United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued November 4, 2014 Decided August 28, 2015

No. 14-5004

BARACK HUSSEIN OBAMA, ET AL.,
APPELLANTS
v.

LARRY ELLIOTT KLAYMAN, ET AL.,
APPELLEES

Consolidated with 14-5005, 14-5016, 14-5017

Appeal from the United States District Court
for the District of Columbia
(No. 1:13-cv-851)
(No. 1:13-cv-881)

H. Thomas Byron, III, Attorney, U.S. Department of Justice, argued the cause for appellants/cross-appellees. With him on the briefs were Stuart F. Delery, Assistant Attorney General, *Ronald C. Machen, Jr.*, U.S. Attorney, and *Douglas N. Letter* and *Henry C. Whitaker*, Attorneys.

Larry E. Klayman argued the cause and filed the briefs for appellees/cross-appellants.

Cindy A. Cohn argued the cause for *amici curiae* Electronic Frontier Foundation, et al. On the brief were *Alex Abdo*, *Jameel Jaffer*, *Arthur B. Spitzer*, and *Mark Rumold*.

Paul M. Smith argued the cause for *amicus curiae* Center for National Security Studies. With him on the brief were *Kate A. Martin*, *Joseph Onek*, and *Michael Davidson*.

Before: BROWN, *Circuit Judge*, and WILLIAMS and SENTELLE, *Senior Circuit Judges*.

Opinion for the Court filed PER CURIAM.

Separate opinions filed by *Circuit Judge* BROWN and *Senior Circuit Judge* WILLIAMS.

Opinion dissenting in part filed by *Senior Circuit Judge* SENTELLE.

PER CURIAM: In the wake of the terrorist attacks of September 11, 2001, Congress enacted the USA PATRIOT Act. Pub. L. No. 107-56, 115 Stat. 272 (2001). Section 215 of that Act empowered the FBI to request, and the Foreign Intelligence Surveillance Court ("FISC") to enter, orders "requiring the production of any tangible things (including books, records, papers, documents, and other items) for an investigation . . . to protect against international terrorism." *Id.* at § 215, 115 Stat. at 291, codified as amended at 50 U.S.C. § 1861(a)(1). Since May 2006, the government has relied on this provision to operate a program that has come to be called "bulk data collection," namely, the collection, in bulk, of call records produced by telephone companies containing "telephony metadata"—the telephone numbers dialed (incoming and outgoing), times, and durations of calls. The FBI has periodically applied for, and the FISC has entered, orders instructing one or more telecommunications service providers to produce, on a daily basis over a period of ninety days, electronic copies of such data. Decl. of Robert J. Holley, Acting Assistant FBI Director, at ¶¶ 10-13, Joint Appendix 224-25.

Under the program, the collected metadata are consolidated into a government database, where (except in exigent circumstances) the NSA may access it only after demonstrating to the FISC a "reasonable articulable suspicion" that a particular phone number is associated with a foreign terrorist organization. Gov't's Br. at 11-12. Even then, the NSA may retrieve call detail records only for phone numbers in contact with the original number—within two steps, or "hops" of it. *Id.* at 11. If telephone number A was used to call telephone number B, which in turn was used to call telephone number C, and if the FISC affirms the government's "reasonable articulable suspicion" that A is associated with a foreign terrorist organization, the FISC may authorize the government to retrieve from the database the metadata associated with A, B, and C. (Before 2014, the FISC orders allowed the government to conduct queries for any number within *three* steps of the approved identifier, and the FISC did not play any role in assessing the government's "reasonable articulable suspicion" for each query. *Id.* at 12 n.3). Once the government has retrieved the metadata, which does not include the content of the calls or the identities of the callers, it uses the data "in conjunction with a range of analytical tools to ascertain contact information that may be of use in identifying individuals who may be associated with certain foreign terrorist organizations because they have been in communication with certain suspected-terrorist telephone numbers or other selectors." *Id.* at 9, 15.

