* held, for different reasons, that long-term GPS monitoring may infringe a Fourth Amendment privacy interest. *Jones* did so, however, only on the ground that placement of a tracking device on a car infringes a property interest. *See* 132 S. Ct. at 950-53. That reasoning cuts against plaintiffs here, because business records containing telephony metadata are the property of telecommunications providers, not their subscribers. *See also Miller*, 425 U.S. at 440 (rejecting customers' privacy interest in bank records because "these are the business records of the banks").

This Court's decision in *Maynard*, and a concurring opinion in *Jones,* advanced a different rationale for the holding of *Jones*: long-term GPS monitoring raises privacy concerns because it enables the government to aggregate private details of an individual's life in a way that "a stranger" observing those movements could not. *Maynard*, 615 F.3d at 560; *Jones*, 132 S. Ct. at 955-56 (Sotomayor, J., concurring). The government's opening brief explained (at 59), however, that this Court's decision in *Maynard* recognized that the same logic does not apply to telephony metadata. Unlike location information acquired and aggregated by GPS monitoring, telephony metadata is conveyed by subscribers to telecommunications companies, which then retain that information and incorporate it into their business records. *See* 615 F.3d at 561 (citing *Smith*, 442 U.S. at 742-43). And unlike the GPS information discussed in *Jones*, the telephony metadata at issue here can be used only under the carefully restricted and judicially supervised querying process, and the vast bulk of the information is never even seen by a person.[3]

[3] The Electronic Frontier Foundation (Amicus Br. at 22) cites the Eleventh Circuit's opinion in *United States* v. *Davis*, 754 F.3d 1205

Continued on next page.

Justice Alito's concurring opinion in *Jones*, in noting the difficulties and ambiguities of appropriately defining privacy protections in the Digital Age, observed that "[a] legislative body is well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way." 132 S. Ct. at 964. The Section 215 program, which the Foreign Intelligence Surveillance Court has repeatedly held is authorized by statute, and which Congress was aware of when it re-authorized Section 215 in 2009 and 2011, *see* App. 268-72, 279-84, reflects that kind of judgment. In authorizing the government to acquire telephony metadata in bulk in order to combat terrorism, Congress provided for supervision of the process by the Foreign Intelligence Surveillance Court, and was careful to require privacy protections through the imposition of minimization procedures on the government's use of the information. *See* 50 U.S.C. §§ 1861(b)(2), (c)(1), (g). The political branches continue to debate the

---

(11th Cir. 2014), which held that the collection of cell-site data can implicate a Fourth Amendment privacy interest. The Eleventh Circuit has since vacated that opinion upon granting rehearing en banc. *See* No. 12-12928, 2014 WL 4358411 (11th Cir. Sept. 4, 2014). Cell-site locational data is not among the telephony metadata acquired under the Section 215 program. App. 203.

best means of accomplishing the Section 215 program's goals, but the Court should not lightly conclude that this program infringes a Fourth Amendment privacy interest where Congress, under current law, has already balanced the relevant interests.

2. Any "Search" Effected By The Section 215 Program Is Reasonable.

The government's opening brief demonstrated that, if the Section 215 bulk telephony-metadata program infringes a Fourth Amendment privacy interest, the program is nevertheless constitutional. *See* U.S. Const. amend. IV; Gov't Br. 60-66. The Fourth Amendment's reasonableness standard requires balancing "the promotion of legitimate governmental interests against the degree to which [any search] intrudes upon an individual's privacy." *Maryland* v. *King*, 133 S. Ct. 1958, 1970 (2013) (citation and internal quotation marks omitted).

Plaintiffs appear to agree that the prevention of terrorist attacks is not only a special governmental need, but, indeed, also one of "the highest order of magnitude." Pl. Br. 48. But plaintiffs claim that the Section 215 program is an unconstitutional means of serving that paramount need because the government has not "describe[d] a single

instance" in which the program has "actually stopped an imminent attack" or "aided . . . in achieving any objective that was time-sensitive in nature." Pl. Br. 48. The Constitution plainly does not require an anti-terrorism program to have demonstrably prevented a specific terrorist attack to be reasonable. To protect the Nation, the government employs a range of counter-terrorism tools and investigative methods in concert, which often serve different functions in order to complement one another in the service of achieving the overarching goal of preventing attacks. Those tools rarely, however, operate in isolation, and nothing in the Fourth Amendment's special-needs jurisprudence requires a showing that any single program prevented a particular attack. The government, in any event, has provided examples in which the Section 215 program provided timely and valuable assistance to ongoing counter-terrorism investigations. *See* App. 229-30.

