APPENDIX

APPENDIX

TABLE OF CONTENTS

APPENDIX A

NOT PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 19-1366

[Filed March 2, 2020]

ELLIOTT J. SCHUCHARDT, individually and doing business as the Schuchardt Law Firm, on behalf of himself and all others similarly situated,	)
Appellant	)
v.	)
PRESIDENT OF THE UNITED STATES OF AMERICA; DIRECTOR OF NATIONAL INTELLIGENCE; DIRECTOR OF THE NATIONAL SECURITY AGENCY AND CHIEF OF THE CENTRAL SECURITY SERVICE; DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION	)

App. 2

Appeal from the United States District Court
for the Western District of Pennsylvania
(D.C. Civil Action No. 2-14-cv-00705)
District Judge: Honorable Cathy Bissoon

Argued September 23, 2019

Before: McKEE, AMBRO, and ROTH, Circuit Judges

(Opinion filed: March 2, 2020)

Elliott J. Schuchardt (Argued)
6223 Highland Place Way
Suite 201
Knoxville, TN 37919

Counsel for Appellant

Joseph H. Hunt
Assistant Attorney General
Scott W. Brady
United States Attorney
Joseph F. Busa (Argued)
H. Thomas Byron III
United States Department of Justice
Civil Division, Appellate Staff 7537
950 Pennsylvania Avenue, N.W.
Washington, DC 20530

Counsel for Appellees

OPINION*

AMBRO, Circuit Judge

Elliott J. Schuchardt alleges that the bulk data collection programs of the National Security Agency ("NSA") under the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq.*, violate the Fourth Amendment because they allow the Government to intercept, access, monitor, and store all or substantially all U.S. domestic e-mail without probable cause. Pl.'s App. 138–67. He filed suit in 2014 against the President of the United States, the Director of National Intelligence, the Director of the NSA, and the Director of the Federal Bureau of Investigation ("FBI"). After the District Court dismissed Schuchardt's suit for lack of facial standing under Federal Rule of Civil Procedure 12(b)(1), we reversed. *See Schuchardt v. President of the U.S.* ("*Schuchardt I*"), 839 F.3d 336 (3d Cir. 2016).

In a facial attack, we review only "the allegations of the complaint and documents referenced therein and attached thereto, in the light most favorable to the plaintiff." *Gould Elecs. Inc. v. United States*, 220 F.3d 169, 176 (3d Cir. 2000). However, if the defendant contests the pleaded jurisdictional facts, "the court must permit the plaintiff to respond with evidence supporting jurisdiction." *Id.* at 177 (citing *Int'l Ass'n of*

* This disposition is not an opinion of the full Court and pursuant to I.O.P. 5.7 does not constitute binding precedent.

Machinists & Aerospace Workers v. Nw. Airlines, Inc., 673 F.2d 700, 711–12 (3d Cir. 1982)).

On remand, the District Court held that Schuchardt failed to rebut the evidence the Government submitted to challenge his factual standing. We agree and thus affirm the District Court's ruling.

A. Procedural Background

Schuchardt specifically alleged that the NSA operates a program known as PRISM through which it collects "massive quantities of e-mail and other data created by [U.S.] citizens" "directly from the servers" of U.S. service providers like Google, Microsoft, Yahoo, Facebook, Dropbox, and Apple. Pl.'s App. 145. As "a consumer of various types of electronic communication, storage, and [I]nternet-search services" of those service providers, *id.* at 156, Schuchardt further asserted that the Government "obtained direct access to the servers" of the providers and was "intercepting, accessing, monitoring and/or storing [his] private communications . . . ." *Id.* at 145, 156, 158.[1]

Schuchardt supplemented his complaint with two categories of exhibits. First, he submitted reports from the Washington Post and Guardian newspapers about

---

[1] The Government argues that this case is about PRISM and not other programs. Gov't Br. 27–31. That question was never squarely before the District Court. Nor is it before us. The Government did not argue on remand that Schuchardt was not permitted to submit non-PRISM evidence, and in fact itself submitted evidence that goes beyond PRISM. *See* Gov't's Add. A; Gov't's Add. B. Schuchardt correctly points out that his complaint is broad enough to include programs beyond PRISM. Schuchardt Reply 12.

classified documents leaked by former NSA contractor Edward Snowden, as well as excerpts of the materials themselves. These exhibits refer to an NSA program engaged in the bulk collection of domestic e-mail metadata. *Id.* at 91–131. Several of the documents appear to be internal NSA slides. One is titled "Dates When PRISM Collection Began For Each Provider," and lists dates when several service providers began collection. Another slide, "New Collection Posture," includes slogans such as "Exploit it All." *Id.* at 109–10.

The second category of documents Schuchardt attached contained affidavits filed in support of the plaintiffs in *Jewel v. NSA*, 965 F. Supp. 2d 1090 (N.D. Cal. 2013), a separate case challenging the NSA's interception of internet traffic. *Id.* at 1098. The affidavits were of former NSA employees William E. Binney, Thomas A. Drake, and J. Kirk Wiebe, who asserted that after September 11, 2001, the agency developed an expansive view of its own surveillance authority. Pl.'s App. 186–219. Binney stated that he was the creator of the technology the Government uses today to conduct large-scale data collection, and that members of his team told him the Government implemented intelligence activities after September 11 known as the President's Surveillance Program that involved the collection of domestic e-mails without the privacy protections built into other NSA programs. *Id.* at 187–88.

The District Court dismissed in 2015 Schuchardt's complaint for lack of standing. A Rule 12(b)(1) motion under the Federal Rules of Civil Procedure to dismiss for lack of subject matter jurisdiction may be treated as

either a facial or factual challenge. *See Mortensen v. First Fed. Sav. & Loan Ass'n*, 549 F.2d 884, 891 (3d Cir. 1977).

The District Court concluded, for facial challenge purposes, that Schuchardt had "identified no facts from which [it] reasonably might infer that [the plaintiff's] own communications have been targeted, seized or stored." Pl.'s App. 14–24. As noted, we reversed in 2016 and concluded that his allegations "plausibly stated an injury in fact personal to" him "as a facial matter." *Schuchardt I*, 839 F.3d at 338. Thus we considered the exhibits Schuchardt submitted and afforded his pleadings the presumption of truth. Though the Government disputed Schuchardt's allegations and submitted evidence, we could not, on a facial attack, consider its submissions. *Id.* at 346, 352–53. Finally, we noted that the Government was "free upon remand to make a factual jurisdictional challenge to Schuchardt's pleading." *Id.* at 353.

On remand, the parties agreed that, rather than engage in discovery as to jurisdiction, the Government would make an informal information disclosure; if Schuchardt was not satisfied, he could resume the litigation. The District Court directed Schuchardt to inform it "whether or not this case w[ould] be dismissed based on the information provided . . . ." Pl.'s App. 10. Thereafter, Schuchardt did not make any discovery or extension requests. The Government filed a renewed motion to dismiss, and Schuchardt filed a response relying on new affidavits from Binney and Wiebe. *Id.* at 63–66. Schuchardt conceded at oral argument that he did not make any discovery or extension requests nor

ask for a hearing to qualify Binney and Wiebe as experts.

The District Court issued an order in February 2019 dismissing Schuchardt's case for lack of standing on a factual challenge. Pl.'s App. 63. It concluded that the Government showed that it "did not engage in dragnet-type collection activity," and in support of that conclusion it incorporated "by reference, as if fully restated, the evidence and arguments recited in [the Government's] opening and reply briefs." *Id.* at 64. Moreover, the documents Schuchardt submitted were inadmissible and did not create a factual dispute as to his standing. The Court went on to state that, "[e]ven permitting all of [Schuchardt's] evidence—which . . . [was] restricted to the recent affidavits of [] Binney and Wiebe," and the documents attached thereto, the Government's "positions carry the day." *Id.* at 64–65. Schuchardt's "post remand efforts" were "underwhelming" and merely amounted to taking the same evidence previously before the District Court and "filter[ing] it through the mouthpiece of purported experts." *Id.* at 65.[2]

B. Jurisdiction and Standard of Review

The District Court had jurisdiction under 28 U.S.C. § 1331. We have jurisdiction per 28 U.S.C. § 1291.

---

[2] Because it incorporated the Government's briefs in their entirety, we discuss the evidence and arguments therein as the Court's own decision. We nonetheless note that the wholesale adoption of one side's briefs is a practice we discourage. *See In re Complaint of Luhr Bros., Inc.*, 157 F.3d 333, 338 (5th Cir. 1998); *Walton v. United Consumers Club, Inc.*, 786 F.2d 303, 313–14 (7th Cir. 1986).

"When reviewing an order dismissing a claim for lack of subject matter jurisdiction, we exercise plenary review over legal conclusions and review findings of fact for clear error." *Adorers of the Blood of Christ v. Fed. Energy Reg. Comm'n*, 897 F.3d 187, 193 (3d Cir. 2018) (citation omitted). We review the District Court's evidentiary findings for abuse of discretion. "In order to justify reversal, a district court's analysis and resulting conclusion must be arbitrary or irrational." *United States v. Bailey*, 840 F.3d 99, 117 (3d Cir. 2016) (citation and quotation marks omitted).[3]

C. Rule 12(b)(1) Factual Challenge

On a Rule 12(b)(1) factual challenge, the plaintiff has the burden of proof, *Mortensen*, 549 F.2d at 891, and the burden of persuasion, *Gould Elecs Inc.*, 220 F.3d at 178. Thus "a 12(b)(1) *factual* challenge strips the plaintiff of the protections and factual deference provided under 12(b)(6) review" for a typical motion to dismiss on the merits, *Hartig Drug Co. Inc. v. Senju Pharm. Co. Ltd.*, 836 F.3d 261, 268 (3d Cir. 2016) (emphasis added) (citation omitted), and under *facial*

---

[3] Schuchardt devoted much of his brief to the merits of this case. Schuchardt Br. 43–55. The District Court did not reach the merits, as it dismissed on a Rule 12(b)(1) motion. Accordingly, we do not consider his arguments as to the merits. Schuchardt also cited for the first time in his opening brief to non-record evidence (for example, a statement by a government scientist) that every e-mail sent in the United States goes into a Government database. Schuchardt Br. 22, 38. With rare exceptions not in play here, we will not consider evidence outside the record. *See Reed v. Phila. Bethlehem & New England R.R. Co.*, 939 F.2d 128, 133 (3rd Cir. 1991).

12(b)(1) review, *see CNA v. United States*, 535 F.3d 132, 139 (3d Cir. 2008).

It is true that a "[j]urisdictional finding of genuinely disputed facts is inappropriate when the jurisdictional issue and substantive issues are so intertwined that the question of jurisdiction is dependent on the resolution of factual issues going to the merits of an action." *Davis v. Wells Fargo*, 824 F.3d 333, 348 (3d Cir. 2016) (citation omitted). When a case raises a disputed factual issue that goes both to the merits and jurisdiction, district courts must "demand less in the way of jurisdictional proof than would be appropriate at a trial stage." *Mortensen*, 549 F.2d at 892. Although we have not defined the contours of the "less in the way of jurisdictional proof" standard, we have held that "[b]ecause at issue in a factual 12(b)(1) motion is the trial court's jurisdiction[,] its very power to hear the case[,] there is substantial authority that the trial court is free to weigh the evidence and satisfy itself as to the existence of its power to hear the case." *Id.* at 891. "The form of the inquiry is flexible . . . : 'As there is no statutory direction for procedure upon an issue of jurisdiction, the mode of its determination is left to the trial court.'" *Id.* at 891 n.16 (quoting *Gibbs v. Buck*, 307 U.S. 66, 71–72 (1939)).

This is not a case where Schuchardt presented competent evidence that the District Court discounted or where it weighed competing evidence presented by the Government and Schuchardt.[4] The Court

[4] This is also not a case where the Government refused to turn over discovery related to its intelligence-gathering activities.

considered the evidence the Government submitted to challenge Schuchardt's standing, stated that the burden of proof was on Schuchardt, gave him an opportunity to be heard, and considered his submissions in detail. On this record, the Court held that he did not create a dispute of material fact as to his standing. *See CNA*, 535 F.3d at 144–46 (affirming dismissal where plaintiffs were heard on the jurisdictional issue but failed to present evidence creating a factual dispute as to subject matter jurisdiction). It did not err by considering the admissibility of Schuchardt's submission, as required expressly by some Circuits. *See McPhail v. Deere & Co.*, 529 F.3d 947, 954 (10th Cir. 2008); *Meridian Sec. Ins. Co. v. Sadowski*, 441 F.3d 536, 540, 542 (7th Cir. 2006).

