IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA
(Pittsburgh Division)

ELLIOTT SCHUCHARDT, individually and d/b/a the Schuchardt Law Firm, Plaintiff, v. DONALD J. TRUMP, President of the United States, *et al.*, Defendants.	Case No. 2:14-cv-0705-CB

BRIEF IN SUPPORT OF DEFENDANTS' RENEWED MOTION TO DISMISS PLAINTIFF'S SECOND AMENDED COMPLAINT

Dated: March 15, 2017

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Director, Federal Programs Branch

JAMES J. GILLIGAN
Special Litigation Counsel

RODNEY PATTON
Senior Counsel

JULIA A. BERMAN
Trial Attorney

TIMOTHY A. JOHNSON
Trial Attorney

CAROLINE J. ANDERSON
Trial Attorney

U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7320
Washington, D.C. 20001
Phone: (202) 305-7919
E-mail: rodney.patton@usdoj.gov

Counsel for Defendants

TABLE OF CONTENTS

PAGE

TABLE OF AUTHORITIES

CASES **PAGE(S)**

PAGE(S)

PAGE(S)

PAGE(S)

STATUTES

PAGE(S)

FEDERAL RULE OF CIVIL PROCEDURE

FEDERAL RULES OF EVIDENCE

LEGISLATIVE MATERIALS

EXECUTIVE ORDERS

MISCELLANEOUS

INTRODUCTION

Plaintiff Elliott Schuchardt seeks to litigate Fourth Amendment and Pennsylvania common-law claims contesting the legality of surveillance conducted by the National Security Agency ("NSA") under a foreign-intelligence program called PRISM. The linchpin of Plaintiff's claim that he has standing to bring such a case is his assertion that the NSA must be collecting his online communications, because PRISM operates as a dragnet that sweeps in all or substantially all Americans' Internet-based communications. Whereas the Third Circuit held that this allegation was entitled to a presumption of truth when Defendants challenged its sufficiency on its face, on this renewed motion to dismiss Defendants contest this allegation as a matter of fact, and it becomes Plaintiff's burden to prove that his allegation of dragnet surveillance is true.

The fatal difficulty for Plaintiff at this stage of the case is that his linchpin allegation is wrong. As the accompanying declaration by the NSA's Director of Operations attests, the NSA does not collect all, or even substantially all, of the online communications sent or received in the United States, whether under PRISM, or any other intelligence program. That reality dispels the sole premise on which Plaintiff claims both the collection of his communications, and the injury that would confer standing on him to challenge the NSA's intelligence-gathering activities. That dispositive fact is unaltered, moreover, by Plaintiff's equally mistaken contention that PRISM collection is conducted under authority of Executive Order 12333, rather than Section 702 of the Foreign Intelligence Surveillance Act.

None of the documentation alluded to in Plaintiff's Second Amended Complaint competently supports his PRISM-as-dragnet allegation. The "evidence" Plaintiff cites is a miscellaneous mix of press reports, statements by former government employees, and exhibits that Plaintiff calls "Snowden's documents." But one way or another the source material that Plaintiff attempts to rely on is inadmissible; the documents are unauthenticated, and the

statements are either hearsay, or otherwise lacking a basis in personal knowledge. More than that, none of this purported evidence, even if admissible, comes close to supporting a factual finding that the NSA collects the online communications of all or substantially all U.S. persons. And that is no less than to be expected, of course, because as knowledgeably attested by the NSA's Director of Operations, the allegation of dragnet surveillance to which Plaintiff's claim of standing is anchored is based on fiction, not fact.

Plaintiff's claims should therefore be dismissed for lack of subject-matter jurisdiction.