Nor is it a constitutional death-knell that plaintiffs perceive the Section 215 program's value to be "primarily focused on speed" and in providing an investigative tool that may be "*faster* than other investigative methods." Pl. Br. 48. Speed can of course be a critical

factor in counter-terrorism investigations. The relevant legal standard under the special-needs doctrine is not, as plaintiffs seem to think, whether the program is indispensable to counter-terrorism efforts. The standard is whether the program is at least a "reasonably effective means" of advancing the government's paramount interest in preventing terrorism. *Bd. of Educ.* v. *Earls*, 536 U.S. 822, 837 (2002). Plaintiffs do not address the declarations in the record establishing that the Section 215 bulk telephony-metadata program enhances the government's ability to uncover and monitor known and unknown terrorist operatives who could otherwise elude detection. App. 213-16, 229-30. The Fourth Amendment requires no more.

The Section 215 bulk telephony-metadata program serves critical governmental needs, and it does so with minimal, if any, intrusion on cognizable privacy interests. Gov't Br. 62-63. Again, plaintiffs can only speculate whether the program has resulted in review by a person of any telephony metadata containing information about plaintiffs' calls. That is a function of the fact that the program includes strictly limited conditions—set, supervised, and enforced by the Foreign Intelligence Surveillance Court—concerning how and when telephony metadata

may be accessed and disseminated. App. 205-09. The Supreme Court has repeatedly upheld special-needs searches given the presence of similar privacy safeguards. *See* Gov't Br. 63 (collecting cases). The Section 215 program is permissible on the same basis.

C. Plaintiffs Are Not Likely To Succeed On Their First Amendment Claim.

In their responsive brief, plaintiffs ask the Court, in the alternative, to hold that they are likely to succeed on their claim (not reached by the district court) that the Section 215 program violates their First Amendment constitutional rights. Pl. Br. 67-71.[4] That argument does not support the injunction entered below.

Burdens on First Amendment rights that are incidental to the enforcement of laws of general applicability are generally permissible. *See, e.g.*, *Cohen* v. *Cowles Media Co.*, 501 U.S. 663, 669 (1991). This Court has applied that principle in the context of government investigations, recognizing that investigations creating incidental burdens that are uncontaminated by any motive of suppressing

[4] A heading in plaintiffs' brief makes mention of a claim under the "Fifth Amendment," Pl. Br. 67, but plaintiffs do not develop that claim in their brief, which in any event would add nothing to plaintiffs' other constitutional claims. *See Albright* v. *Oliver*, 510 U.S. 266, 273 (1994).

expression are consistent with the First Amendment. *See Reporters Comm. for Freedom of the Press* v. *AT&T*, 593 F.2d 1030, 1051-53 (D.C. Cir. 1978). There is no indication that any burdens the Section 215 program places on association are anything but incidental, particularly given the program's carefully crafted privacy safeguards.

Plaintiffs err in comparing the Section 215 program to instances in which an organization was compelled to disclose its membership lists, or an individual was required to disclose the organizations to which he belongs. Pl. Br. 68-69. The Section 215 program does not compel plaintiffs to do anything. Even if telephony metadata about plaintiffs' calls has been produced to the government under the Section 215 program (which there is no evidence of), plaintiffs do not explain how the speculative prospect that their metadata might be returned in response to a query could reasonably affect their behavior in any legally significant way. And even were there any real prospect that information about plaintiffs' associational activities would come to the government's attention as a result of the Section 215 program, that consequence would be a function of plaintiffs' choice to disclose that information to their telecommunications provider in the first place.