D. The District Court's Evidentiary Rulings

Thus we turn to the evidentiary rulings of the District Court. It held that the documents Schuchardt submitted on remand were unauthenticated and contained hearsay, and that Binney and Wiebe's opinions did not meet the reliability requirements for admission of expert testimony. Gov't's Add. A 8–9, 25–26; Gov't's Add. B 6–7.[5] The Court considered Schuchardt's lack of evidence in light of the

---

Schuchardt made no discovery requests, and the Court did not rule on any applicable national security privileges.

[5] The Government inaccurately argues that Schuchardt's opening brief failed to address the evidentiary holdings. Gov't Br. 23. Schuchardt did argue, if summarily, that the Court understated Binney's expertise and that he could have authenticated the documents. Schuchardt Br. 30–33.

Government's admissible submission and concluded that Schuchardt failed to meet his burden of proof.

1. Schuchardt Presented Unauthenticated Documents.

A party seeking to rely on a piece of evidence must offer proof sufficient to support a finding that the item is what that party claims it to be. Fed. R. Evid. 901(a); *United States v. Browne*, 834 F.3d 403, 408 (3d Cir. 2016). That evidence "must itself be admissible." *In re Japanese Elec. Prods. Antitrust Litig.*, 723 F.2d 238, 285 (3d Cir. 1983). As for the purported NSA slides, Pl.'s App. 108–13, Schuchardt did not explain what they were, other than describing them as the "Snowden documents," Gov't's Add. A 8–9, 25–26. The District Court could only speculate about what they were. The origin and nature of the new documents attached to Binney's affidavit on remand were equally dubious. The new documents included maps showing "tap points" where the NSA connects into service providers' networks and slides explaining collection. Pl.'s App. 244–47. Schuchardt argues that Binney and Wiebe authenticated the documents in their affidavits, Schuchardt Reply 6, because those documents related to programs they created and worked on, Pl.'s App. 231, and because Binney obtained them from publications, which in turn allegedly got the documents from Snowden, *id.* at 232. The Court correctly rejected this argument because Binney claimed no personal knowledge that the documents he obtained from the publications were those allegedly misappropriated by Snowden. Gov't's Add. B 6–7. Neither Binney nor

Wiebe claimed he created the documents or to know who did.

Schuchardt's argument that the Snowden documents were authenticated by the Government's admissions that Snowden misappropriated documents also fails. Any general admissions by Government officials that Snowden stole documents did not authenticate the specific documents Schuchardt submitted to the Court. *See ACLU v. U.S. Dep't of State*, 878 F. Supp. 2d 215, 224 (D.D.C. 2012). Hence there was no abuse of discretion in ruling that those documents were not properly authenticated.

2. Schuchardt Presented Evidence Based on Hearsay.

Hearsay is any statement, other than one made by a declarant while testifying at the trial or hearing, "offer[ed] in evidence to prove the truth of the matter asserted." Fed. R. Evid. 801. It is generally inadmissible as evidence. *See United States v. Pelullo*, 964 F.2d 193, 203 (3d Cir. 1992). The District Court concluded that the NSA slides "constitute written out-of-court statements regarding PRISM's operation that [Schuchardt] offers for the truth of the matters asserted," and are inadmissible hearsay. Gov't's Add. A 26. It reached the same conclusion regarding the new documents attached to Binney's affidavit because Binney claimed no personal knowledge of the documents and obtained them from journalists, who allegedly obtained them from Snowden, so that "[e]ach link in this chain of custody is . . . predicated on . . . hearsay." Gov't's Add. B 6–7. As for the newspaper articles and editorials, the Court held that they too

were hearsay. Schuchardt offered no substantial argument why these materials were subject to a hearsay exception. We accordingly affirm the District Court in barring them.

3. Schuchardt Failed to Qualify His Expert Witnesses.

Federal Rule of Evidence 702 governs the use of expert testimony in federal courts and imposes three threshold considerations: qualifications, reliability, and fit. *See In re Paoli R.R. Yard PCB Litig.*, 35 F.3d 717, 741–43 (3d Cir. 1994). An expert witness must have specialized expertise or knowledge. *See id.* at 741. Though we construe the specialized knowledge requirement liberally, "at a minimum, a proffered expert witness . . . must possess skill or knowledge greater than the average layman . . . ." *Waldorf v. Shuta*, 142 F.3d 601, 625 (3d Cir. 1998). District courts perform a screening function, typically called a *Daubert* hearing, to ensure that evidence presented is, among other things, reliable. *See Daubert v. Merrell Dow Pharm., Inc.*, 509 U.S. 579, 597 (1993). It is so if "based on the 'methods and procedures of science' rather than on 'subjective belief or unsupported speculation . . . .'" *Paoli*, 35 F.3d at 742 (citation omitted). Rule 703 permits experts to rely on hearsay so long as it is of the kind normally employed by experts in the field. *See In re TMI Litig.*, 193 F.3d 613, 697 (3d Cir. 1999). However, the trial judge must conduct an independent evaluation of the reasonableness of relying on the type of data underlying the opinion. *See Paoli*, 35 F.3d at 748.

Binney stated in his affidavit that he "was the primary designer and developer of a number of programs designed to acquire and analyze very large amounts" of information from the "Internet" before leaving the NSA in 2001. Pl.'s App. 228–29. He continues to serve as a consultant to foreign governments on intelligence collection and has testified before foreign government agencies. *Id.* at 240. According to Binney, after the September 11 attacks the NSA's surveillance program changed to allow indiscriminate bulk data collection, and the President's Surveillance Program thereafter involved the "collection of the full content of domestic e-mail traffic." *Id.* at 230. Binney based his conclusions on "the highly-detailed information contained in the documents leaked by [Snowden]." *Id.* at 231. Binney stated that "[t]he documents provided by Mr. Snowden are the type of data that experts in the intelligence community would typically and reasonably rely upon . . . ." *Id.* at 232. Wiebe submitted a two-page affidavit agreeing with Binney's assessment based on his review of the same documents. *Id.* at 249–54.

The District Court concluded that Binney and Wiebe were not qualified to testify as experts. Neither identified or described the field of "scientific, technical, or other specialized knowledge" in which he is purportedly an expert. Gov't Add. B 9. Wiebe did not discuss the exhibits at all in his affidavit, and Binney did not explain how the exhibits led him to reach his conclusions. *Id.* at 9–10. The Court therefore could not determine whether their conclusions were based on reliable principles and methods. It also discounted Schuchardt's argument that the affidavits were

admissible under Rule 703 based on Binney's assertion that the Snowden documents are the "type of data that experts in the intelligence community would typically and reasonably rely upon." *Id.* at 10 n.7.[6] That assertion provided no basis for the Court to conduct an independent evaluation into reasonableness. *Id.* Moreover, Schuchardt did not request a *Daubert* hearing or submit evidence regarding Binney and Wiebe's field of expertise or their methodologies. Accordingly, the Court did not abuse its discretion in barring their testimony as experts.

4. The Government's Evidence

Contrast Schuchardt's lack of competent evidence against the admissible submissions by the Government. These included a sworn declaration from Wayne Murphy, the Director of Operations at the NSA, who was "responsible for . . . managing the integration and use of the NSA's global foreign intelligence authorities" and had "personal knowledge" of the matters alleged in Schuchardt's complaint. Pl.'s App. 173. He stated that "[n]either PRISM nor any other NSA intelligence-gathering activity involves the bulk collection (or storage) of all or substantially all of the e-mail (or other Internet-based communications) of all U.S. persons." *Id.* The District Court credited those statements and reasoned that Schuchardt could not show that his communications would have been

---

[6] The District Court also separately ruled, and we affirm, that Binney and Wiebe could not testify as fact witnesses because they did not claim any personal knowledge of the NSA's current collection programs. Gov't's Add. A 29–31.

targeted and collected. Gov't Add. A 22. The Government also cited other authorities, such as the Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act issued in July 2014 by the Privacy and Civil Liberties Oversight Board, as well as case law from other Circuits, acknowledging the targeted nature of PRISM, *see, e.g., United States v. Mohamud*, 843 F.3d 420, 440 (9th Cir. 2016).

* * * * *

Because the District Court did not abuse its discretion in concluding that Schuchardt's evidence was inadmissible and that the Government's evidence stood uncontroverted, we affirm its ruling that Schuchardt lacked factual standing for his suit.

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 19-1366

[Filed March 2, 2020]

ELLIOTT J. SCHUCHARDT, individually and doing business as the Schuchardt Law Firm, on behalf of himself and all others similarly situated,	)
Appellant	)
v.	)
PRESIDENT OF THE UNITED STATES OF AMERICA; DIRECTOR OF NATIONAL INTELLIGENCE; DIRECTOR OF THE NATIONAL SECURITY AGENCY AND CHIEF OF THE CENTRAL SECURITY SERVICE; DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION	)

Appeal from the United States District Court
for the Western District of Pennsylvania
(D.C. Civil Action No. 2-14-cv-00705)
District Judge: Honorable Cathy Bissoon

Argued September 23, 2019

Before: McKEE, AMBRO, and ROTH, Circuit Judges

JUDGMENT

This cause came on to be heard on the record before the United States District Court for the Western District of Pennsylvania and was argued on September 23, 2019.

On consideration whereof, IT IS ORDERED AND ADJUDGED by this Court that the judgment of the District Court entered February 4, 2019, is hereby affirmed. Costs taxed against Appellant. All of the above in accordance with the opinion of this Court.

ATTEST:

Dated: March 2, 2020

s/ Patricia S. Dodszuweit
Clerk

APPENDIX B

IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF PENNSYLVANIA

Civil Action No. 14-705

Judge Cathy Bissoon

[Filed February 4, 2019]

ELLIOTT SCHUCHARDT,)
)
Plaintiff,)
v.)
)
DONALD J. TRUMP, *et al.*,)
)
Defendants.)
)

ORDER

Defendants' renewed Motion to Dismiss (Doc. 57) for lack of standing will be granted. The parties are well-acquainted with the underlying facts and arguments in this case; including the Court of Appeals for the Third Circuit's Opinion and instructions on remand. The only issue is: has Plaintiff plausibly shown, under the factual-challenge-to-standing paradigm (as opposed to facial), that the government captured his information through dragnet-type data collection.

The Circuit Court specifically held that Plaintiff's "alleged facts - even if proven – do not conclusively establish that PRISM operates as a dragnet on the scale he has alleged." Doc. 38 at 31. The Court acknowledged that the "[s]everal commentators and . . . few courts" to "have examined PRISM appear to agree with the Government's view of the program's 'targeted' nature." *Id.* at 32-33. It envisioned the government renewing its standing-challenge, this time factually as opposed to facially; and it raised the prospect of jurisdictional discovery, and the relevant-considerations attendant thereto.

Rather than engage in jurisdictional discovery, the parties agreed that the government would make an informal informational-disclosure; and Plaintiff contemplated that he might be thus-satisfied, rendering additional litigation unnecessary. Ultimately, however, Plaintiff remained unconvinced, and Defendants have renewed their Motion to Dismiss.

Nowhere in opposition does Plaintiff complain that he was denied a fair opportunity to marshal evidence to contradict the government's record. Rather, he has enlisted the efforts of two purported "experts," Messrs. Binney and Wiebe (who are no strangers to this litigation). These individuals have not worked for the NSA since 2001, and their affidavits rely on the same categories of materials that already were before the District and Circuit Courts the first time around.

A current evaluation of Plaintiff's claims is heavily-influenced by the context and legal framework now applicable. Given that the standing-inquiry has shifted from a facial challenge to a factual one, Plaintiff carries

the burden, and the standard is a preponderance-of-the-evidence. ACE Amer. Ins. Co. v. Guerriero, 738 Fed. Appx. 72, 76 (3d Cir. June 20, 2018); *accord* GBForefront, L.P. v. Forefront Mgmt. Grp., LLC, 888 F.3d 29, 35 (3d Cir. 2018) (cited and relied upon in ACE American).

Defendants have shown, by a preponderance of the evidence, that the government did not engage in dragnet-type collection activity – as discussed by the Circuit Court - thereby establishing a plausible claim that Plaintiff's data was captured. In support of this conclusion, the Court incorporates by reference, as if fully restated, the evidence and arguments recited in Defendants' opening and reply briefs (Docs. 58 & 73).