BACKGROUND

PRISM Collection Under FISA Section 702

In 1978 Congress enacted the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* ("FISA") "to regulate the use of electronic surveillance within the United States for foreign intelligence purposes," S. Rep. No. 95-604, at 7 (1977), placing certain types of foreign-intelligence surveillance under the oversight of the Foreign Intelligence Surveillance Court ("FISC"), *see* 50 U.S.C. § 1803. Before the Government may conduct "electronic surveillance" (as defined in FISA) to obtain foreign-intelligence information, the statute generally requires the Government to obtain an order from a FISC judge. *See id.* §§ 1801(f), 1804(a), 1805. To obtain such an order, the Government must show "probable cause to believe that . . . the [surveillance] target … is a foreign power or an agent of a foreign power," and that "each of the facilities or places at which the surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id.* § 1805(a)(2).[1/] The Government must also establish that it will employ "minimization procedures" that are "reasonably designed in light of the purpose and technique of the particular surveillance[ ] to minimize the acquisition and retention,

[1/] The statute defines "foreign power" to include "a group engaged in international terrorism or activities in preparation therefor," and an "agent of a foreign power" as a non-U.S. person (*i.e.*, neither a U.S. citizen nor a lawful permanent resident) who "engages in international terrorism or activities in preparation therefor[ ]." 50 U.S.C. § 1801(a)(4), (b)(1)(C), (i).

and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information." *Id*. §§ 1801(h), 1805(a)(3), (c)(2)(A).

When Congress enacted FISA, it focused on foreign-intelligence surveillance of persons *within the United States*, by limiting the definition of "electronic surveillance," to which FISA's requirements are keyed, to domestically targeted foreign-intelligence-collection activities. *Id.* § 1801(f). Congress intentionally excluded from FISA the vast majority of Government surveillance then conducted outside the United States, even if it targeted U.S. persons abroad or incidentally acquired, while targeting other parties abroad, communications to or from U.S. persons or persons located in the U.S. *See* S. Rep. No. 95-701, at 7, 34-35, 71 (1978).

In 2006, Congress began considering amendments to modernize FISA because of changes in communications technology. *See* S. Rep. No. 110-209, at 2-5 (2007); *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138, 1143-44 (2013). FISA's definition of "electronic surveillance" excluded international radio communications to allow the Government to monitor international radio traffic outside FISA's confines. But whereas international communications were predominantly carried by radio or satellite when FISA was enacted, they were now predominantly carried by fiber optic cables, and so qualified as wire communications subject to FISA's requirements. *See Modernization of the FISA: Hearing before the S. Select Comm. on Intel*., 110th Cong., 1st Sess., at 18-19 (2007) ("May 1, 2007 FISA Mod. Hrg.").[2/]

Further, FISA's "electronic surveillance" definition "place[d] a premium on the location of the collection": intercepts of wire or other non-radio communications conducted inside the United States were covered, while those conducted outside the U.S. generally were not. *Id.*

[2/] *Compare* 50 U.S.C. § 1801(f)(2) (defining wire communication as "electronic surveillance" if, *inter alia*, one party is in the United States), *with id.* § 1801(f)(3) (defining radio communication as "electronic surveillance" only if all intended parties are in the United States).

at 19; 50 U.S.C. § 1801(f)(2). The global integration of communications technology had rendered this distinction outmoded too. *See* May 1, 2007 FISA Mod. Hrg. at 19 ("Today, a single communication can transit the world even if the two people communicating are only located a few miles apart."). Due to these technological changes, the Government had to expend significant resources to craft FISA applications for surveillance that was originally intended to be outside FISA's scope. *Id.* at 18. The fix needed for this problem was a "technology-neutral" framework for surveillance of foreign targets, focused not on "how a communication travels or where it is intercepted," but instead on "who is the subject of the surveillance, which really is the critical issue for civil liberties purposes." *Id.* at 46.