D. No Statutory Claims Are Properly Before This Court.

In our opening brief, we explained that plaintiffs are not likely to succeed on the merits based on any assertion that the Section 215 bulk telephony-metadata program is unauthorized by statute, because plaintiffs have dropped their statutory claims from this case. Gov't Br. 25 n.10; *see* Minute Order, No. 13cv881 (July 30, 2014) (granting plaintiffs leave to file amended complaint asserting only constitutional claims). Plaintiffs do not dispute that assertion in their responsive brief, and appropriately do not urge affirmance of the district court's injunction on the basis of statutory claims they have abandoned. Plaintiffs also do not challenge the district court's holding that their earlier attempt to challenge the statutory basis for the Section 215 program is precluded by the comprehensive scheme of judicial review of Section 215 production orders established by Congress in the Foreign Intelligence Surveillance Court. *See* 957 F. Supp. 2d at 19-23.

Amicus Curiae Center for National Security Studies nonetheless challenges that ruling and contends as well—contrary to repeated rulings of the Foreign Intelligence Surveillance Court—that the program is unauthorized by statute. CNSS Amicus Br. 2-31. The only

basis it gives for saying that those arguments are properly before the Court is a footnote, in which it claims that the Court can address them because "a party's decision not to put a claim before the Court of Appeals does not prohibit the Court from considering the issue in order to abide by its duty to resolve the case on alternative statutory grounds where available." CNSS Amicus Br. 5 n.3. The problem, however, is not simply that plaintiffs have not raised statutory claims "before the Court of Appeals"; plaintiffs no longer are raising those claims in any aspect of the case. No alternative statutory grounds are therefore "available" to conclude that plaintiffs are likely to succeed on the merits.[5]

E. The District Court Abused Its Discretion In Balancing The Equities And Assessing The Public Interest When It Entered The Preliminary Injunction.

The government's opening brief showed that the district court gave inadequate consideration to the public interest and failed to

[5] The doctrine of constitutional avoidance is not a basis for the Court to address statutory claims that plaintiffs are not asserting. The classic statement of that doctrine makes clear that the prerequisite to avoiding a constitutional question is "if there is also present" in the case "some other ground upon which the case may be disposed of." *Ashwander* v. *Tenn. Valley Auth.*, 297 U.S. 288, 347 (1936) (Brandeis, J., concurring). There is no other ground here.

balance the equities correctly when it entered the preliminary injunction. Gov't Br. 66-67. The government explained that, even if plaintiffs have standing to sue, and even if plaintiffs have cognizable Fourth Amendment privacy interests in play here, those interests are minimal, especially given the remote likelihood that metadata about plaintiffs' calls has been, or would in the future ever be, reviewed by a human being. On the other side of the balance, the government and the public have a substantial interest in having the Section 215 bulk telephony-metadata program continue to advance the interest of preventing terrorist attacks on the Nation.

Plaintiffs declare that "the public has no interest in 'protecting' the Government from the burdens of complying with the Constitution." Pl. Br. 53. That assertion conflates the question whether plaintiffs are likely to succeed on the merits—only one of four factors it is plaintiffs' burden to establish in seeking a preliminary injunction—with whether the equities favor the extraordinary remedy of preliminary injunctive relief. *See Winter* v. *Natural Res. Def. Council*, 555 U.S. 7, 22 (2008); *see also Chaplaincy of Full Gospel Churches* v. *England*, 454 F.3d 290, 304 (D.C. Cir. 2006). Plaintiffs do not address the government's

showing that complying with a preliminary injunction would be technologically and practically difficult, would consume considerable resources, and could degrade the program's overall efficacy. App. 218. Plaintiffs also have no answer to the fact that the district court erred as a matter of law in ordering the government to destroy any records regarding plaintiffs and to refrain from collecting records regarding plaintiffs in the future, which is improper preliminary relief because it grants plaintiffs full relief on the merits that could not be corrected were the government to prevail on final judgment. *See Dorfmann* v. *Boozer*, 414 F.2d 1168, 1173 n.13 (D.C. Cir. 1969). The injunction should be reversed for this reason as well, wholly independent and apart from the fact that plaintiffs' constitutional claims fail.