The court need not delve into the niceties of the various individual evidentiary-challenges raised by Defendants, as relates to Plaintiff's materials. Even permitting all of Plaintiff's evidence - which, by the time of his current briefing, is restricted to the recent affidavits of Messrs. Binney and Wiebe[1] – Defendant's positions carry the day under the preponderance-of-the evidence standard (a conclusion that should not be entirely surprising, given the language of the Circuit Court's Opinion).

This Court sees little benefit to rehashing the arguments and factual recitations in Defendants' briefing, which are meticulous and already have been

---

[1] *See* Pl.'s Opp'n Br. (Doc. 68) at 10-11 (declining to resist Defendants' arguments regarding the non-competence of evidence "*previously filed* in this case," because Plaintiff now is relying on his "two new affidavits") (emphasis in original).

incorporated by reference. The Court does offer, though, these additional overarching observations. Plaintiff's new affidavits, in large part, rely on the same underlying evidence already before this Court and the Circuit. What new documents are referenced – even assuming their authenticity and admissibility – do not tip the scales under the preponderance of the evidence standard. *See* Defs.' Reply (Doc. 73) at 3-4 (explaining why the new documents still do not demonstrate dragnet-collection, as alleged by Plaintiff). More generally, the notion that Plaintiff can take largely the same evidence; filter it through the mouthpiece of purported experts (with modest embellishment); and hope to satisfy his burdens under the presently-applicable standards; seems rather weak tea, given the Circuit Court's discussions.

While this Court questions-not Plaintiff's sincerity and passion, his post-remand efforts, candidly, are somewhat underwhelming. Perhaps the limitations say less of Plaintiff's efforts than an inconvenient-reality – in light of the record now before the Court, PRISM has *not* been shown to be the dragnet-type collection mechanism suggested. There really is not much more to be said.

The Court appreciates the candor and reasonableness with which Plaintiff has approached the remand. *See* discussion *supra* (noting Plaintiff's willingness to keep an open mind regarding continued-pursuit of this litigation, depending on what the government ultimately presented). Hopefully, he can close this chapter feeling that his civic-duty has been met, to the fullest of his abilities; and that his overall

objectives have been achieved. *Cf.* Defs.' Br. (Doc. 58) at 10 (by the time of remand, Plaintiff's claims regarding the bulk collection of telephone metadata were mooted by the passage of the USA FREEDOM Act; he had no claim for money damages; and all that remained was his claim for injunctive relief based on the government's alleged bulk collections under PRISM).[2]

For all of the reasons stated herein, Defendants' renewed Motion to Dismiss (**Doc. 57**) is **GRANTED**, and a judgment order under Rule 58 will issue contemporaneously herewith.

IT IS SO ORDERED.

February 4, 2019

s/Cathy Bissoon
Cathy Bissoon
United States District Judge

cc (via ECF email notification):

All Counsel of Record

---

[2] This Court takes comfort in knowing that the legislature has imposed measures of accountability, as relates to the programs-in-question, including PRISM. *See id.* at 15-16 (discussing the Privacy and Civil Liberties Oversight Board's Report, which supports the government's evidence that PRISM achieves targeted, not dragnet-type, data collection).

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF
PENNSYLVANIA

Civil Action No. 14-705

Judge Cathy Bissoon

[Filed February 4, 2019]

ELLIOTT SCHUCHARDT,	)
	)
Plaintiff,	)
v.	)
	)
DONALD J. TRUMP, *et al.*,	)
	)
Defendants.	)
	)

JUDGMENT ORDER

FINAL JUDGMENT hereby is entered pursuant to Rule 58 of the Federal Rules of Civil Procedure. This case has been marked closed.

IT IS SO ORDERED.

February 4, 2019

s/Cathy Bissoon
Cathy Bissoon
United States District Judge

cc (via ECF email notification):

All Counsel of Record

APPENDIX C

PRECEDENTIAL

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 15-3491

[Filed October 5, 2016]

ELLIOTT J. SCHUCHARDT, individually and doing business as the Schuchardt Law Firm, on behalf of himself and all others similarly situated,
Appellant

v.

PRESIDENT OF THE UNITED STATES; DIRECTOR OF NATIONAL INTELLIGENCE; DIRECTOR OF THE NATIONAL SECURITY AGENCY AND CHIEF OF THE CENTRAL SECURITY SERVICE; DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION

Appeal from the United States District Court
for the Western District of Pennsylvania
(W.D. Pa. No. 2-14-cv-00705)
District Judge: Honorable Cathy Bissoon

Argued: May 17, 2016

Before: *SMITH, *Chief Judge*, HARDIMAN, and NYGAARD, *Circuit Judges*.

(Filed: October 5, 2016)

Elliot J. Schuchardt [Argued]
309 Braeburn Drive
Winchester, VA 22601
Counsel for Appellant

Andrew G. Crocker, Esq.
Electronic Frontier Foundation
815 Eddy Street
San Francisco, CA 94109
Counsel for Amicus Appellant

Benjamin C. Mizer
David J. Hickton
H. Thomas Byron III
Henry C. Whitaker [Argued]
United States Department of Justice
Appellate Section, Room 7256
950 Pennsylvania Avenue, N.W.

---

* Honorable D. Brooks Smith, United States Circuit Judge for the Third Circuit, assumed Chief Judge status on October 1, 2016

Washington, DC 20530
Counsel for Appellee

OPINION

HARDIMAN, *Circuit Judge.*

This appeal involves a constitutional challenge to an electronic surveillance program operated by the National Security Agency (NSA) under the authority of Section 702 of the Foreign Intelligence Surveillance Act (FISA). Elliott Schuchardt appeals an order of the United States District Court for the Western District of Pennsylvania dismissing his civil action for lack of jurisdiction. The District Court held that Schuchardt lacked standing to sue because he failed to plead facts from which one might reasonably infer that his own communications had been seized by the federal government. Because we hold that, at least as a facial matter, Schuchardt's second amended complaint plausibly stated an injury in fact personal to him, we will vacate the District Court's order and remand.

I

Schuchardt's appeal is the latest in a line of cases raising the question of a plaintiff's standing to challenge surveillance authorized by Section 702. Congress amended FISA in 2008 to "supplement[] pre-existing FISA authority by creating a new framework under which the Government may . . . target[] the communications of non-U.S. persons located abroad." *Clapper v. Amnesty International USA*, 133 S. Ct. 1138,

1144 (2013); *see also* FISA Amendments Act of 2008, Pub. L. No. 110–261, 122 Stat. 2436, 2438, 50 U.S.C. § 1881a. On the day Section 702 became law, its constitutionality was challenged by "attorneys and human rights, labor, legal, and media organizations whose work allegedly require[d] them to engage in . . . telephone and e-mail communications" with persons located outside the United States. *See id.* at 1145. The *Clapper* plaintiffs claimed that Section 702 was facially unconstitutional under the Fourth Amendment, which prohibits unreasonable searches and seizures. *See id.* at 1146.

A

The dispositive question presented to the Supreme Court in *Clapper* was whether the plaintiffs had established an "imminent" injury "fairly traceable" to the government's conduct under Section 702. *See* 133 S. Ct. at 1147. Because the plaintiffs had brought suit on the day the law was enacted, there was no evidence that their communications had been intercepted—there was only a looming "threat of [future] surveillance." *Id.* at 1145–46. Nonetheless, the plaintiffs claimed they had standing because there was an "objectively reasonable likelihood" that their communications would be intercepted based on the nature of their contacts with persons outside of the country. *Id* at 1146.

The Supreme Court rejected this argument as "inconsistent" with longstanding precedent requiring that "threatened injury must be *certainly impending* to constitute injury in fact," *Clapper*, 133 S. Ct. at 1147 (emphasis in original) (quoting *Whitmore v. Arkansas*,

495 U.S 149, 158 (1990)). And because the plaintiffs could rely only on a "speculative chain of possibilities" to support their allegations of future harm from unlawful government surveillance, they failed to demonstrate an injury that was "certainly impending." *Id.* at 1150.

In particular, the Court characterized the *Clapper* plaintiffs' "speculative chain" as entailing five inferential leaps:

> (1) the Government will decide to target the communications of non-U.S. persons with whom [the plaintiffs] communicate;
>
> (2) in doing so, the Government will choose to invoke its authority under [Section 702] rather than . . . another method of surveillance;
>
> (3) the Article III judges who serve on the Foreign Intelligence Surveillance Court will conclude that the Government's proposed surveillance procedures . . . satisfy [Section 702's] many safeguards and are consistent with the Fourth Amendment;
>
> (4) the Government will succeed in intercepting the communications of [the plaintiffs'] contacts; and
>
> (5) [the plaintiffs] will be parties to the particular communications that the Government intercepts.

133 S. Ct. at 1148.

On summary judgment, the plaintiffs had failed to "set forth by affidavit or other evidence specific facts" supporting these inferences. *Id.* at 1149 (internal quotation marks omitted). Accordingly, they lacked standing to challenge the constitutionality of Section 702. *Id.*

B

Soon after *Clapper* was decided, former NSA contractor Edward Snowden leaked a trove of classified documents to journalists writing for the *Washington Post* and *Guardian*.[1] Those documents referenced the existence of an NSA program engaged in the bulk collection of domestic telephone metadata, *i.e.*, "details about telephone calls, including for example, the length of a call, the phone number from which the call was made, and the phone number called," but not the voice content of the call itself. *ACLU v. Clapper*, 785 F.3d 787, 793 (2d Cir. 2015); *see also Smith v. Obama*, 816 F.3d 1239, 1241 (9th Cir. 2016); *Obama v. Klayman*, 800 F.3d 559, 561 (D.C. Cir. 2015). The operational parameters of the program were summarized in a classified order of the Foreign Intelligence Surveillance Court (FISC) directed at Verizon Business Network Services. *ACLU*, 785 F.3d at 795. In short, based on Section 215 of the USA PATRIOT Act, Pub. L. No. 107–56, 115 Stat. 272, 287 (2001) (codified as amended at 50 U.S.C. § 1861 *et seq.*), Verizon was producing to

---

[1] *See, e.g.*, Ellen Nakashima, *Verizon Providing All Call Records to U.S. Under Court Order*, Wash. Post (June 6, 2013), https://perma.cc/LZK7-37CJ; *see also* Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, Guardian (June 6, 2013), https://perma.cc/UR2A-492H.

the government, "all call detail records or 'telephony metadata' . . . on *all* telephone calls made through its systems or using its services where one or both ends of the call are located in the United States." *ACLU*, 785 F.3d at 795.

The government's bulk collection of telephone metadata precipitated a number of lawsuits. In one case, the Second Circuit held that the government had exceeded its statutory authority under Section 215 to obtain "relevant" information by constructing an "all-encompassing" database of "every telephone call made or received in the United States." *ACLU*, 785 F.3d at 812–13. Under the statute's sunset provision, however, authorization for the bulk telephone metadata collection program expired on June 1, 2015. *See* Pub. L. No. 112–14, 125 Stat. 216 (2011) (authorizing an extension); *Smith*, 816 F.3d at 1241. And although the program was subsequently reauthorized by the USA FREEDOM Act, Pub. L. No. 114–23, 129 Stat. 268 (2015), that act "prohibits any further bulk collection." *Smith*, 816 F.3d at 1241. In reliance on that prohibition, the Ninth Circuit has determined that "claims related to the ongoing collection of metadata [under Section 215] are [now] moot." *Id.*

Separate and apart from the bulk collection of telephone metadata under Section 215, the documents leaked to the *Washington Post* and *Guardian* also shed light on a previously undisclosed electronic surveillance program operating under Section 702 called PRISM.[2]

---

[2] *See, e.g.*, Barton Gellman & Laura Poitras, *U.S. British Intelligence Mining Data from Nine U.S. Internet Companies in*

Slides from a presentation purportedly authored by the NSA described PRISM as "collect[ing] directly from the servers" the full content of user communications exchanged using services provided by several large U.S. companies—including Microsoft, Google, Yahoo, Apple, and Facebook. App. 53. Another slide depicted a timeline showing the inception of PRISM collection from each company, beginning with Microsoft in September 2007 and ending with Apple in October 2012. Yet another slide suggested a slogan for the NSA's "New Collection Posture": "Sniff it All, Know it All, Collect it All, Process it All, Exploit it All, and Partner it All." App. 61.