Plaintiffs contend that this bulk collection constitutes an unlawful search under the Fourth Amendment; they seek injunctive and declaratory relief as well as damages. Third Amended Complaint ¶ 53, *Klayman v. Obama*, 13-cv-851 (D.D.C. Feb. 10, 2014), ECF No. 77. The district court issued a preliminary injunction barring the government from

collecting plaintiffs' call records, but stayed its order pending appeal. *Klayman v. Obama*, 957 F. Supp. 2d 1, 44-45 (2013).

The court reverses the judgment of the district court, and for the reasons stated in the opinions of Judge Brown and Judge Williams orders the case remanded to the district court. (Judge Sentelle dissents from the order of remand and would order the case dismissed.) The opinions of the judges appear below after a brief explanation of why the case is not moot.

* * *

Under a "sunset" clause, the section of the U.S. Code amended by Section 215 was scheduled to revert to its pre-2001 form on June 1, 2015 unless Congress acted. See Pub. L. No. 109-177, § 102(b)(1), 120 Stat. 192, 194-95 (2006); Pub. L. No. 112-14, § 2(a), 125 Stat. 216, 216 (2011). That date came and went without any legislative action. One day after the deadline, however, Congress enacted the USA Freedom Act, which revived the language added by Section 215 with some substantial changes. See Pub. L. No. 114-23, Tit. I, 129 Stat. 268, 269-77 (2015), codified at 50 U.S.C. § 1861. The Act's changes do not take effect until 180 days after the date of enactment (June 2, 2015). *Id.* § 109(a), 129 Stat. at 276. And the legislation provides for continuation of pre-existing authority until the effective date of the new legislation: "Nothing in this Act shall be construed to alter or eliminate the authority of the Government to obtain an order under title V of the Foreign Intelligence Surveillance Act of 1978 (50 U.S.C. 1861 et seq.) as in effect prior to the effective date . . . during the period ending on such effective date." *Id.* § 109(b), 129 Stat. at 276.

Cessation of a challenged practice moots a case only if "there is no reasonable expectation . . . that the alleged violation will recur." *Larsen v. U.S. Navy*, 525 F.3d 1, 4

(D.C. Cir. 2008) (quotations and citations omitted). Here, any lapse in bulk collection was temporary. Immediately after Congress acted on June 2 the FBI moved the FISC to recommence bulk collection, United States' Mem. of Law, *In re Application of the FBI*, No. BR 15-75 (FISC, filed Jun. 2, 2015), and the FISC confirmed that it views the new legislation as effectively reinstating Section 215 for 180 days, and as authorizing it to resume issuing bulk collection orders during that period. See Opinion and Order, *In re Application of the FBI*, Nos. BR 15-75, Misc. 15-01 (FISC June 29, 2015) (Mosman, J.); Mem. Op., *In re Applications of the FBI*, Nos. BR 15-77, BR 15-78 (FISC Jun. 17, 2015) (Saylor, J.). Accordingly, plaintiffs and the government stand in the same positions that they did before June 1, 2015.

* * *

The preliminary injunction entered by the district court is hereby vacated and the case remanded for such further proceedings as may be appropriate.

So ordered.

BROWN, *Circuit Judge*: I disagree with the district court's conclusion that plaintiffs have established a "substantial likelihood of success on the merits." *See, e.g.*, *Sottera, Inc. v. Food & Drug Admin.*, 627 F.3d 891, 893 (D.C. Cir. 2010). I write separately to emphasize that, while plaintiffs have demonstrated it is only *possible*—not substantially likely—that their own call records were collected as part of the bulk-telephony metadata program, plaintiffs have nonetheless met the bare requirements of standing. Accordingly, I join the court in vacating the preliminary injunction entered by the district court.

In order to establish his standing to sue, a plaintiff must show he has suffered a "concrete and particularized" injury. *Lujan v. Defenders of Wildlife*, 504 U.S.555, 560–61 (1992). In other words, plaintiffs here must show *their own* metadata was collected by the government. *See, e.g.*, *Clapper v. Amnesty International*, 133 S. Ct. 1138, 1148 (2013) ("[R]espondents fail to offer any evidence that their communications have been monitored under § 1881a, a failure that substantially undermines their standing theory."); *ACLU v. NSA*, 493 F.3d 644, 655 (6th Cir. 2007) ("If, for instance, a plaintiff could demonstrate that her privacy had actually been breached (i.e., that her communications had actually been wiretapped), then she would have standing to assert a Fourth Amendment cause of action for breach of privacy."); *Halkin v. Helms*, 690 F.2d 977, 999–1000 (D.C. Cir. 1982) ("[T]he absence of proof of actual acquisition of appellants' communications is fatal to their watchlisting claims.").