II. THE DISTRICT COURT CORRECTLY DENIED PLAINTIFFS ADDITIONAL PRELIMINARY INJUNCTIVE RELIEF.

In their cross-appeal, plaintiffs urge this Court to reverse the district court's decision to deny plaintiffs even broader preliminary injunctive relief than the district court entered with regard to the Section 215 bulk telephony-metadata program.[6] Specifically, plaintiffs

[6] Plaintiffs claim that the district court should have extended its injunction of the Section 215 program to plaintiff Mary Ann Strange, in

Continued on next page.

claim that the district court should have entered a preliminary injunction not only against that program, but also against other government programs that, they assert, involve "internet data surveillance activity." Pl. Br. 55-56. The district court correctly concluded that plaintiffs lack standing to pursue that claim. *See* 957 F. Supp. 2d at 8 n.6.

A. Plaintiffs Lack Standing To Challenge The Acquisition Of Content.

Plaintiffs' claim that the government has acquired their "Internet [d]ata [c]ontent," Pl. Br. 66, is apparently a reference to the acquisition of information under Section 702 of the Foreign Intelligence Surveillance Act.

---

addition to plaintiffs Charles Strange and Larry Klayman, because she is a subscriber of Verizon Wireless. Pl. Br. 54-55. That is wrong not just for the reasons discussed above in the standing section of the brief, but also for the additional reason that plaintiffs have provided no evidence that Mary Ann Strange is a subscriber of Verizon Wireless. Charles Strange's affidavit states only that he, not Mary Ann Strange, is a subscriber of Verizon Wireless. App. 101. Plaintiffs cite a paragraph in their amended complaint alleging that Mary Ann Strange is also a Verizon Wireless subscriber, Pl. Br. 54-55, but a preliminary injunction must be supported by evidence and factual findings, not mere allegations in the complaint. *See* Fed. R. Civ. P. 52(a)(2); *England*, 454 F.3d at 304-05.

Section 702 permits the government to acquire foreign-intelligence information by targeting the communications of non-U.S. persons located outside the United States, and includes court-imposed minimization procedures designed to protect the privacy of any communications of U.S. persons that may be incidentally acquired in the course of targeting foreign persons. *See* 50 U.S.C. § 1881a; App. 254-55. Information acquired under Section 702 can include the content of communications as well as metadata. Collection under Section 702 is ongoing and continues today.

Plaintiffs lack standing to challenge surveillance under Section 702 under the Supreme Court's express holding in *Clapper* v. *Amnesty International USA*, 133 S. Ct. 1138 (2013). In *Amnesty International*, the Court held that the plaintiffs there lacked standing to mount a constitutional challenge to Section 702 absent any indication that the government had incidentally acquired their communications in the course of targeting non-U.S. persons abroad under that provision. *See id.* at 1148-50. As in *Amnesty International*, plaintiffs in this case have provided no evidence that their communications have been acquired under Section 702, App. 98-104, and they can only speculate whether

the government has ever targeted those communications or would do so in the imminent future.

B. Plaintiffs Lack Standing To Challenge The Former Bulk Internet Metadata Program.

Plaintiffs likewise lack standing to challenge the bulk collection of Internet metadata under a now-discontinued government program.

Plaintiffs' claim implicates a government program under which the government was authorized to collect Internet metadata (not content) in bulk—not as plaintiffs assert under "Section 215," Pl. Br. 55-56, but rather under Section 402 of the Foreign Intelligence Surveillance Act. *See* App. 270. Section 402 is the so-called "pen/trap" provision, which authorizes the Foreign Intelligence Surveillance Court to issue orders "approving the installation and use of a pen register or trap and trace device" in order to obtain information relevant to counter-terrorism investigations. 50 U.S.C. § 1842(a). The government explained, in a now-declassified letter that was provided to the Senate Select Committee on Intelligence in December 2011, that the program was terminated in 2011 for operational and resource reasons. *See* App. 275. After terminating the program, the government destroyed the remaining bulk Internet metadata in its possession. *See* Decl. of Teresa

H. Shea ¶ 34, *Jewel* v. *National Security Agency*, No. 4:08cv4373 (N.D. Cal.) (Mar. 17, 2014), *available at* http://www.dni.gov/files/documents/0505/NSA%20Shea%202014%20Declassified%20Jewel,%20First%20Unitarian%20Declaration.pdf.