II

On June 2, 2014, Schuchardt filed a complaint in the District Court asserting constitutional, statutory, and state law claims against the President, the Director of National Intelligence, and the Directors of the NSA and Federal Bureau of Investigation. He alleged that the Government was violating the Fourth Amendment by storing his confidential communications "in a computer database, or through a government program, which the Defendants call 'Prism.'" Civil Complaint ¶ 22, *Schuchardt v. Obama*, No. 2-14-cv-00705-CB (W.D. Pa. June 2, 2014), ECF No. 1. He sought to enjoin "the [Government] from

---

Broad Secret Program, Wash. Post (June 7, 2013), https://perma.cc/YJU2-U9TZ; Glenn Greenwald & Ewan MacAskill, *NSA Prism Program Taps in to User Data of Apple, Google and Others*, Guardian (June 7, 2013), https://perma.cc/RPA9-RXSY

engaging in any further collection of . . . [his] information." *Id.* ¶ 37.

Schuchardt responded to the Government's successive motions to dismiss by amending his complaint twice. In addition to refining and expanding his allegations, Schuchardt supplemented his averments with exhibits, the contents of which fall into two general categories. First, he supported his allegations regarding PRISM with excerpts of the classified materials that were the focus of the *Washington Post* and *Guardian* reports, as well as several of the reports themselves. Second, he included affidavits filed in support of the plaintiffs in *Jewel v. NSA* (*Jewel I*), 965 F. Supp. 2d 1090 (N.D. Cal. 2013), a case challenging the NSA's interception of internet traffic flowing through a telecommunications facility in San Francisco pursuant to an Executive Order issued shortly after September 11, 2001. *Id.* at 1098. *Jewel I* was decided on remand from *Jewel v. NSA*, 673 F.3d 902 (9th Cir. 2011), in which the Ninth Circuit held that the plaintiffs had adequately pleaded Article III standing to sue. *See* 673 F.3d at 913. The affidavits in *Jewel I* were filed by former NSA employees who asserted that the agency had, since September 11, developed an expansive view of its own surveillance authority and the technology to back it up. *See, e.g.*, App. 126 ("The post-September 11 approach was that NSA could circumvent federal statutes and the Constitution as long as there was some visceral connection to looking for terrorists. . . . [The NSA] has, or is in the process of obtaining, the capability to seize

and store most electronic communications passing through its U.S. intercept centers.").[3]

Based on the record he had compiled, Schuchardt's second amended complaint alleged that because the Government was "intercepting, monitoring and storing the content of *all or substantially all* of the e-mail sent by American citizens," his own online communications had been seized in the dragnet. App. 82, 95–99 (emphasis added). In particular, Schuchardt asserted that he was "a consumer of various types of electronic communication, storage, and internet services," including "the e-mail services provided by Google and Yahoo; the internet search services of Google; the cloud storage services provided by Google and Dropbox; [and] the e-mail and instant message services provided by Facebook." App. 95–96. Then, relying on the

---

[3] Schuchardt's second amended complaint also asserted: a Fourth Amendment claim challenging the bulk collection of telephone metadata under Section 215, App. 99 (Count II); a Pennsylvania state-law claim, App. 100 (Count III), and a First Amendment claim, App. 101 (Count IV), challenging both PRISM and the telephone metadata program; and statutory claims under FISA seeking injunctive relief, App. 103 (Count V), and damages, App. 104 (Count VI). At oral argument, Schuchardt belatedly conceded that his claims regarding the bulk collection of telephone metadata were mooted by the USA FREEDOM Act. *See* Transcript of Oral Argument at 5, *Schuchardt v. Obama*, No. 15-3491 (3d Cir. May 17, 2016). He also agreed that his claim for monetary damages under FISA was barred by the doctrine of sovereign immunity, and that he was no longer pursuing his claims under the First Amendment. *Id.* at 10–11. In light of Schuchardt's concessions, we do not address these issues, and focus solely on whether he has standing to litigate his Fourth Amendment claim for injunctive relief based on the Government's alleged bulk collection of online communications under PRISM, App. 95 (Count I).

operational details of PRISM made public by the *Washington Post* and *Guardian*, he alleged that: (1) the Government "had obtained direct access to the servers" of the companies providing him with these services; (2) the Government was "unlawfully intercepting, accessing, monitoring and/or storing [his] private communications . . . made or stored through such services"; and (3) the Government was "collecting such information in order to 'data mine' the nation's e-mail database." App. 84, 95–97.

In its motion to dismiss Schuchardt's second amended complaint, the Government principally took issue with his allegation that the "NSA collects the online communications . . . of *all* Americans, including, therefore, his." *See* Brief in Support of Defendants' Motion to Dismiss Plaintiff's Second Amended Complaint at 2, *Schuchardt v. Obama*, No. 2-14-cv-00705-CB (W.D. Pa. Dec. 11, 2014), ECF No. 21 (emphasis added). Specifically, the Government argued that because Section 702 authorizes the targeted surveillance of only persons outside the United States, it was implausible that PRISM—a program operating under the authority of Section 702—was a dragnet capturing all the country's domestic online communications. In support of its position, the Government cited a report on PRISM prepared by the Privacy and Civil Liberties Oversight Board (PCLOB),[4]

---

[4] Privacy & Civil Liberties Oversight Board, Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act (July 2, 2014), *available at* https://www.pclob.gov/library/702-Report.pdf [hereinafter PCLOB Report].

an independent agency tasked with "review[ing] actions the executive branch takes to protect the Nation from terrorism, ensuring that the need for such actions is balanced with the need to protect privacy and civil liberties." 42 U.S.C. § 2000ee(c)(1). Based on its review, the PCLOB determined that "[i]n PRISM collection, the government . . . sends selectors—such as an email address—to a United States-based electronic communications service provider," who is then by law "compelled to give the communications sent to or from that selector to the government." PCLOB Report at 33. Far from being the dragnet that Schuchardt had alleged, therefore, "PRISM collection under Section 702 may be targeted only at non-U.S. persons located abroad who possess or are likely to receive foreign-intelligence information." Brief in Support of Defendants' Motion to Dismiss at 10, *Schuchardt v. Obama*, No. 2-14-cv-00705-CB (W.D. Pa. Aug. 11, 2014), ECF No. 8. Because none of Schuchardt's allegations suggested that he or his associates would be targeted as such persons, the Government argued that he had failed to include "well-pleaded allegations and non-conclusory allegations of fact" necessary to establish his standing. Brief in Support of Defendants' Motion to Dismiss Plaintiff's Second Amended Complaint at 4, *Schuchardt v. Obama*, No. 2-14-cv-00705-CB (W.D. Pa. Dec. 11, 2014), ECF No. 21.

The District Court granted the Government's motion to dismiss Schuchardt's second amended complaint, but took a slightly different tack than what the Government had suggested. After considering four cases examining constitutional standing to sue in cases challenging national security surveillance—*Clapper*,

ACLU, *Jewel*, and *Klayman*—the Court deduced a "meaningful distinction" that explained their divergent outcomes. *Schuchardt v. Obama*, 2015 WL 5732117, at *6 (W.D. Pa. Sept. 30, 2015). "In situations where plaintiffs are able to allege with some degree of particularity that their own communications were specifically targeted—for example by citing a leaked FISC order or relying on a detailed insider account—courts have concluded that the particularity requirement has been satisfied." *Id.* "On the other hand, courts have refused to find standing based on naked averments that an individual's communications must have been seized because the government operates a data collection program and the individual utilized the service of a large telecommunications company." *Id.*

Applying the pleading standard it had gleaned from *Clapper*, *ACLU*, *Jewel*, and *Klayman*, the District Court began by noting that the facts underpinning Schuchardt's allegations were drawn almost entirely from "media reports and publicly available information." *Id.* Accordingly, his lawsuit fell "squarely within the second category" of cases, *i.e.*, those brought by plaintiffs who lacked Article III standing. *Id.* Furthermore, Schuchardt "had identified no facts from which the Court reasonably might infer that his own communications have been targeted, seized, or stored." *Id.* As such, he was "indistinguishable from every other American subscribing to the services of a major telephone and/or internet service provider." *Id.* His "only discernible distinction [was] his heightened personal-interest in the subject," which was "insufficient to confer standing." *Id.* (citing *Schlesinger*

v. Reservists Comm. to Stop the War, 418 U.S. 208, 220 (1974)).

III

The District Court had jurisdiction over Schuchardt's claims under 28 U.S.C. § 1331, as well as the inherent power to ascertain its own jurisdiction. *See Arbaugh v. Y. & H. Corp.*, 546 U.S. 500, 514 (2006). We have jurisdiction under 28 U.S.C. § 1291. *See also Bender v. Williamsport Area Sch. Dist.*, 475 U.S. 534, 541–42 (1986). We review de novo the District Court's order dismissing Schuchardt's second amended complaint. *See Fleisher v. Standard Ins. Co.*, 679 F.3d 116, 120 (3d Cir. 2012).

At the outset, we note that there is an important distinction between "facial" and "factual" attacks on subject matter jurisdiction raised in a motion under Rule 12(b)(1) of the Federal Rules of Civil Procedure. *See Mortensen v. First Fed. Sav. & Loan*, 549 F.2d 884, 891 (3d Cir. 1977). In a facial attack, we review only "the allegations of the complaint and documents referenced therein and attached thereto, in the light most favorable to the plaintiff." *Gould Elecs. v. United States*, 220 F.3d 169, 176 (3d Cir. 2000). If, however, the defendant contests the pleaded jurisdictional facts, "the court must permit the plaintiff to respond with evidence supporting jurisdiction." *Id.* at 177 (citing *Int'l Ass'n of Machinists & Aerospace Workers v. Nw. Airlines, Inc.*, 673 F.2d 700, 711–12 (3d Cir. 1982)). "The court may then determine jurisdiction by weighing the evidence presented by the parties," but "if there is a dispute of a material fact, the court must

conduct a plenary trial on the contested facts prior to making a jurisdictional determination." *Id.*

It is clear from the record in this case that the District Court viewed the Government's motion to dismiss as a facial attack on its jurisdiction. The Court's analysis focused solely on Schuchardt's second amended complaint; it did not consider any extrinsic facts proffered by the Government, including, for example, the nature of PRISM collection as determined by the PCLOB. *See Schuchardt*, 2015 WL 5732117, at *5–7. Accordingly, our review of the District Court's order will accept as true all of Schuchardt's plausible allegations, and draw all reasonable inferences in his favor.[5]

IV

We begin our analysis with first principles. As a plaintiff seeking to invoke federal jurisdiction, Schuchardt bears the burden of establishing each element of his standing to sue under Article III. *See Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). "[T]he irreducible constitutional minimum of standing contains three elements." *Id.* at 560.

> First, the plaintiff must have suffered an injury in fact—an invasion of a legally protected

---

[5] Schuchardt has also challenged on appeal the District Court's order denying his request for a preliminary injunction, a decision the Court rendered more than six months before granting the Government's motion to dismiss. Because Schuchardt failed to identify that unrelated order in his notice of appeal, however, we lack jurisdiction to consider his arguments. *See Sulima v. Tobyhanna Army Depot*, 602 F.3d 177, 184 (3d Cir. 2010).

> interest which is (a) concrete and particularized, and (b) actual or imminent, not conjectural or hypothetical. Second, there must be a causal connection between the injury and the conduct complained of—the injury has to be fairly traceable to the challenged action of the defendant, and not the result of the independent action of some third party not before the court. Third, it must be likely, as opposed to merely speculative, that the injury will be redressed by a favorable decision.

Id. at 560–61 (internal quotation marks, citations, and alterations omitted).

Because a motion to dismiss raising a facial attack on subject matter jurisdiction relies solely on the pleadings, "we apply the same standard of review we use when assessing a motion to dismiss for failure to state a claim." *See Finkelman v. NFL*, 810 F.3d 187, 194 (3d Cir. 2016). "Thus, to survive a motion to dismiss for lack of standing, a plaintiff must allege facts that affirmatively and plausibly suggest that [he] has standing to sue." *Id.* (internal quotation marks omitted). That is, the plaintiff must "plausibly allege facts establishing each constitutional requirement." *Hassan v. City of New York*, 804 F.3d 277, 289 (3d Cir. 2015); *see also Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1547 (2016).

Against this doctrinal backdrop, Schuchardt's Article III standing turns on two inquiries. First, were his allegations sufficiently "particularized" to demonstrate that he suffered a discrete injury? *See Lujan*, 504 U.S. at 560. Second, were those facts

pleaded with enough detail to render them plausible, "well-pleaded" allegations entitled to a presumption of truth? *See Ashcroft v. Iqbal*, 556 U.S. 662, 681 (2009); *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 554 (2007). We address each inquiry in turn.