The record, as it stands in the very early stages of this litigation, leaves some doubt about whether plaintiffs' own metadata was ever collected. Plaintiffs' central allegation is that defendants "violated the Fourth Amendment to the U.S. Constitution when they unreasonably searched and seized and

continue to search Plaintiffs' phone records . . . without reasonable suspicion or probable cause." Third Amended Complaint at ¶ 53, *Klayman I*, 957 F. Supp. 2d 1. Plaintiffs have supported this claim with specific facts, notably: (1) The NSA operates a bulk telephony-metadata collection program; and (2) on April 25, 2013, the FISC issued an order requiring Verizon *Business Network Services* to produce its subscribers' call detail records to the NSA on a daily basis from April 25, 2013 to July 19, 2013. However, plaintiffs are Verizon *Wireless* subscribers and not Verizon *Business Network Services* subscribers. Thus, the facts marshaled by plaintiffs do not fully establish that their own metadata was ever collected.

In his opinion below, Judge Leon eloquently explains how these facts are nonetheless sufficient to draw the inference that "the NSA has collected and analyzed [plaintiffs'] telephony metadata and will continue to operate the program consistent with FISC opinions and orders." *Klayman v. Obama*, 957 F. Supp. 2d 1, 29 (D.D.C. 2013). In particular, Judge Leon infers from the government's efforts to "create a *comprehensive* metadata database" that "the NSA *must* have collected metadata from Verizon Wireless, the single largest wireless carrier in the United States, as well as AT&T and Sprint, the second[-] and third-largest carriers." *Id.* at 27.

As Judge Leon's opinion makes plain, plaintiffs have set forth significant evidence about the NSA's bulk-telephony metadata program. As a result, this case is readily distinguishable from cases like *Tooley v. Napolitano*, 586 F.3d 1006 (D.C. Cir. 2009), in which allegations of unlawful surveillance were dismissed as "patently insubstantial." *Id.* at 1009–10 (concluding that the governmental surveillance scheme described in plaintiff's allegations was "not

realistically distinguishable from allegations of little green men.").

This evidence also sets this case apart from *Clapper*. There, plaintiffs' claim of standing relied "on a highly attenuated chain of possibilities." 133 S. Ct. at 1148. One link of that chain was that plaintiffs' "theory necessarily rests on their assertion that the Government will target *other individuals*—namely, their foreign contacts."[1] *Id*. The *Clapper* plaintiffs, however, had "no actual knowledge of the Government's § 1881a targeting practices" nor could they even show that the surveillance program they were challenging even existed. *Id.* at 1148–49 ("Moreover, because § 1881a at most *authorizes*—but does not *mandate* or *direct*—the surveillance that respondents fear, respondents' allegations are necessarily conjectural."); *cf. United Presbyterian Church in the USA v. Reagan*, 738 F.2d 1375, 1380–81 (D.C. Cir. 1984) (dismissing a complaint as a "generalized grievance" against the "entire national intelligence-gathering system" where plaintiffs were unable to show the injury they suffered was the result of a specific government surveillance program.) By contrast, here, plaintiffs have set forth specific evidence showing that the government operates a bulk-telephony metadata program that collects subscriber information from domestic telecommunications providers, including Verizon Business Network Services. Contrary to the assertions of my colleagues, these facts bolster plaintiffs' position: where the *Clapper* plaintiffs relied on speculation and conjecture to press their claim, here, plaintiffs offer an inference derived

[1] The statute authorizing the surveillance program at issue in *Clapper*, 50 U.S.C. § 1881a, explicitly provided that, as U.S. persons, plaintiffs could not be targeted for surveillance. 133 S. Ct. at 1148.