Plaintiffs lack standing to challenge that program. Plaintiffs have provided no evidence that the government ever collected any metadata containing information about their Internet communications. *See* App. 98, 101. Although the government has disclosed that it once conducted bulk Internet collection under Section 402, it has not disclosed the program's scope, including the identity of the providers involved in the now-ceased program. Plaintiffs ignore this basic defect in claiming standing.

Plaintiffs dispute the district court's reasoning that they lack standing to challenge this program because the program was discontinued years ago. *See* Pl. Br. 55-66. Plaintiffs complain that the government has "offered no real proof that they discontinued" this program. Pl. Br. 56. Plaintiffs once again invert the burden of proof of showing standing, which is on them not the government. *E.g.*, *Amnesty Int'l*, 133 S. Ct. at 1149 n.4. In any event, the government has provided

the "proof" that plaintiffs demand. App. 275; *see also* Decl. of Teresa H. Shea ¶ 34, *Jewel* v. *National Security Agency*, No. 4:08cv4373 (N.D. Cal.) (filed Mar. 19, 2014), *available at* http://www.dni.gov/files/documents/0505/NSA%20Shea%202014%20Declassified%20Jewel,%20First%20Unitarian%20Declaration.pdf. Plaintiffs' speculation, Pl. Br. 57-61, that the government is lying about discontinuing that program is no basis for concluding that plaintiffs have suffered a constitutionally cognizable injury.

Plaintiffs invoke mootness cases holding that "'a defendant's voluntary cessation of a challenged practice does not deprive a federal court of its power to determine the legality of the practice.'" Pl. Br. 62-63 (quoting *Friends of the Earth* v. *Laidlaw Envt'l Servs., Inc.*, 528 U.S. 167, 189 (2000)). But the question here is whether plaintiffs had standing at the time the complaint was filed, not whether the case became moot thereafter, and they clearly did not. *See Laidlaw*, 528 U.S. at 190-92 (distinguishing standing and mootness). In any event, the "voluntary cessation" doctrine—which is designed to prevent a defendant from manipulatively avoiding litigation—is inapplicable where, as here, the alleged "cessation" occurred long before the suit was

filed. *See Clarke* v. *United States*, 915 F.2d 699, 705-06 (D.C. Cir. 1990) (en banc). Here, the government terminated the program some years ago for operational and resource reasons, not to avoid litigation.

CONCLUSION

The district court's preliminary injunction should be reversed.

Respectfully submitted,

JOYCE R. BRANDA
Acting Assistant Attorney General

RONALD C. MACHEN JR.
United States Attorney

DOUGLAS N. LETTER
H. THOMAS BYRON III

/s/ Henry C. Whitaker
HENRY C. WHITAKER
(202) 514-3180
Attorneys, Appellate Staff
Civil Division, Room 7256
U.S. Department of Justice
950 Pennsylvania Ave., N.W.
Washington, D.C. 20530

SEPTEMBER 2014

CERTIFICATE OF COMPLIANCE WITH FEDERAL RULE OF APPELLATE PROCEDURE 32(A)

I hereby certify that that this brief complies with the requirements of Federal Rule of Appellate Procedure 32(a)(5) and (6) because it has been prepared in 14-point Century Schoolbook, a proportionally spaced font.

I further certify that this brief complies with the type-volume limitation of Federal Rule of Appellate Procedure 32(a)(7)(B) because it contains 6,706 words excluding the parts of the brief exempted under Rule 32(a)(7)(B)(iii), according to the count of Microsoft Word.

/s/ Henry C. Whitaker
HENRY C. WHITAKER

CERTIFICATE OF SERVICE

I hereby certify that on September 19, 2014, I electronically filed the foregoing brief with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit by using the appellate CM/ECF system. I further certify that I will cause 8 paper copies of this brief to be filed with the Court within two business days.

/s/ Henry C. Whitaker
HENRY C. WHITAKER