A

A "particularized" Article III injury is one that "affect[s] the plaintiff in a personal and individual way." *In re Schering Plough Corp. Intron/Temodar Consumer Class Action*, 678 F.3d 235, 245 (3d Cir. 2012) (quoting *Lujan*, 504 U.S. at 560 n.1). That putative litigants must suffer in some discrete and personal fashion ensures, first, that "the legal questions presented . . . will be resolved, not in the rarified atmosphere of a debating society, but in a concrete factual context conducive to a realistic appreciation of the consequences of judicial action," and, second, that our "exercise of judicial power" shows "[p]roper regard for the . . . other two coequal branches of the Federal Government." *Valley Forge Christian Coll. v. Ams. United for the Separation of Church & State, Inc.*, 454 U.S. 464, 471–74 (1982). These two concerns—respect for the judicial role and separation of powers—are most salient when courts are asked "to review actions of the political branches in the fields of intelligence gathering and foreign affairs." *Clapper*, 133 S. Ct. at 1147.

The Supreme Court has identified a subset of cases in which plaintiffs routinely fail to demonstrate particularized injury because they present only "generalized grievances," *i.e.*, injuries that are "undifferentiated and 'common to all members of the

public.'" *Lujan*, 504 U.S. at 573–74 (quoting *United States v. Richardson*, 418 U.S. 166, 177 (1974)). "Whether styled as a constitutional or prudential limit on standing, the Court has sometimes determined that where large numbers of Americans suffer alike, the political process, rather than the judicial process, may provide the more appropriate remedy." *Fed. Election Comm'n v. Akins*, 524 U.S. 11, 23 (1998). Such cases often involve government action directed at the public at large, or harms that by their nature touch upon interests that are widely shared. *See, e.g.*, *Schlesinger*, 418 U.S. at 217 (plaintiffs asserting violation of the Incompatibility Clause by members of Congress also serving in the armed reserves lacked standing because their only interest was "to have the Judicial Branch compel the Executive Branch to act in conformity with the [law] . . . an interest shared by all citizens"); *Sierra Club v. Morton*, 405 U.S. 727, 734–36 (1972) (association challenging development of national park lacked standing based on alleged "special interest" in conservation).

Nevertheless, "[t]he fact that an injury may be suffered by a large number of people does not of itself make that injury a nonjusticiable generalized grievance." *Spokeo*, 136 S. Ct. at 1548 n.7. "The victims' injuries from a mass tort, for example, are widely shared, to be sure, but each individual suffers a particularized harm." *Id.*; *see also Massachusetts v. EPA*, 549 U.S. 497, 526 n.24 (2007) ("[S]tanding is not to be denied simply because many people suffer the same injury. . . . To deny standing to persons who are in fact injured simply because many others are also injured, would mean that the most injurious and

widespread Government actions could be questioned by nobody."). And although particularity and concreteness are distinct elements constituting injury in fact, *see Spokeo*, 136 S. Ct. at 1545, the Supreme Court has also observed that the "judicial language" accompanying generalized grievances "invariably appears in cases where the harm is not only widely shared, *but also of an abstract or indefinite nature*—for example, harm to the 'common concern for obedience to law.'" *Akins*, 524 U.S. at 23 (emphasis added).

We applied these principles in a recent case involving allegations of government surveillance. In *Hassan v. City of New York*, the plaintiffs claimed that the New York City Police Department (NYPD) had implemented a program "to monitor the lives of Muslims, their businesses, houses of worship, organizations, and schools." 804 F.3d at 285. The program allegedly entailed "widespread" photo and video surveillance of "organizations and businesses . . . visibly or openly affiliated with Islam," and the infiltration of "Muslim-affiliated" groups with informants and undercover police officers. *Id.* at 285–86. The information gathered was compiled into a series of reports "document[ing] . . . American Muslim life in painstaking detail." *Id.* (internal quotation marks omitted). The *Hassan* plaintiffs discovered the program after some of these reports became "widely publicized," and they asserted that the fallout required them to alter their ordinary day-to-day conduct. *See id.* at 287–88.

We held that the plaintiffs' allegations in *Hassan* were sufficient to demonstrate particularized injury

under Article III. After determining that they had asserted "an invasion of a legally protected interest"—"[t]he indignity of being singled out [by the government] for special burdens on the basis of one's religious calling"—we observed that the particularized nature of an injury does not turn on the number of persons that may claim it. *Id.* at 289. "[T]hat hundreds or thousands (or even millions) of other persons may have suffered the same injury does not change the individualized nature of the asserted rights and interests at stake." *Id.* at 291 (citing *Akins*, 524 U.S. at 24). "Harm to all—even in the nuanced world of standing law—cannot be logically equated with harm to no one." *Id.* And with regard to allegations of widespread government surveillance, we stated that because the plaintiffs had "claim[ed] to be the very targets of the allegedly unconstitutional surveillance, they [were] unquestionably 'affect[ed] . . . in a personal and individual way.'" *Id.* (quoting *Lujan*, 504 U.S. at 560 n.1).

Like the plaintiffs in *Hassan*, Schuchardt has alleged a program of government surveillance that, though universal in scope, is unmistakably personal in the purported harm. His second amended complaint describes PRISM as a dragnet that collects "all or substantially all of the e-mail sent by American citizens by means of several large internet service providers." App. 82. The collected information allegedly encompasses Schuchardt's personal communications, and includes not only the kind of intensely private details that one could reasonably expect to find in the email accounts of most Americans—"bank account numbers; credit card numbers; passwords for financial

data; [and] health records"—but also data influenced by Schuchardt's personal circumstances, namely "trade secrets" and "communications with clients of Schuchardt's law firm, which are privileged and confidential under applicable law." App. 96.

The Government strenuously disputes the plausibility of Schuchardt's assertion that PRISM collects "all or substantially all of the e-mail sent by American citizens," and we address that dispute in detail below. But putting aside for the moment the question of whether Schuchardt's allegations concerning PRISM are entitled to a presumption of truth, the consequences that he identifies as flowing from the Government's alleged dragnet are undoubtedly personal to him insofar as he has a constitutional right to maintain the privacy of his personal communications, online or otherwise. *See Plumhoff v. Rickard*, 134 S. Ct. 2012, 2022 (2014) ("Fourth Amendment rights are personal rights . . . which may not be vicariously asserted." (quoting *Alderman v. United States*, 394 U.S. 165, 174 (1969)). That interest is neither indivisibly abstract nor indefinite, *see Warshak v. United States*, 631 F.3d 266, 288 (6th Cir. 2010), and the fact that a large percentage of the population may share a similar interest "does not change [its] individualized nature" because Schuchardt's allegations make clear that he is among the persons that are the "very targets of the allegedly unconstitutional surveillance." *Hassan*, 804 F.3d at 291; *cf. Riley v. California*, 134 S. Ct. 2473, 2484–85 (2014) (extending the warrant requirement to searches of cellular phones, "which are now such a pervasive and insistent part of daily life that the

proverbial visitor from Mars might conclude they were an important feature of human anatomy").

B

Having determined that Schuchardt's allegations stated a particularized injury under Article III, we now consider whether those allegations should be credited as true for the purpose of resolving the Government's jurisdictional objection. As noted previously, the District Court construed the Government's motion to dismiss as a facial attack on its subject matter jurisdiction. As a result, we must accept Schuchardt's allegations as true, with the important caveat that the presumption of truth attaches only to those allegations for which there is sufficient "factual matter" to render them "plausible on [their] face." *Iqbal*, 556 U.S. at 679. Conclusory assertions of fact and legal conclusions are not entitled to the same presumption. *See id.*; *see also Twombly*, 550 U.S. at 57; *Connelly v. Lane Constr. Corp.*, 809 F.3d 780, 787 (3d Cir. 2016) ("Under the pleading regime established by *Twombly* and *Iqbal*, a court reviewing the sufficiency of a complaint must . . . identify allegations that, 'because they are no more than conclusions, are not entitled to the assumption of truth.'" (quoting *Iqbal*, 556 U.S. at 679)).[6]

---

[6] We have instructed courts to follow a three-step process to determine the sufficiency of a complaint in accordance with *Twombly* and *Iqbal*. "First, [the court] must take note of the elements the plaintiff must plead to state a claim. Second, it should identify allegations that, because they are no more than conclusions, are not entitled to the assumption of truth. Finally, when there are well-pleaded factual allegations, the court should assume their veracity and then determine whether they plausibly

We have recognized that "[t]he plausibility determination is a 'context-specific task that requires the reviewing court to draw on its judicial experience and common sense.'" *See, e.g.*, *Connelly*, 809 F.3d at 786–87 (quoting *Iqbal*, 556 U.S. at 675). At the same time, we have cautioned that the plausibility standard does not impose a heightened pleading requirement, and that Federal Rule of Civil Procedure 8(a) continues to require only a "showing" that the pleader is entitled to relief. *See, e.g.*, *Phillips v. Cty. of Allegheny*, 515 F.3d 224, 233–34 (3d Cir. 2008) ("The [Supreme] Court emphasized . . . that it was neither demanding a heightened pleading of specifics nor imposing a probability requirement.")). Indeed, although *Twombly* and *Iqbal* emphasized the plaintiff's burden of pleading sufficient "factual matter," the Supreme Court also expressly "disavow[ed]" the requirement that a plaintiff plead "specific facts." *Boykin v. KeyCorp*, 521 F.3d 202, 215 (2d Cir. 2008) (quoting *Twombly*, 550 U.S. at 569, and *Erickson v. Pardus*, 551 U.S. 89, 93 (2007)).

Implicit in the notion that a plaintiff need not plead "specific facts" to survive a motion to dismiss is that courts cannot inject evidentiary issues into the plausibility determination.[7] *See Twombly*, 550 U.S. at

---

give rise to an entitlement to relief." *Connelly*, 809 F.3d at 787 & n.4 (internal citations, quotations marks, and original modifications omitted).

[7] The "evidentiary issues" to which we refer are distinct from the question of what documents may be considered in resolving a motion to dismiss applying the standard of review under Rule

556 ("[A] well-pleaded complaint may proceed even if it strikes a savvy judge that actual proof of those facts is improbable."). This includes the weighing of facts or the requirement that a plaintiff plead "specific facts" beyond those necessary to state a valid claim. *See id.* at 573 n.8 ("[W]hen a complaint adequately states a claim, it may not be dismissed based on a district court's assessment that the plaintiff will fail to find evidentiary support for his allegations or prove his claim to the satisfaction of the factfinder."). The same logic precludes a court from rejecting pleaded facts based on some blanket exclusion of evidence. *See Ricciuti v. New York City Transit Auth.*, 941 F.2d 119, 124 (2d Cir. 1991). "A contrary rule would confuse the principles applicable to a motion to dismiss with those governing a motion for summary judgment." *Campanella v. Cty. of Monroe*, 853 F. Supp. 2d 364, 378 (W.D.N.Y. 2012); *see also Whitney v. Guys, Inc.*, 700 F.3d 1118, 1128–29 (8th Cir. 2012).