Congress addressed this problem through enactment of the FISA Amendments Act of 2008 ("FAA"), Pub. L. No. 110-261. The FAA provision at issue here, Section 702 of FISA, 50 U.S.C. § 1881a, "supplements 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, without regard to the means by which the targeted communications are transmitted or where they are intercepted. Section 702 provides that, upon FISC approval of a "certification" submitted by the Government,[3/] the Attorney General and the Director of National Intelligence ("DNI") may jointly authorize, for up to one year, the "targeting of persons reasonably believed

[3/] To approve the Government's certification the FISC must find: (1) that the Government's "targeting procedures" included with the certification are reasonably designed to ensure that any acquisition conducted thereunder (a) will be limited to persons reasonably believed to be located outside the United States, and (b) will not intentionally acquire communications known to be purely domestic, 50 U.S.C. § 1881a(i)(2)(B); (2) that the Government's minimization procedures also meet FISA's requirements, *id.* § 1881a(i)(2)(C); *see also id.* §§ 1801(h), 1821(4); (3) that the targeting and minimization procedures are also consistent with the Fourth Amendment, *id.* § 1881a(i)(3)(A); and (4) that the certification contains all other statutorily required elements, including an attestation that a significant purpose of the acquisitions is to obtain foreign intelligence, *id.* § 1881a(g)(2)(A)(v), (i)(2)(A).

to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 188la(a), (g); Declaration of Wayne Murphy ("Murphy Decl.") ¶¶ 10-11 (Exh. 1, hereto).[4/] The Government must acquire the information from or with the assistance of an electronic communications service provider, to which end the Attorney General and the DNI may issue "directives" to providers compelling their assistance in the acquisition of the targeted communications. 50 U.S.C. § 1881a(g)(2)(A)(vi); Murphy Decl. ¶ 12. Under the express terms of Section 702, the Government cannot intentionally target a U.S. person overseas or persons (including U.S. persons) known to be in the United States. *Id.* § 1881a(b). The acquisition must also be "conducted in a manner consistent with the [F]ourth [A]mendment." *Id.* § 188la(b)(5).

Pursuant to the authority conferred by Section 702, in accordance with certifications approved by the FISC, the NSA conducts a program of communications collection publicly known as PRISM. *See* Murphy Decl. ¶¶ 4-5, 11, 23. Under PRISM, certain electronic communications are acquired with the compelled assistance of electronic communications service providers through the "tasking" (*i.e.* designation) of "selectors." *See id.* ¶ 14. A selector is a term associated with a specific communications facility used by a target such as the target's e-mail address; selectors cannot be key words such as "bomb" or the names of targeted individuals or organizations. *See id.* ¶ 12. Prior to tasking a selector, NSA analysts must follow FISC-approved targeting procedures to ensure they are targeting a non-U.S. person reasonably believed to be located outside the United States, who possesses or is likely to receive or communicate foreign-intelligence information authorized for acquisition, such as, for example, members of a foreign terrorist organization. *See id.* ¶¶ 4, 13-14. Analysts must also assess whether tasking the particular selector will be likely to acquire foreign-intelligence information.

[4/] As the Director of Operations for the NSA, Mr. Murphy is "responsible for, among other things, managing the integration and use of the NSA's global foreign intelligence authorities." Murphy Decl. ¶ 1.

See id. ¶ 13. These determinations then must undergo internal NSA review. *See id.* Once tasking requests receive approval, the selectors are sent to providers, which then furnish the Government with the electronic communications associated with the approved selectors such as e-mails to or from a specific e-mail address. *See id.* ¶¶ 13-14. The identities of Section 702 targets are classified, as are the identities of the electronic communications service providers that assist in the acquisition of communications under Section 702. *See id.* ¶ 15.

PRISM thus involves targeted collection aimed at capturing communications associated with approved selectors, not bulk collection in which communications data are collected on a large scale without use of specified selectors. *See id.* ¶¶ 4, 9, 11; *see also id.* ¶ 5 n.1. Because of its targeted nature, NSA's PRISM program does not involve the collection or storage of all or even substantially all of the e-mail (or other Internet-based communications) sent or received by persons in the United States. *See id.* ¶¶ 3, 4, 11, 14. Additionally, as a program authorized under Section 702, PRISM collection cannot target U.S. persons; the only permissible targets are non-U.S. persons located abroad who possess or are likely to receive or communicate foreign-intelligence information authorized for acquisition. *See id.* ¶¶ 4, 10-11, 13-14; 50 U.S.C. § 1881a(b), (g)(2).