from known facts. *See In re Application of the Federal Bureau of Investigation for an Order Requiring the Production of Tangible Things from Verizon Business Network Services, Inc. on behalf of MCI Communication Services, Inc. d/b/a Verizon Business Services*, No. BR-13-80 (Foreign Intelligence Surveillance Court, April 25, 2013), J.A. 250–53.[2]

However, the burden on plaintiffs seeking a preliminary injunction is high. Plaintiffs must establish a "substantial likelihood of success on the merits." *Sottera, Inc.*, 627 F.3d at 893. Although one could reasonably infer from the evidence presented the government collected plaintiffs' own metadata, one could also conclude the opposite. Having barely fulfilled the requirements for standing at this threshold stage, Plaintiffs fall short of meeting the higher burden of proof required for a preliminary injunction.

Judge Williams is right to remind us that any number of unexpected constraints may frustrate the effectiveness of a given program. Appropriations may fall short. Technicians may err. Legal challenges may stymie the most dedicated bureaucrats.[3] But while *post hoc* obstacles may undermine a program's efficacy, they do not alter its intended objective, which, here, remains (commonsensically) the comprehensive collection of telephonic metadata.

---

[2] Although originally classified "top secret," this order was declassified on July 11, 2013. The order expired on July 19, 2013.

[3] FISA provides that a "person receiving a production order may challenge the legality of [that order]…by filing a petition with the [FISC]." 50 U.S.C. § 1861 (f)(2)(A)(i). However, such petitions are filed under seal and may not be disclosed. *Id.* § 1861 (d)(1), (f)(2)(D)(4), (f)(2)(D)(5).

On remand it is for the district court to determine whether limited discovery to explore jurisdictional facts is appropriate. *See*, *e.g.*, *Natural Resources Defense Council v. Pena*, 147 F.3d 1012, 1024 (D.C. Cir. 1998). Of course, I recognize that, in order for additional discovery to be meaningful, one of the obstacles plaintiffs must surmount is the government's unwillingness to make public a *secret* program. *See United Presbyterian Church in the U.S.A.*, 738 F.2d at 1382; *cf. ACLU*, 493 F.3d at 655 ("In the present case, the plaintiffs concede that there is no single plaintiff who can show that he or she has actually been wiretapped. Moreover, due to the State Secrets Doctrine, the proof needed either to make or negate such a showing is privileged, and therefore withheld from discovery or disclosure."). It is entirely possible that, even if plaintiffs are granted discovery, the government may refuse to provide information (if any exists) that would further plaintiffs' case. Plaintiffs' claims may well founder in that event. But such is the nature of the government's privileged control over certain classes of information. Plaintiffs must realize that secrecy is yet another form of regulation, prescribing not "what the citizen may do" but instead "what the citizen may know." DANIEL P. MOYNIHAN, SECRECY: THE AMERICAN EXPERIENCE 59 (1999). Regulations of this sort may frustrate the inquisitive citizen but that does not make them illegal or illegitimate. Excessive secrecy limits needed criticism and debate. Effective secrecy ensures the perpetuation of our institutions. In any event, our opinions do not comment on the propriety of whatever privileges the government may have occasion to assert.

WILLIAMS, *Senior Circuit Judge*: "[A] party seeking a preliminary injunction must demonstrate, among other things, a likelihood of success on the merits." *Munaf v. Geren*, 553 U.S. 674, 690 (2008) (internal quotations and citations omitted); see also *Mills v. District of Columbia*, 571 F.3d 1304, 1308 (D.C. Cir. 2009) (requiring a "*substantial* likelihood of success on the merits") (emphasis added) (quotations and citations omitted). In this context, the "merits" on which plaintiff must show a likelihood of success encompass not only substantive theories but also establishment of jurisdiction. The "affirmative burden of showing a likelihood of success on the merits . . . necessarily includes a likelihood of the court's *reaching* the merits, which in turn depends on a likelihood that plaintiff has standing." *Nat'l Wildlife Fed'n v. Burford*, 835 F.2d 305, 328 (D.C. Cir. 1987) (Williams, J., concurring and dissenting). And to show standing, a plaintiff must demonstrate an "injury in fact" that is "actual or imminent, not conjectural or hypothetical." *Friends of the Earth, Inc. v. Laidlaw Envt'l Servs. (TOC), Inc.*, 528 U.S. 167, 180 (2000).