Accordingly, although it is unclear whether the District Court applied a heightened pleading standard

---

12(b)(6), or, as relevant here, addressing a facial challenge to subject matter jurisdiction under Rule 12(b)(1). The general rule for determining the scope of the pleadings in this scenario is that a district court "may consider *only* the allegations contained in the pleading[s] to determine [their] sufficiency," but is permitted to consider "document[s] *integral to or explicitly relied* upon in the complaint," and "any undisputedly authentic document that a defendant attaches . . . if the plaintiff's claims are based on the document," without converting the motion into one for summary judgment. *See In re Asbestos Prods. Liability Litig. (No. VI)*, 822 F.3d 125, 133 & n.7 (3d Cir. 2016) (internal citations and quotation marks omitted). *See generally* 5B Charles Alan Wright & Arthur R. Miller, *Federal Practice and Procedure* § 1350 n.1 (3d ed. 2016).

in this case, to the extent that its opinion suggests that Schuchardt's reliance on "media reports and other publicly-available information" was impermissible, we disagree.[8] *See Schuchardt*, 2015 WL 5732117, at *6. Indeed, we held that the plaintiffs in *Hassan* had plausibly pleaded both their standing to sue and claims for relief based on NYPD surveillance reports that the plaintiffs had discovered only *after* they had been "widely publicized." *See* 804 F.3d at 287. Similarly, we take the District Court's enumeration of the types of evidence giving rise to the plaintiffs' standing in *Jewel* and *ACLU*—"a leaked FISC order or a detailed insider account"—as merely a suggestion of facts that would have strongly supported the plausibility of Schuchardt's allegations, rather than a requirement that he plead those specific facts. *See* 2015 WL 6732117, at *6. Such limitations on the scope or source of facts that a plaintiff may plead to reach the threshold of plausibility run counter to the longstanding principles animating pretrial dispositions,

---

[8] Despite *Clapper*'s observation that the standing inquiry is "especially rigorous" in matters touching on "intelligence gathering and foreign affairs," 133 S. Ct. at 1147, to our knowledge no court has imposed a heightened pleading standard for cases implicating national security. *See Jewel*, 673 F.3d at 913 ("Article III imposes no heightened standing requirement for the often difficult cases that involve constitutional claims against the executive involving surveillance."). In this appeal, we will assume without deciding that a heightened pleading standard does not apply. *See, e.g.*, *Jones v. Bock*, 549 U.S. 199, 212–13 (2007) (explaining that "courts should generally not depart from the usual practice under the Federal Rules on the basis of perceived policy concerns," including the imposition of a pleading standard more stringent than the "short and plain statement" of the claim under Rule 8).

as set forth in *Twombly* and *Iqbal*, and come close to the weighing of evidence and credibility determinations that are the exclusive province of the factfinder. *See Iqbal*, 556 U.S. at 681 ("It is the conclusory nature of respondent's allegations, rather than their extravagantly fanciful nature, that disentitles them to the presumption of truth."); *Twombly*, 550 U.S. at 556 ("Rule 12(b)(6) does not countenance . . . dismissals based on a judge's disbelief of a complaint's factual allegations." (quoting *Neitzke v. Williams*, 490 U.S. 319, 327 (1989)); *see also Anderson v. Liberty Lobby, Inc.*, 477 U.S. 242, 255 (1986).

The upshot of all this for Schuchardt is that his reliance on news articles and other disclosures concerning PRISM weighs neither in his favor nor against him. Instead, these public reports (and the leaked classified materials accompanying them) are simply part and parcel of the "factual matter" that must be considered in assessing the plausibility of his allegations. We will therefore examine those reports in conjunction with the rest of Schuchardt's pleadings to ascertain whether he plausibly alleged a particularized injury under Article III.

2

Based on our review of the pleadings, the plausibility of Schuchardt's alleged injury—that the Government has been "unlawfully intercepting, accessing, monitoring and/or storing [his] private communications," App. 95—depends on the plausibility of his assertion that PRISM functions as an indiscriminate dragnet which captures "all or substantially all of the e-mail sent by American

citizens." App. 82. Aside from this sweeping allegation, Schuchardt has supplied no facts suggesting how (or why) the Government would have been interested in his online activity. His burden, therefore, was to allege enough "factual matter" to make plausible the Government's virtual dragnet. *Iqbal*, 556 U.S. at 679; *see also Arpaio v. Obama*, 797 F.3d 11, 19 (D.C. Cir. 2015).

Schuchardt pleaded facts drawn from news articles published by the *Guardian*, as well as the leaked and purportedly classified materials from which those articles were derived. As we noted in Part I.B, *supra*, these documents state that the NSA, through PRISM, has obtained "direct" access to the technical facilities of several major internet service providers. App. 53, 84. They indicate specific dates for when those providers granted the Government access, App. 60, and that the degree of access those providers granted enables the Government to query their facilities at will for "real-time interception of an individual's internet activity." App. 66. They also describe the types of activity that may be accessed, encompassing "both the content and metadata of . . . private e-mail communications" sent by those providers on behalf of their subscribers. App. 59, 96. Finally, they claim that the rate of data "[c]ollection is outpacing [the Government's] ability to ingest, process and store [the data] to the 'norms' to which [it has] become accustomed," App. 64, and that the NSA's overriding surveillance goal is to "[c]ollect it [a]ll," App. 61.

By including these factual averments in his second amended complaint, Schuchardt outlined a coherent

and plausible case supporting his PRISM-as-dragnet allegations. First, his alleged facts specify, at least to some degree, the means through which the NSA captures "all or substantially all of the e-mail sent by American citizens," App. 82, namely, by compelling companies that provide email and other internet services to cooperate with the NSA in the collection of their customers' data. Although the technical details of how each company's email service integrates within PRISM's infrastructure are not specified, "on a motion to dismiss, we 'presum[e] that general allegations embrace those specific facts that are necessary to support the claim.'" *Lujan*, 504 U.S. at 561 (quoting *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 781, 889 (1990)). Moreover, according to the NSA itself, PRISM entails data "collection directly from the servers" of these companies, and Schuchardt describes events involving Lavabit, a company that resisted the Government's demands to "install a device on its server which would have provided the [Government] with access to the full content of all e-mail messages for all of Lavabit's . . . customers." *See* App. 53, 84, 87. Thus, the pleaded facts plausibly allege the technical means through which PRISM purportedly achieves a nationwide email dragnet.[9]

---

[9] We do not read the Ninth Circuit's opinion in *Jewel* to suggest a different conclusion. To be sure, the plaintiff in *Jewel* was able to allege "with particularity" that her communications were seized by "focus[ing]" her complaint on interceptions occurring at a specific technical facility operated by a single telecommunications provider. *See* 673 F.3d at 910 (discussing the plaintiff's allegations concerning AT&T's "SG3 Secure Room" and "particular electronic communications equipment" at the company's "Folsom Street" facility in San Francisco). Although the details she alleged were

Second, Schuchardt's allegations are replete with details confirming PRISM's operational scope and capabilities. The exhibits attached to his second amended complaint include a slide from a purported NSA presentation identifying company names and the dates they began cooperating with the agency. Another slide confirms that—consistent with a dragnet capturing "all or substantially all of the e-mail sent by American citizens"—the scale of the data collected by PRISM is so vast that the Government reported difficulty processing it according "to the 'norms' to which [it has] become accustomed." App. 64; *see also* App. 52 (characterizing PRISM as the "SIGAD Used Most in NSA Reporting");[10] App. 61 (indicating the NSA's "New Collection Posture" of "Collect[ing] it All").

Finally, the pleaded facts support Schuchardt's allegation that the scope of PRISM's data collection encompasses his personal email. The NSA presentation identifies specific companies participating in the

---

quite colorful, they differ in degree, not in kind from Schuchardt's averments. In both cases, the parties relied on an insider account of the alleged surveillance program at issue—Schuchardt on a former NSA contractor, and *Jewel* on a former AT&T telecommunications technician. Those insiders in turn have relied either on documentary evidence allegedly produced by the Government itself, or their personal experiences in executing the surveillance program.

[10] SIGAD stands for the term "Signals Intelligence Activity Designator," which "is an alphanumeric designator that identifies a facility used for collecting Signals Intelligence (SIGINT)." Laura K. Donohue, *Section 702 and the Collection of International Telephone and Internet Content*, 38 Harv. J. L. & Pub. Pol'y 117, 119 n.3 (2015).

PRISM program, and indicates that NSA analysts receive the content of emails collected as part of the program. Schuchardt alleged that he uses email services provided by two of those companies—Google and Yahoo—so we need not speculate about whether Schuchardt's own communications were captured because he specified the scope of PRISM's dragnet with enough "factual matter" to make additional inferential leaps unnecessary. *See Klayman*, 800 F.3d at 559 (opinion of Brown, J.) (permitting the inference that the bulk telephone metadata program under Section 215 encompassed the plaintiff's communications in light of facts alleging "the government's efforts to 'create a *comprehensive* metadata database.'").

3

The Government raises three principal arguments challenging the plausibility of Schuchardt's PRISM allegations. First, it argues that *Clapper* and its application by the D.C. Circuit in *Klayman* require us to find his allegations implausible. We disagree.

Two aspects of *Clapper* distinguish it from this case. First, because the *Clapper* plaintiffs raised a facial constitutional challenge to Section 702 on the day the statute was enacted, they pleaded only *prospective* injury, *i.e.*, "potential future surveillance." *See* 133 S. Ct. at 1150. And because that "potential" relied on a "speculative chain of possibilities," the Supreme Court concluded that they had failed to satisfy the imminence and traceability elements of injury-in-fact under Article III. Here, in contrast, Schuchardt's alleged injury has already occurred insofar as he claims the NSA seized his emails. It is therefore not surprising that the

Government has been unable to formulate an analogous "speculative chain" that would doom Schuchardt's constitutional standing.

Another critical distinction between this case and *Clapper* is that the district court entered summary judgment, a procedural posture that required the plaintiffs to identify a triable issue of material fact supported by an evidentiary record. *See id.* at 1146, 1149. In contrast, Schuchardt sought to avoid dismissal in a facial jurisdictional challenge raised under Rule 12(b)(1), which requires him only to state a plausible claim, a significantly lighter burden. This distinction in the standard of review is also reflected in cases concerning national security surveillance from our sister courts. *Compare ACLU*, 785 F.3d at 800 (plaintiffs had standing on motion to dismiss); *Jewel*, 673 F.3d at 906–07 (same), *with Klayman*, 800 F.3d at 568 (opinion of Williams, J.) (plaintiffs lacked standing to pursue preliminary injunction because there was no "substantial likelihood" that they could establish injury-in-fact, observing that summary judgment imposes a "*lighter* burden" than the "substantial likelihood of success" necessary to obtain a preliminary injunction); *ACLU v. NSA*, 493 F.3d 644, 650–51, 667–70 (6th Cir. 2007) (plaintiffs failed to establish injury-in-fact on summary judgment because they had "no evidence" on various points of causation). Here, Schuchardt has gone beyond mere allegations to survive a motion to dismiss by creating a limited evidentiary record to support his allegations.

The Government's reliance on *Klayman* is also misplaced. There, the D.C. Circuit vacated the district

court's preliminary injunction, holding that the plaintiffs had failed to demonstrate a substantial likelihood of success on the merits. *See* 800 F.3d at 561. However, the panel split on the issue of the plaintiffs' standing, and also disagreed on whether to remand the case for further proceedings or outright dismissal. *See id.* at 564 (opinion of Brown, J.) (plaintiffs had satisfied "the bare requirements of standing," remanding for jurisdictional discovery); *id.* at 565 (opinion of Williams, J.) (plaintiffs lacked standing to seek preliminary injunction, remanding for jurisdictional discovery); *id.* at 569 (opinion of Sentelle, J.) (plaintiffs lacked standing *vel non*, remanding with order to dismiss). Under these circumstances, it seems clear to us that *Klayman*'s persuasive force is minimized by its splintered reasoning, different procedural posture, and the fact that the D.C. Circuit addressed itself to a now-defunct surveillance program authorized by a separate provision of FISA. Accordingly, neither *Clapper* nor *Klayman* supports the Government in this case.

Second, the Government contends that Schuchardt's allegations "say at most that the government may have the *capability* to seize and store *most* electronic communications," but "[t]hey do not say that the government is searching or seizing most, let alone all, e-mail." Gov't Br. 21. We agree that Schuchardt's alleged facts—even if proven—do not conclusively establish that PRISM operates as a dragnet on the scale he has alleged. The language of the leaked materials Schuchardt relies on is imprecise. The use of the term "direct" in the NSA's presentation could mean, for example, that the Government has complete discretion to search all electronic information held by

a company participating in PRISM at will; this would certainly be consistent with the "real-time" interception capability that the NSA allegedly possesses, and could qualify as an unconstitutional "seizure" of all information stored on the company's servers. On the other hand, "direct" could mean that the Government merely has the legal authority to compel participating companies to turn over "communications that may be of foreign-intelligence value because they are . . . associated with the e-mail addresses that are used by suspected foreign terrorists." Gov't Br. 22. In that scenario, it is implausible that Schuchardt's communications would be targeted by PRISM.

At this early stage of litigation, however, Schuchardt is entitled to any inference in his favor that may be "reasonably" drawn from his pleaded facts. *See, e.g.*, *King Drug Co. of Florence, Inc. v. SmithKline Beecham Corp.*, 791 F.3d 388, 398 n.11 (3d Cir. 2015) (citing *Iqbal*, 556 U.S. at 678–79). And as we have explained, the inference that PRISM "collects all or substantially all of the e-mail sent by American citizens," App. 82, is one supported by his pleaded "factual matter." Accordingly, in this procedural posture, we cannot accept the Government's preferred inference.