Executive Order 12333

President Reagan issued Executive Order ("E.O.") 12333 in 1981, then the latest in a series of executive orders "designed to specify the organization, procedures, and limitations applicable to the foreign intelligence and counterintelligence activities of the Executive Branch." Murphy Decl. ¶ 19. The order, which has been amended three times since but is still in effect, *see id.* ¶¶ 19-20, "governs foreign intelligence activities across the Intelligence Community," *id.* ¶ 20, and authorizes the NSA to, *inter alia*, "[c]ollect (including through clandestine means), process, analyze, produce, and disseminate signals intelligence information and data for foreign

intelligence and counterintelligence purposes to support national and departmental missions," and "for the conduct of military operations." E.O. 12333 § 1.7(c). The order expressly provides that nothing in it "shall be construed to authorize any activity in violation of the Constitution or statutes of the United States." *Id.* § 2.8.

Executive Order 12333 is not the legal authority under which the NSA conducts PRISM collection; PRISM collection is conducted exclusively under authority of FISA Section 702. *See* Murphy Decl. ¶¶ 5, 23. And, while the "specific sources and methods" the NSA employs to facilitate collection under Executive Order 12333 are classified, *see id.* ¶ 22, "the NSA does not, under Executive Order 12333, or any other authority, collect in bulk (or store) all or substantially all of the e-mail (or other Internet-based communications) of all U.S. persons," *see id.* ¶ 5. *See also id.* ¶ 4, 14, 22.

Plaintiff's Second Amended Complaint

Plaintiff initiated this suit on June 2, 2014, against the President, the DNI, the Director of the NSA, and the Director of the FBI, in their official capacities, averring that the Defendants "are unlawfully intercepting, accessing and storing [his] private communications," Civil Complaint ¶ 7, ECF No. 1, in claimed violation of his legal rights.[5/] Plaintiff then twice amended his complaint to meet arguments in Defendants' successive motions to dismiss that his allegations failed to establish his standing, and failed to state claims on which relief could be granted. *See* ECF Nos. 5-8, 11, 13-14, 19. Plaintiff's Second Amended Complaint, ECF No. 19 ("2d Am. Compl."), is now his operative pleading.

[5/] Pursuant to Federal Rule of Civil Procedure 25(d), President Trump and Acting DNI Michael P. Dempsey have been automatically substituted for former President Obama and former DNI James R. Clapper, respectively, as defendants sued in their official capacities.

In brief, Plaintiff alleges that Defendants are conducting a program of "bulk collection of domestic e-mail," 2d Am. Compl. ¶ 1,[6/] "known as 'Prism,'" *id.* ¶¶ 35, 99; *see also id.* ¶¶ 72, 73. He maintains that PRISM collection, contrary to the terms of Section 702 (and the facts) encompasses the electronic communications of all persons in the United States, not just those communications to or from targeted selectors. *Id.* ¶ 27 (Defendants are "storing the content of all or substantially all of the e-mail sent by American citizens by means of several large internet service providers."); *id.* ¶ 55 ("The content of all e-mail sent or passing through the United States is monitored and/or stored by the Defendants without a warrant."); *id.* ¶¶ 103, 104. According to Plaintiff, Defendants conduct this dragnet surveillance by obtaining "direct access to the servers of several large internet companies, including Yahoo[!], Google, Facebook, Twitter, Dropbox, and Apple." *Id.* ¶ 35; *see also id.* ¶¶ 38-39, 41, 61, 99. Given that he is a consumer of electronic communications services made available by a number of the providers from which the Government allegedly is collecting "all" content, *id.* ¶ 87; *see* Affidavit of Elliott J. Schuchardt, ECF No. 23-7, ¶¶ 6, 8, Plaintiff concludes that the Defendants must be "unlawfully intercepting, accessing, monitoring and/or storing the private communications of [his], made or stored through such services," 2d Am. Compl. ¶ 88; *see also id.* ¶¶ 92-96 (alleging collection of his "private e-mail communications," "internet search history," "instant messages," and documents stored on the "Dropbox cloud storage service"), and storing them in its "Prism" database, *id.* ¶ 99.