Plaintiffs claim to suffer injury from government collection of records from their telecommunications provider relating to their calls. But plaintiffs are subscribers of Verizon Wireless, not of Verizon Business Network Services, Inc.—the sole provider that the government has acknowledged targeting for bulk collection. Gov't's Br. at 38; Appellees' Br. at 26-28; see also Secondary Order, *In re Application of FBI*, No. BR 13-80 (FISC, Apr. 25, 2013) (Vinson, J.). Thus, unlike some others who have brought legal challenges to the bulk collection program, plaintiffs lack direct evidence that records involving their calls have actually been collected. Cf. *ACLU v. Clapper*, 785 F.3d 787, 801 (2d Cir. 2015) (finding that Verizon Business subscribers had standing to challenge the bulk collection program because "the government's own orders demonstrate that appellants'

call records are indeed among those collected as part of the telephone metadata program").

Plaintiffs' contention that the government is collecting data from Verizon Wireless (a contention that the government neither confirms nor denies, Gov't's Br. at 38-39), depends entirely on an inference from the existence of the bulk collection program itself. Such a program would be ineffective, they say, unless the government were collecting metadata from every large carrier such as Verizon Wireless; ergo it must be collecting such data. Appellee's Br. 27-28. This inference was also the district judge's sole basis for finding standing. *Klayman v. Obama*, 957 F. Supp. 2d 1, 27 & n.36 (2013).

Yet the government has consistently maintained that its collection "never encompassed all, or even virtually all, call records and does not do so today." Gov't's Br. at 39; Decl. of Teresa Shea, NSA Signals Intelligence Director at ¶ 8, Addendum to Gov't's Br. at 101 (similar). While one district judge has claimed that "the Government acknowledged that since May 2006, it has collected this information for substantially every telephone call in the United States," neither of his sources—an Administration "White Paper" and a declaration by an NSA official—actually supports the claim. *ACLU v. Clapper*, 959 F. Supp. 2d 724, 735 (S.D.N.Y. 2013), *vacated and remanded*, 785 F.3d 787 (2d Cir. 2015); see Administration White Paper, Bulk Collection of Telephony Metadata Under Section 215 of the USA Patriot Act at 3 (Aug. 9, 2013) ("FBI obtains orders from the FISC directing *certain* telecommunications service providers to produce business records that contain information about communications between telephone numbers . . ." (emphasis added)); Decl. Teresa Shea ¶ 14, *ACLU v. Clapper*, 13-cv-3994 (S.D.N.Y. Oct. 1, 2013), ECF No. 63 ("FBI obtains orders from the FISC directing *certain* telecommunications

service providers to produce all business records created by them (known as call detail records) that contain information about communications between telephone numbers" (emphasis added)).

I note the Second Circuit's observation that the government had not "seriously" disputed the contention that "all significant service providers" were subject to the bulk collection program. *ACLU*, 785 F.3d at 797. But in that case the government said, "Various details of the program remain classified, precluding further explanation here of its scope," and went on to insist that "the record does not support the conclusion that the program collects 'virtually all telephony metadata' about telephone calls made or received in the United States. Nor is that conclusion correct." See Appellees' Br. at 7, *ACLU v. Clapper*, No. 14-42 (2d Cir. filed Apr. 10, 2014) (citations omitted). Thus the government's assertions in the two cases are parallel. Of course the Second Circuit's comment was irrelevant to its conclusion, as the plaintiffs in that case were not subscribers of Verizon Wireless but of Verizon Business, whose data the government acknowledged collecting. See *ACLU*, 785 F.3d at 801.

It appears true, as plaintiffs and the district court suggest, that the effectiveness of the program expands with its coverage; every number that goes uncollected reduces the utility of the government's "two-hop" querying. Indeed, it may well be that a reduction in coverage of, say, 50% would diminish the effectiveness of the program by far more than that proportion. Yet, in the face of the government's representations that it has never collected "all, or even virtually all" call records, I find plaintiffs' claimed inference inadequate to demonstrate a "substantial likelihood" of injury.