Finally, the Government disputes the notion that PRISM is a dragnet, *i.e.*, that it is "based on the indiscriminate collection of information in bulk." *See* Gov't Br. 22 (quoting PCLOB Report at 111). According to the Government, "the program consists entirely of targeting specific persons that may be of foreign-intelligence value because they are, for example,

associated with the e-mail addresses that are used by suspected foreign terrorists." *Id.* Under this view, to intercept communications using PRISM:

> Analysts first identify a non-U.S. person located outside the United States who is likely to communicate certain types of foreign intelligence information, such as an individual who belongs to a foreign terrorist organization or facilitates its activities. Analysts also attempt to identify a means by which this foreign target communicates, such as an e-mail address, or a telephone number; any such address, number, or other identifier is known as a "selector." PRISM collection occurs when the government obtains from telecommunications providers . . . communications sent to or from specified selectors.

Gov't Br. 6–7 (internal citations omitted).

Several commentators[11] and the few courts[12] that have examined PRISM appear to agree with the Government's view of the program's "targeted" nature. So too has the PCLOB, whose report on PRISM the

---

[11] *See, e.g.*, Donohue, *supra* note 8, at 119 n.2 ("Once foreign intelligence acquisition has been authorized under Section 702, the government sends written directives to electronic communication service providers compelling their assistance in the acquisition of communications." (quoting PCLOB Report at 7)); Nathan Alexander Sales, *Domesticating Programmatic Surveillance: Some Thoughts on the NSA Controversy*, 10 I/S: J. L. & Pol'y for Info. Soc'y 523, 526 (2014) ("[In] PRISM . . . the NSA targets specific non-Americans who are reasonably believed to be located outside the country, and also engages in bulk collection of some foreign-to-foreign communications that happen to be passing through telecommunications infrastructure in the United States."). The *Washington Post* also amended its initial report on PRISM to suggest that "imprecision on the part of the NSA" in the wording of its presentation left open the possibility that PRISM collection still required the agency to request materials from the participating companies, rather than directly from the companies' servers. *See* Jonathan Hall, *Washington Post Updates, Hedges on Initial PRISM Report*, Forbes (June 7, 2013, 9:08 PM), https://perma.cc/7L6A-H22D.

[12] *See, e.g.*, *United States v. Hasbajrami*, 2016 WL 1029500, at *6 (E.D.N.Y. Mar. 8, 2016) ("In PRISM collection, the government identifies the user accounts it wants to monitor and sends a 'selector'—a specific communications facility, such as a target's email address or telephone number—to the relevant communications service provider. A government directive then compels the communications service provider to give it communications sent to or from that selector (*i.e.*, the government 'tasks' the selector)." (internal citations omitted)); *Wikimedia Found. v. NSA*, 143 F. Supp. 3d 344, 348–49 (D. Md. 2015) ("Under a surveillance program called 'PRISM,' U.S.-based Internet Service Providers furnish the NSA with electronic communications that contain information specified by the NSA.").

Government has asked us to consider. *See* PCLOB Report at 33–34. These authorities are substantial, and if correct, would tend to undermine Schuchardt's ability to show that his own electronic communications were seized by the PRISM program.

The problem for the Government at this stage is that the scope of materials that a court may consider in evaluating a facial jurisdictional challenge raised in a motion under Rule 12(b)(1) is not unconstrained. As with motions under Rule 12(b)(6), the court is limited to the four corners of the complaint, "document[s] *integral to or explicitly relied* upon in the complaint," and "any undisputedly authentic document that a defendant attaches . . . if the plaintiff's claims are based on the document." *In re Asbestos Prods. Liability Litig. (No. VI)*, 822 F.3d 125, 133 & n.7 (3d Cir. 2016) (quoting *In re Burlington Coat Factory Sec. Litig.*, 114 F.3d 1410, 1426 (3d Cir. 1997)). Schuchardt's pleadings are in no way "based on" any countervailing authorities that support the Government's position, nor are those authorities integral to or explicitly relied upon by his complaint—accordingly, we must ignore their persuasive value, whatever it may be, at this stage of the litigation. *See Gould Elecs.*, 220 F.3d at 176. Likewise, insofar as the Government's arguments present new information disagreeing with the factual premises underlying Schuchardt's claims, we cannot consider them in this *facial* jurisdictional challenge, the sole purpose of which is to test the legal sufficiency of the plaintiff's jurisdictional averments. Instead, disagreements concerning jurisdictional facts should be presented in a *factual* challenge, at which time the court, after allowing the plaintiff "to respond with

evidence supporting jurisdiction," may fully adjudicate the parties' dispute, including the resolution of any questions of fact. *Id.* at 177.

V

Our decision today is narrow: we hold only that Schuchardt's second amended complaint pleaded his standing to sue for a violation of his Fourth Amendment right to be free from unreasonable searches and seizures. This does not mean that he *has* standing to sue, as the Government remains free upon remand to make a factual jurisdictional challenge to Schuchardt's pleading. In anticipation of such a challenge, we provide the following guidance to the District Court on remand.

Schuchardt has suggested that he is entitled to jurisdictional discovery. *See* Transcript of Oral Argument at 40–41, *Schuchardt v. Obama*, No. 15-3491 (3d Cir. May 17, 2016). We leave that question to the District Court's discretion with the caveat that "jurisdictional discovery is not available merely because the plaintiff requests it." *Lincoln Benefit Life Ins. Co. v. AEI Life, LLC*, 800 F.3d 99, 108 n.38 (3d Cir. 2015). Jurisdictional discovery is not a license for the parties to engage in a "fishing expedition," *id.*, and that fact is particularly true in a case like this one, which involves potential issues of national security. In this very context, the Supreme Court has cautioned that jurisdictional discovery—even if conducted *in camera*—cannot be used to probe the internal (and most likely classified) workings of the national security apparatus of the United States. *See Clapper*, 131 S. Ct. at 1149 n.4 ("[T]his 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."). For that reason, the District Court should take care to circumscribe the scope of discovery and any *ex parte* and *in camera* procedures to only the factual questions necessary to determine its jurisdiction.[13]

Finally, nothing in our opinion should be construed to preclude the Government from raising any applicable privileges barring discovery—including the state secrets doctrine—or to suggest how the District Court should rule on any privilege the Government may choose to assert. *See United States v. Reynolds*, 345 U.S. 1, 10 (1953).

* * *

For the stated reasons, we will vacate the District Court's order dismissing Schuchardt's second amended complaint and remand for proceedings consistent with this opinion.

---

[13] For example, the linchpin of Schuchardt's standing is his allegation that PRISM collects "all or substantially all of the e-mail sent by American citizens." The District Court may wish to consider what discovery is necessary for it to adjudicate the veracity of that allegation while permitting Schuchardt an adequate evidentiary response. *See also Jewel v. NSA*, 2015 WL 545925, at *4 (N.D. Cal. Feb. 10, 2015) (holding that plaintiffs had failed to establish their standing to challenge Upstream, another putative NSA electronic surveillance program, because "the evidence at summary judgment [was] insufficient to establish that the Upstream collection process operates in the manner in which Plaintiffs allege[d] it does").

UNITED STATES COURT OF APPEALS
FOR THE THIRD CIRCUIT

No. 15-3491

[Filed October 5, 2016]

ELLIOTT J. SCHUCHARDT, individually and doing business as the Schuchardt Law Firm, on behalf of himself and all others similarly situated, Appellant	)
v.	)
PRESIDENT OF THE UNITED STATES; DIRECTOR OF NATIONAL INTELLIGENCE; DIRECTOR OF THE NATIONAL SECURITY AGENCY AND CHIEF OF THE CENTRAL SECURITY SERVICE; DIRECTOR OF THE FEDERAL BUREAU OF INVESTIGATION	)

Appeal from the United States District Court
for the Western District of Pennsylvania
(W.D. Pa. No. 2-14-cv-00705)
District Judge: Honorable Cathy Bissoon

Argued: May 17, 2016

Before: SMITH, *Chief Judge*, HARDIMAN, and NYGAARD, *Circuit Judges*.

JUDGMENT

This cause came to be considered on the record from the United States District Court for the Western District of Pennsylvania and was argued on May 17, 2016. On consideration whereof, it is now hereby

ORDERED and ADJUDGED by this Court that the order of the United States District Court for the Western District of Pennsylvania entered on September 30, 2015, be and the same is hereby VACATED and REMANDED. All of the above in accordance with the Opinion of this Court.

No costs shall be taxed.

ATTEST:

s/Marcia M. Waldron
Clerk

Dated: October 5, 2016

APPENDIX D

IN THE UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF PENNSYLVANIA

Civil Action No. 14-705

Judge Cathy Bissoon

[Filed September 30, 2015]

ELLIOTT SCHUCHARDT,	)
	)
Plaintiff,	)
v.	)
	)
BARACK H. OBAMA, *et al.*,	)
	)
Defendants.	)
	)

MEMORANDUM AND ORDER

I. MEMORANDUM

Defendants' Motion to Dismiss (Doc. 20) will be granted.

INTRODUCTION

This action is one of several lawsuits arising from recent public revelations that the United States government, through the National Security Agency ("NSA"), and in conjunction with various

telecommunications and internet companies, has been collecting data concerning the telephone and internet activities of American citizens located within the United States. The Plaintiff, Elliott J. Schuchardt ("Schuchardt"), alleges that the NSA's bulk data collection programs violate the Fourth Amendment to the United States Constitution by allowing the government to seize and search records related to the telephone and internet activities of ordinary American citizens without demonstrating probable cause. He also asserts claims based on the First Amendment, the Foreign Intelligence Surveillance Act ("FISA") and Pennsylvania common law. He seeks declaratory and injunctive relief as well as civil liability pursuant to 18 U.S.C. § 1810.

BACKGROUND

In order to properly contextualize the factual claims in this litigation, a brief overview of several pertinent statutes is warranted. In 1978, Congress enacted the Foreign Intelligence Surveillance Act, 50 U.S.C. §§1801 *et seq.* ("FISA"), to "authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes." Clapper v. Amnesty Int'l USA, -- U.S. --, 133 S. Ct. 1138, 1143 (2013). FISA provided a procedure for the federal government to legally obtain domestic electronic surveillance related to foreign targets, *see* 50 U.S.C. §§ 1804(a)(3) & 1805(a)(2), and created an Article III court – the Foreign Intelligence Surveillance Court ("FISC") – with jurisdiction "to hear applications for and grant orders approving" such surveillance. 50 U.S.C. §1803(a)(1).

In the wake of the terrorist attacks of September 11, 2011, Congress passed the USA PATRIOT Act, Pub. L. No. 107-56, § 215, which, *inter alia*, empowered the FBI to seek authorization from the FISC to "require[e] the production of any tangible things (including books, records, papers, documents, and other items) for an investigation . . . to protect against international terrorism." 50 U.S.C. 1861(a)(1). Since 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." See Obama v. Klayman, -- F.3d --, 2015 WL 5058403 (D.C. Cir. Aug. 28, 2015) ("Klayman II").

In 2008, Congress amended FISA by way of the FISA Amendments Act ("FAA"), Pub. L. No. 110-261 (2008). The pertinent FAA provision, Section 702 of FISA, 50 U.S.C. § 1881a, "supplement[ed] pre-existing FISA authority by creating a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting . . . non-U.S. persons located abroad." Amnesty Int'l, 133 S. Ct. at 1144. The government relies upon the authority granted by Section 702 to collect internet data and communications through a program called "PRISM." 2d Am. Compl. (Doc. 19) ¶¶ 33, 35.

American citizens first learned of the government's bulk data collection programs through a series of articles published in *The Guardian*, a British

newspaper, in June 2013. Id. Each article relied on leaked documents provided by a former NSA government contractor, Edward Snowden. Id. ¶¶ 24-27, 33-39. The first of these articles, published on June 5, 2013, revealed a leaked order from the FISC directing Verizon Business Network Services, Inc. ("Verizon Business") to produce "call detail records or 'telephony metadata'" to the NSA for all telephone calls made through its systems within the United States (including entirely-domestic calls). Id. ¶ 33. Shortly thereafter, the government acknowledged that the FISC order was genuine and that it was part of a broader program of bulk collection of telephone metadata. Id. ¶ 34; ACLU v. Clapper, 785 F.3d 787, 796 (2d Cir. 2015).

The following day, June 6, 2013, *The Guardian* published a second article detailing the manner in which the PRISM collection program was used to intercept, access and store e-mail and other internet data created by United States citizens using large internet companies, such as Yahoo, Google, Facebook, Dropbox and Apple. Id. ¶¶ 35-38. According to the leaked documents, the government began collecting information from, *inter alia*, Yahoo on March 12, 2008; from Google on January 14, 2009; from Facebook on June 3, 2009; and from Apple in October 2012. Id. ¶ 39. Discussing the scope of the government's data collection abilities, Snowden, in a series of public statements and interviews, averred that he could search, seize, and read anyone's electronic communications at any time from his desk during his time working with the NSA. Id. ¶¶ 45-46.