In support of his assertion that the PRISM program operates as a virtual dragnet, sweeping in all Americans' communications, and therefore his own, Plaintiff relies on (i) a set of exhibits attached to his First Amended Complaint, ECF No. 11 ("1st Am. Compl.") that he refers to as "Snowden's documents," 1st Am. Compl., Exhs. D-I; *see* 2d Am. Compl. ¶¶ 35-44;

[6/] This citation refers to paragraph 1 appearing on page 2 of the Second Amended Complaint, under the heading "Background," rather than paragraph 1 appearing in the section headed "Parties" on page 1.

(ii) articles about NSA intelligence-gathering activities published by the *Guardian* newspaper, 1st Am Compl., Exhs. C, J, K; *see* 2d Am. Compl. ¶¶ 35, 45, 46; (iii) affidavits filed by former NSA employees in support of the allegations in *Jewel v. NSA*, No. 08-cv-4373 (N.D. Cal.), another case challenging alleged NSA intelligence-gathering activities; 2d Am. Compl. ¶¶ 8-12, 18-21; and (iv) an editorial authored by a former State Department employee regarding NSA intelligence collection under Executive Order 12333, *id.* ¶¶ 59-61.

Plaintiff contends further that Defendants (improperly) rely upon not one but two "[p]urported [a]uthorit[ies]" to conduct the alleged bulk collection of Americans' e-mails under PRISM. *See id.* ¶¶ 56-75. Specifically, he avers that "Defendants are doing the bulk of their collection under the purported authority of Executive Order 12333," *id.* ¶ 63; *see also id.* ¶ 61, as well as "purporting to act pursuant to Section 702" of FISA. *Id.* ¶ 69.

In Counts I, III and IV of his complaint Plaintiff asserts violations of his rights under the First and Fourth Amendments, and Pennsylvania common law, and seeks injunctive relief prohibiting Defendants from engaging in any further collection of his online communications. 2d Am. Compl. ¶¶ 110, 125, 135; *see id.* at 22-23, 25, 27. He also seeks damages, in Count VI, for alleged violations of FISA. *Id.* ¶ 150; *see id.* at 29.

The Second Amended Complaint also takes issue with, and in Counts II-VI seeks various forms of relief regarding, the NSA's prior bulk collection of call-detail records, containing non-content telephony metadata, under Section 215 of the USA PATRIOT Act, Pub. L. No. 107-56, 115 Stat. 272, 287 (2001), *codified at* 50 U.S.C. § 1861. 2d Am Compl. ¶¶ 1, 33-34, 115-122. *See also* Br. in Support of Defs.' Motion to Dismiss Pls.' 1st Am. Compl., ECF No. 14, at 2-5. The Section 215 program was terminated in November 2015 by the enactment of the USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268, and bulk collection of call-detail records under Section 215 is now statutorily barred. *Id.* §§ 103, 109, 129 Stat. at 272, 276, *codified at*

50 U.S.C. § 1861(c)(3); *see Schuchardt v. President of the U.S.*, 839 F.3d 336, 340 (3d Cir. 2016), citing *Smith v. Obama*, 816 F.3d 1239, 1241 (9th Cir. 2016).

Prior Proceedings on the Second Amended Complaint

Defendants moved to dismiss the Second Amended Complaint for lack of subject-matter jurisdiction, arguing that it contains no well-pleaded allegations of fact that affirmatively and plausibly suggest that Plaintiff's online communications have ever been acquired under the NSA's PRISM program. Defendants moved in the alternative to dismiss the complaint for failure to state claims on which relief can be granted. *See* ECF Nos. 20-21. On September 30, 2015, the Court granted Defendants' motion to dismiss for lack of subject matter jurisdiction, finding that Plaintiff "has identified no facts from which the Court reasonably might infer that his own communications have been targeted, seized or stored." *Schuchardt v. Obama*, 2015 WL 5732117, at *6 (W.D. Pa. Sept. 30, 2015).