Clapper v. Amnesty International, 133 S. Ct. 1138 (2013), represents the Supreme Court's most recent

evaluation of comparable inferences and cuts strongly against plaintiffs' claim that they have a substantial likelihood of prevailing as to standing. There, a group of US-based "attorneys and human rights, labor, legal, and media organizations" challenged the surveillance authorized by the FISA Amendments Act of 2008. *Id.* at 1145. The statute empowered the Attorney General and the Director of National Intelligence to jointly seek an order from the FISC authorizing "the targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information" for a period of up to one year. 50 U.S.C. § 1881a. Plaintiffs claimed they were injured by the surveillance because their work required them "to engage in sensitive and sometimes privileged telephone and e-mail communications with colleagues, clients, sources, and other individuals located abroad" and that "some of the people with whom they exchange foreign intelligence information [we]re likely targets of surveillance under § 1881a" because they communicate with "people the Government 'believes or believed to be associated with terrorist organizations,' 'people located in geographic areas that are a special focus' of the Government's counterterrorism or diplomatic efforts, and activists who oppose governments that are supported by the United States Government." 133 S. Ct. at 1145.

But as the Court observed, the *Clapper* plaintiffs had "no actual knowledge of the Government's § 1881a targeting practices" and accordingly "merely speculate[d] and ma[d]e assumptions about whether their communications with their foreign contacts will be acquired under § 1881a." *Id.* at 1148. The premises for their speculation were hardly trivial. They claimed (and it was not disputed) (1) that they engaged in communications eligible for surveillance under the disputed section, (2) that the government had a strong motive to intercept these particular communications because of the subject matter and identities involved, (3) that the government

had (under separate legal authority) already intercepted 10,000 phone calls and 20,000 emails involving one individual who is now in regular communication with one of the plaintiffs, and (4) that the government had the capacity to intercept these communications. *Id.* at 1157-59. The Court held that these allegations left it merely "speculative whether the Government w[ould] imminently target communications to which respondents [we]re parties," and so provided an inadequate basis for standing. *Id*. at 1148-49 (citations and some quotations omitted).

Here, the plaintiffs' case for standing is similar to that rejected in *Clapper*. They offer nothing parallel to the *Clapper* plaintiffs' evidence that the government had *previously* targeted them or someone they were communicating with (No. 3 above). And their assertion that NSA's collection must be comprehensive in order for the program to be most effective is no stronger than the *Clapper* plaintiffs' assertions regarding the government's motive and capacity to target their communications (Nos. 2 & 4 above).

The strength of plaintiffs' inference from the government's interest in having an effective program rests on an assumption that the NSA prioritizes effectiveness over all other values. In fact, there are various competing interests that may constrain the government's pursuit of effective surveillance. Plaintiffs' inference fails to account for the possibility that legal constraints, technical challenges, budget limitations, or other interests prevented NSA from collecting metadata from Verizon Wireless. Many government programs (even ones associated with national defense) seem to be calibrated or constrained by collateral concerns not directly related to the program's stated objectives, such as funding deficiencies, bureaucratic inertia, poor leadership, and diversion to non-defense interests of resources nominally dedicated to defense. It is possible that such factors have

operated to hamper the breadth of the NSA's collection. In fact, both the district court and the plaintiffs contradict their own assertions about the effectiveness of the program by emphatically asserting its ineffectiveness in support of their conclusions that it violates the Fourth Amendment. See *Klayman*, 957 F. Supp. 2d at 40-41 ("I have serious doubts about the efficacy of the metadata collection program . . . ."); Appellees' Br. at 47-49; Appellees' Reply at 30-33.

Judge Brown distinguishes *Clapper* on the grounds that the plaintiffs here have offered "specific evidence" about the government's bulk collection program. Op. of Brown, J., at 3. But, assuming their evidence to be in some sense more specific, the relevant inquiry is whether that evidence indicates that the program targets plaintiffs. As to that, the plaintiffs here do no better than those in *Clapper*.