Since those revelations, several former NSA employees and whistleblowers have stepped forward to supply further details concerning the scope and breadth of the government's data collection programs.[1] William Binney, a former senior employee of the NSA, stated that the NSA used a computer program to collect and search domestic internet traffic, a process known as "data-mining." Id. ¶¶ 9, 19. Mark Klein, a former AT&T technician, revealed that the NSA was copying e-mail communications on AT&T's network by means of a secret facility set up in San Francisco. Id. ¶ 13. Thomas Drake, another NSA employee, asserted that the NSA has been, or may be, obtaining the ability to seize and store "most electronic communications." Id. ¶ 20. A third former NSA employee, Kirk Wiebe, corroborated the allegations made by Drake and Binney. Id. ¶ 21.

Based on the averments above, as well as various public interviews conducted by Snowden, Schuchardt alleges that the NSA is collecting and storing "massive quantities of e-mail and other data created by United States citizens." Id. ¶ 36. Because he utilizes several major internet and telecommunications companies – including Gmail, Google, Yahoo, Dropbox, Facebook and Verizon Wireless – Schuchardt contends that the government must, therefore, be "unlawfully intercepting, accessing, monitoring and/or storing the private communications of the Plaintiff, made or stored through such services." Id. ¶¶ 86-87. This presumption

---

[1] Schuchardt has borrowed the majority of his allegations from affidavits filed in another lawsuit, Jewel v. N.S.A., 2015 WL 545925 (N.D. Cal. Feb. 10, 2015).

underpins each of Plaintiff's claims, and he purports to represent a "nationwide class" of "American citizens" similarly-situated. Id. at ¶ 76.

ANALYSIS

Resolution of the instant Motion turns entirely on the issue of standing. In order to establish standing to sue, a plaintiff must show that he has suffered a "concrete and particularized" injury. Lujan v. Defenders of Wildlife, 504 U.S. 555, 560-61 (1992). For an injury to be sufficiently particularized, the plaintiff must allege "such a personal stake in the outcome of the controversy as to warrant *his* invocation of federal-court jurisdiction." Summers v. Earth Island Inst., 555 U.S. 488, 493 (2009) (internal quotations omitted) (emphasis in original). An abstract, generalized grievance that is "common [to] all members of the public" will not suffice. Schlesinger v. Reservists Comm. to Stop the War, 418 U.S. 208, 220 (1974).

The crux of the government's Motion is that Schuchardt lacks standing because he has not plausibly alleged that the government has ever collected any of *his* communications. In other words, even if data-collection has occurred, Schuchardt has provided no facts demonstrating that he is "among the injured." Lujan, 504 U.S. at 563.

Several recent decisions have addressed the issue of standing in the context of the government's bulk data-collection programs. In Amnesty International v. Clapper, the United States Supreme Court addressed a challenge to the constitutionality of Section 702 brought by a group of plaintiffs who alleged that their

communications were likely among those intercepted because they regularly communicated with foreign persons who were probable targets of government surveillance. Amnesty Int'l., 133 S. Ct. at 1145. Although the plaintiffs had no specific knowledge as to how the government's targeting practices worked, they provided evidence that: they had engaged in communications that fell within the purview of Section 702; that the government had a strong motive to intercept those communications because of the subject matter and identities involved; that the government had already intercepted large numbers of calls and emails involving a specific individual who communicated regularly with the plaintiffs; and that the government had the capacity to intercept the aforementioned communications. Id. at 1157-59. The Court held that these allegations were inadequate to establish standing because they relied on a "speculative chain of possibilities" and displayed "no actual knowledge" as to whether the plaintiffs ever were specifically targeted. Id. at 1148.[2]

In ACLU v. Clapper, a group of current and former Verizon Business customers challenged the government's data collection program based on several FISC orders that had been declassified by the government. Clapper, 785 F.3d 787, 796 (2d Cir. 2015). The Court of Appeals for the Second Circuit concluded that the plaintiffs had standing because the government's "own orders demonstrate[ed] that

---

[2] Unlike the instant case, Amnesty International did not involve allegations that the government has relied on Section 702 to collect and store entirely-domestic communications.

[plaintiffs'] call records are indeed among those collected as part of the telephone metadata program." Id. at 801. The court observed:

> [Plaintiffs'] alleged injury requires no speculation whatsoever as to how events will unfold under § 215 – [plaintiffs'] records (among those of numerous others) have been targeted for seizure by the government; the government has used the challenged statute to effect that seizure; the orders have been approved by the FISC; and the records have been collected.

Id. at 801-802.

The Court of Appeals for the Ninth Circuit reached the same conclusion in Jewel v. National Security Agency, a challenge to the NSA's bulk data-collection program brought by a group of current and former subscribers to AT&T's telephone and/or internet services. Jewel v. National Security Agency, 673 F.3d 902, 906 (9th Cir. 2011). The plaintiffs relied heavily on allegations from a former AT&T employee that the government had created a secure room at an AT&T facility in San Francisco for the purpose of monitoring the internet and telephone activities of all AT&T customers. Id. The named plaintiff, Jewel, alleged that she was specifically affected because AT&T "diverted all of her internet traffic into 'SG3 Secure Rooms' in AT&T facilities all over the country, including AT&T's Folsom Street facility in San Francisco, 'and information of interest [was] transmitted from the equipment in the SG3 Secure Rooms to the NSA based on rules programmed by the NSA.'" Id. The district court dismissed on standing grounds, concluding that

the complaint lacked "allegations specifically linking any of the plaintiffs to the alleged surveillance activities." Id. at 907.

The Court of Appeals for the Ninth Circuit reversed, finding that Jewel had alleged a sufficiently concrete and particularized injury based on her "highly specific" allegations concerning the operation of the alleged surveillance operation. The court noted that the complaint "described in detail the particular electronic communications equipment used ('4ESS switch' and 'WorldNet Internet Room') at the particular AT&T facility (Folsom Street, San Francisco) where Jewel's personal and private communications were allegedly intercepted in a secret room known as the 'SG3 Secure Room.'" Id. at 910 (internal quotations omitted). The court emphasized that the specificity of Jewel's allegations heavily influenced its decision:

> Significantly, Jewel alleged with particularity that *her* communications were part of the dragnet. The complaint focused on AT&T and was not a scattershot incorporation of all major telecommunications companies or a blanket policy challenge. Jewel's complaint also honed in on AT&T's Folsom Street facility, through which all of Jewel's communications allegedly passed and were captured.

Id. (first emphasis in original, second added).

Another recent decision, Klayman v Obama, involved a challenge to the bulk data-collection program brought by users of Verizon Wireless telecommunications services. The plaintiffs argued that

they had standing based on an FISC order targeting Verizon Business (an entity distinct from Verizon Wireless) and by virtue of the sheer scope of the government's data collection efforts. Klayman, 957 F.Supp.2d at 26-27. The district court agreed, opining that the government's attempt to "create a *comprehensive* metadata database" meant that it "*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 (emphasis in original). The court granted a preliminary injunction barring the government from any further data collection. Id. at 43.

On review, the Court of Appeals for the District of Columbia vacated the preliminary injunction and remanded with instructions for the district court to consider whether a limited period of jurisdictional discovery was appropriate. Klayman II, 2015 WL 5058403, at *3. In a decision featuring separate opinions from each of the three judges, the panel agreed that the district court had erred in granting the preliminary injunction, but disagreed as to whether the plaintiffs had established standing. Id.

Writing first, Judge Janice Brown emphasized that the plaintiffs had provided "specific evidence that the government operate[d] a bulk-telephony metadata program that collects subscriber information from domestic telecommunications providers, including Verizon Business Network Services." Id. at *4. She agreed with the district court that, in order to create a database of any appreciable value, the government must also necessarily collect metadata from large

carriers such as Verizon Wireless. Id. Relying on this inference, Judge Brown held that the plaintiffs had "barely fulfilled the requirements for standing at this threshold stage" but "[fell] short of meeting the higher burden of proof required for a preliminary injunction." Id.

Judge Stephen Williams agreed that the plaintiffs were not entitled to preliminary relief, and also questioned whether they had satisfied their burden as to standing. He noted that the "[p]laintiffs' contention that the government is collecting data from Verizon Wireless . . . 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." Id. at *5. Judge Williams observed that this type of speculative inference concerning the government's capabilities was "no stronger than the [Amnesty International] plaintiffs' assertions regarding the government's motive and capacity to target their communications." Id. at *7. He concluded that plaintiffs had "failed to demonstrate a 'substantial likelihood' that the government is collecting [data] from Verizon Wireless" or that plaintiffs "are otherwise suffering any cognizable injury." Id. at *8. Nonetheless, Judge Williams joined Judge Brown in recommending that the matter be remanded for jurisdictional discovery. Id.

The third member of the panel, Judge David Sentelle, concluded that the case should be dismissed entirely:

[P]laintiffs never in any fashion demonstrate that the government is or has been collecting . . . 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, "[Amnesty International] 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." While [Amnesty International] 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 [Amnesty International] plaintiffs. [They] 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.

* * * * * * *

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." . . . 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.

Id. at *9-10.

In reviewing the foregoing decisions, a meaningful distinction emerges. In situations where plaintiffs are able to allege with some degree of particularity that their own communications were specifically targeted – for example, by citing a leaked FISC order or relying on a detailed insider account – courts have concluded that the particularity requirement has been satisfied. See Clapper, 785 F.3d at 801 (noting that the plaintiffs were specifically targeted by an FISC order and that their data was unquestionably collected); Jewel, 673 F.3d at 910 ("Significantly, Jewel alleged with particularity that *her* communications were part of the dragnet.") (emphasis in original). On the other hand, courts have refused to find standing based on naked averments that an individual's communications must have been seized because the government operates a data collection program and the individual utilized the service of a large telecommunications company or companies. See Amnesty Int'l, 133 S. Ct. at 1148 (holding that claims based on a "speculative chain of possibilities" are insufficient); Klayman II, 2015 WL 5058403, at *5-10 (criticizing plaintiffs' reliance on conjecture to attempt to establish standing).

Schuchardt falls squarely within the second category. In reliance on publicly available information, only, he has outlined government programs aimed at the wide-scale collection of communications data. He

also alleges – again, based on media reports and other publicly-available information – that the government may have the capability to collect telephone, email and internet traffic from every American citizen.

Unlike in Jewel and ACLU, Schuchardt has identified no facts from which the Court reasonably might infer that his own communications have been targeted, seized or stored. As his pleadings so much as admit, he is indistinguishable from every other American subscribing to the services of a major telephone and/or internet service provider.[3] Schuchardt's only discernable distinction is his heightened personal-interest in the subject, and, while his civicmindedness may be laudable in other contexts, is insufficient to confer standing. *See* Jewel at 910 (rejecting sufficiency of "scattershot" allegations encompassing "all major telecommunications companies" and/or "a blanket policy challenge" made in the absence of personal standing); *see also* Schlesinger, 418 U.S. at 220 (generalized grievances "common [to] all members of the public" do not confer standing).

For all of the reasons stated above, the Court hereby enters the following:

II. ORDER

Defendants' Motion to Dismiss (**Doc. 20**) is **GRANTED**.

---

[3] *Cf.* discussion *supra* (highlighting Plaintiff's class-allegations, purporting to represent "a nationwide" class of all "American citizens" who are subscribers of several major internet service providers, and Verizon).

September 30, 2015

s\Cathy Bissoon
Cathy Bissoon
United States District Judge

cc (via ECF email notification):

All Counsel of Record

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF
PENNSYLVANIA

Civil Action No. 14-705

Judge Cathy Bissoon

[Filed September 30, 2015]

ELLIOTT SCHUCHARDT,)
)
Plaintiff,)
v.)
)
BARACK H. OBAMA, *et al.*,)
)
Defendants.)
)

JUDGMENT ORDER

Consistent with the Memorandum and Order entered today, FINAL JUDGMENT hereby is entered against Plaintiff under Rule 58 of the Federal Rules of Civil Procedure. This case has been marked closed.

IT IS SO ORDERED.

September 30, 2015 s\Cathy Bissoon
Cathy Bissoon
United States District Judge

cc (via ECF email notification):

All Counsel of Record

Additional material from this filing is available in the Clerk's Office.