On appeal the Third Circuit vacated the Court's order of dismissal and remanded, holding that "at least as a facial matter," Plaintiff's Second Amended Complaint "plausibly stated an injury in fact personal to him." *Schuchardt*, 839 F.3d at 338. The Court of Appeals began by observing that Plaintiff, at oral argument, had "belatedly conceded that his claims regarding the bulk collection of telephone metadata were mooted by the [passage of] the USA FREEDOM Act." *Id.* at 341 n.3. 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.* As a result, the Court of Appeals "focus[ed] solely on whether [Plaintiff] has standing to litigate his Fourth Amendment claim for injunctive relief based on the Government's alleged bulk collection of online communications under PRISM." *Id.*

Next making note of the distinction between a "facial" and a "factual" attack on a court's jurisdiction under Federal Rule of Civil Procedure 12(b)(1), the Court of Appeals concluded that

this Court had "viewed the Government's motion to dismiss as a facial attack on its jurisdiction [because] it did not consider any extrinsic facts proffered by the Government." *Id.* at 343. The Court of Appeals therefore had to "accept as true all of [Plaintiff's] plausible allegations, and draw all reasonable inferences in his favor." *Id.* The Court recognized that "[a]side from his sweeping allegation" that "PRISM functions as an indiscriminate dragnet … captur[ing] all or substantially all of the e-mail sent by American citizens," Plaintiff "has supplied no facts suggesting" that the Government has collected any of his online communications. *Id.* at 349; *see id.* at 354 n.13. The Court remarked further that Plaintiff's alleged facts, even if proven, "do not conclusively establish that PRISM operates as a dragnet," and that the "substantial" authorities supporting the "Government's view of [PRISM's] 'targeted' nature," if correct, "would tend to undermine [Plaintiff's] ability to show" his standing. *Id.* at 351-53. Nevertheless, constrained by the scope of materials that a court may consider on a Rule 12(b)(1) facial challenge, the Court of Appeals, in a "narrow" holding, concluded that Plaintiff had pled sufficiently his "standing to sue for a violation of his Fourth Amendment" rights. *Id.* at 353. At the same time, the Court of Appeals pointed out that "the Government remains free upon remand to make a factual jurisdictional challenge to [Plaintiff's] pleading." *Id.* at 353.[7/]

On remand this Court held a telephone status conference, on February 3, 2017, to determine how this case should proceed. *See* ECF Nos. 46-47. In order to avoid potentially unnecessary motions practice, the Court suggested that Defendants furnish Plaintiff with the facts they would use in support of a factual attack on his standing to challenge PRISM collection. After Defendants provided unclassified materials to Plaintiff regarding the scope of NSA PRISM

[7/] Noting that Plaintiff had suggested at oral argument that he was "entitled" to jurisdictional discovery on remand, the Court of Appeals observed that "jurisdictional discovery is not available merely because the plaintiff requests it," and that jurisdictional discovery "cannot be used to probe the internal (and most likely classified) workings of the national security apparatus of the United States." *Id.* at 353-54 (citation omitted).

collection under Section 702 of FISA, Plaintiff informed counsel for Defendants that he intends to move forward with the case because he believes that bulk collection of all Americans' electronic communications is occurring pursuant to Executive Order 12333.

In light of Plaintiff's concessions before the Court of Appeals, *see Schuchardt*, 839 F.3d at 341 n.3, his Second Amended Complaint has been trimmed to just two operative counts, Counts I and III, alleging that the purported collection of his online communications violates his rights under the Fourth Amendment and Pennsylvania common law. *See* 2d Am. Compl. ¶¶ 1, 85-113, 123-31. Both claims seek injunctive and other equitable relief to prevent Defendants "from engaging in any further collection" of his communications. *Id.* at 22-23, 25.