Plaintiffs complain that the government should not be allowed to avoid liability simply by keeping the material classified. But the government's silence regarding the scope of bulk collection is a feature of the program, not a bug. The *Clapper* Court rejected a request for "in camera" review of classified government materials precisely on the ground that any such approach would tend to undermine the program's effectiveness:

> As an initial matter, it is *respondents'* burden to prove their standing by pointing to specific facts, not the Government's burden to disprove standing by revealing details of its surveillance priorities. Moreover, this type of hypothetical disclosure proceeding would allow a terrorist (or his attorney) to determine whether he is currently under U.S. surveillance simply by filing a lawsuit challenging the Government's surveillance program. Even if the terrorist's attorney were to comply with a

> protective order prohibiting him from sharing the Government's disclosures with his client, the court's postdisclosure decision about whether to dismiss the suit for lack of standing would surely signal to the terrorist whether his name was on the list of surveillance targets.

133 S. Ct. at 1149 n.4 (citations omitted). These considerations apply with equal force here, where the government has sought to maintain a similarly strategic silence regarding the scope of its bulk collection.

It is true that *Clapper* came to the Court on review of cross-motions for summary judgment, not a preliminary injunction, but the Court's rejection of the *Clapper* plaintiffs' claims is nonetheless telling. Those plaintiffs actually faced a *lighter* burden than do ours: in granting the government's motion for summary judgment, the Court necessarily found that plaintiffs' inferences were inadequate even to preserve the *question* of standing as a "genuine issue." See *Amnesty Int'l USA v. McConnell*, 646 F. Supp. 2d 633, 641 (S.D.N.Y. 2009) (quoting Fed. R. Civ. P. 56(c)), *vacated and remanded sub nom. Amnesty Int'l USA v. Clapper*, 638 F.3d 118 (2d Cir. 2011), *rev'd*, 133 S. Ct. 1138 (2013). Here, by contrast, plaintiffs must show a "substantial likelihood" of standing.

Accordingly, I find that plaintiffs have failed to demonstrate a "substantial likelihood" that the government is collecting from Verizon Wireless or that they are otherwise suffering any cognizable injury. They thus cannot meet their burden to show a "likelihood of success on the merits" and are not entitled to a preliminary injunction.

It remains possible that on remand plaintiffs will be able to collect evidence that would establish standing. Indeed, noting that the government was "uniquely in control of the facts, information, documents, and evidence regarding the

extent and nature of their mass surveillance," they moved in the district court to depose "an employee of the NSA." Pls.' Mot. For Leave, *Klayman v. Obama*, 13-cv-851 (D.D.C. Oct. 30, 2013), ECF No. 15. But the district judge denied the motion as moot after granting the preliminary injunction. Minute Order, *Klayman v. Obama*, 13-cv-851 (D.D.C. Jan. 21, 2014). Given the possibility that plaintiffs' efforts along these lines may be fruitful, I join Judge Brown in remanding to the district court for it to decide whether limited discovery to explore jurisdictional facts is appropriate.

I am uncertain about the meaning of Judge Brown's view that although plaintiffs have failed to show a substantial likelihood of success on standing, they have nonetheless "fulfilled the requirements for standing," if only "barely." Op. of Brown, J., at 4. If the latter "fulfill[ment]" means simply that standing cannot be ruled out and thus poses no jurisdictional obstacle to discovery on standing, I agree. To the extent that Judge Brown regards the "burden of proof required for a preliminary injunction" as "higher," *id*., I don't understand in what sense the burden would be higher than in other contexts (motions for judgment on the pleadings, for summary judgment, or after hearing), or the basis for regarding it as higher than in those contexts.

SENTELLE, *Senior Circuit Judge*, dissenting in part: I will not restate either the facts or the background law, as I fully agree with my colleagues' statements on those subjects. Indeed, I agree with virtually everything in Judge Williams' opinion, save for its conclusion, and I even agree with part of that. My colleagues believe that the preliminary injunction entered by the district court must be vacated, as plaintiffs have failed to establish a "substantial likelihood of success on the merits." Brown Op. 1; Williams Op. 3. I agree. However, my colleagues also believe that the case should be remanded for further proceedings. I do not agree. Like Judge Williams, I believe that the failure to establish the likelihood of success depends at least in the first instance on plaintiffs' inability to establish the jurisdiction of the court. I also agree with Judge Williams that plaintiffs have not established the jurisdiction of the court. That being the case, I would not remand the case for further proceedings, but would direct its dismissal.

As my colleagues recognize, in order to bring a cause within the jurisdiction of the court, the plaintiffs must demonstrate, *inter alia*, that they have standing. "[T]o show standing, a plaintiff must demonstrate an 'injury in fact' that is 'actual or imminent, not conjectural or hypothetical.'" Williams Op. at 1 (quoting *Friends of the Earth, Inc. v. Laidlaw Envt'l Servs. (TOC), Inc.*, 528 U.S. 167, 180 (2000). As Judge Williams goes on to note, "[p]laintiffs claim to suffer injury from government collection of records from their telecommunications provider relating to their calls." *Id.* at 1; *see also* Brown Op. 2. However, plaintiffs never in any fashion demonstrate that the government is or has been collecting such records from their telecommunications provider, nor that it will do so. Briefly put, and discussed in more detail by Judge Williams, plaintiffs' theory is that because it is a big collection and they use a big carrier, the government must be getting at their records. While this may be a better-than-usual conjecture, it is nonetheless no more

than conjecture.

As Judge Williams further notes, "*Clapper v. Amnesty International*, 133 S. Ct. 1138 (2013), represents the Supreme Court's most recent evaluation of comparable inferences and cuts strongly against plaintiffs' claim that they have a substantial likelihood of prevailing as to standing." Williams Op. at 3–4. While *Clapper* involved collection under a different statutory authorization, the standing claims of the plaintiffs before us and the plaintiffs in that case are markedly similar. In fact, the plaintiffs' claim before us is weaker than that of the *Clapper* plaintiffs. The *Clapper* plaintiffs at least claimed that the government had previously targeted them or someone with whom they were communicating. The plaintiffs before us make no such claim. I would go farther than Judge Williams. *Clapper* does not just "cut[ ] strongly against plaintiffs' claims that they have a substantial likelihood of prevailing as to standing," *Clapper* cuts their claims out altogether.

Plaintiffs have not demonstrated that they suffer injury from the government's collection of records. They have certainly not shown an "injury in fact" that is "actual or imminent, not conjectural or hypothetical." *Friends of the Earth, Inc.*, 528 U.S. at 180. I agree with the conclusion of my colleagues that plaintiffs have not shown themselves entitled to the preliminary injunction granted by the district court. However, we should not make that our judicial pronouncement, since we do not have jurisdiction to make any determination in the cause. I therefore would vacate the preliminary injunction as having been granted without jurisdiction by the district court, and I would remand the case, not for further proceedings, but for dismissal.

In *Clapper*, the Court stated, "Yet respondents have no

actual knowledge of the Government's . . . targeting practices. Instead, respondents merely speculate and make assumptions about whether their communications with their foreign contacts will be acquired . . . ." 133 S. Ct. at 1148. After discussing the speculative nature of plaintiffs' claims, the Supreme Court summed up its decision as "respondents' speculative chain of possibilities does not establish that injury based on potential future surveillance is certainly impending or is fairly traceable to [the government's acts]." *Id.* at 1150. Therefore, in a conclusion fully applicable to the case before us, the Supreme Court held "that respondents lack Article III standing because they cannot demonstrate that the future injury they purportedly fear is certainly impending and because they cannot manufacture standing by incurring costs in anticipation of non-imminent harm." *Id.* at 1155.

Without standing there is no jurisdiction. Without jurisdiction we cannot act. *See Steel Co. v. Citizens for a Better Environment*, 523 U.S. 83, 94–95 (1998). Therefore, I agree with my colleagues that the issuance of the preliminary injunction was an *ultra vires* act by the district court and must be vacated. However, I believe we can do no more. I would remand the case for dismissal, not further proceedings.