ARGUMENT

I. LEGAL STANDARDS

"[T]he judicial power of the United States" is limited by Article III of the Constitution "to the resolution of 'cases' and 'controversies.'" *Valley Forge Christian Coll. v. Ams. United for Separation of Church & State*, 454 U.S. 464, 471 (1982); *see DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 341 (2006); *In re Schering Plough Corp. Intron/Temodar Consumer Class Action*, 678 F.3d 235, 244 (3d Cir. 2012). A plaintiff's standing to sue "is an essential and unchanging part of the case-or-controversy requirement," *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992), without which the court lacks jurisdiction to entertain the suit. *Warth v. Seldin*, 422 U.S. 490, 498 (1975); *Kerchner v. Obama*, 612 F.3d 204, 207 (3d Cir. 2010). The Supreme Court "ha[s] always insisted on strict compliance with this jurisdictional standing requirement." *Raines v. Byrd*, 521 U.S. 811, 819 (1997).[8/]

[8/] Plaintiff's class-action allegations, 2d Am. Compl. ¶¶ 76-84, are immaterial to the standing analysis. Plaintiff must establish his standing regardless of whether he seeks to litigate his claims individually or on behalf of a class. *Hayes v. Wal-Mart Stores, Inc.*, 725 F.3d 349, 360-61 (3d Cir. 2013); *McNair v. Synapse Grp., Inc.*, 672 F.3d 213, 223-24 (3d Cir. 2012).

To establish Article III standing, a plaintiff must seek relief from an injury that is "concrete, particularized, and actual or imminent; fairly traceable to the challenged action; and redressable by a favorable ruling." *Amnesty Int'l*, 133 S. Ct. at 1147 (citation omitted). The alleged injury must be "distinct and palpable," not "abstract or conjectural or hypothetical." *Danvers Motor Co. v. Ford Motor Co.*, 432 F.3d 286, 291 (3d Cir. 2005); speculative claims of injury will not support Article III standing. *See Amnesty Int'l*, 133 S. Ct. at 1147. As the "party invoking federal jurisdiction," a plaintiff "bears the burden of establishing these elements" of standing. *Defenders of Wildlife*, 504 U.S. at 561. Each element of standing "must be supported in the same way as any other matter on which the plaintiff bears the burden of proof, *i.e.*, with the manner and degree of evidence required at the successive stages of the litigation." *Id.*

"A Rule 12(b)(1) motion," such as this one, "may be treated as either a facial or factual challenge to the court's subject matter jurisdiction." *Gould Elec., Inc. v. United States*, 220 F.3d 169, 176 (3d Cir. 2000).[9/] A facial challenge "attacks the complaint on its face without contesting its alleged facts," *Hartig Drug Co. v. Senju Pharm. Co.*, 836 F.3d 261, 268 (3d Cir. 2016), so that "the court must treat the complaint's well-pleaded jurisdictional facts as true and view them in the light most favorable to the plaintiff." *Byrd v. Aaron's, Inc.*, 14 F. Supp. 3d 667, 679 (W.D. Pa. 2014). In contrast, a factual challenge "attacks allegations underlying the assertion of jurisdiction in the complaint," "strip[ping] the plaintiff of the protections and factual

[9/] A line of cases in the Third Circuit suggests that a Rule 12(b)(1) factual attack cannot be made until after the answer has been served so that the "plaintiff's allegations have been controverted." *Mortensen v. First Fed. Sav. & Loan Ass'n*, 549 F.2d 884, 892 & n.17 (3d Cir. 1977). The Third Circuit has since rejected *Mortensen's* "dictum" as "wrong," because the Supreme Court has "made clear that a facially sufficient complaint may be dismissed before an answer is served if it can be shown by affidavits that subject matter jurisdiction is lacking." *Berardi v. Swanson Mem'l Lodge No. 48*, 920 F.2d 198, 200 (3d Cir. 1990). Recent Third Circuit case law suggests that a factual challenge to jurisdiction is appropriate so long as the defendant files an answer "or otherwise present[s] competing facts." *Davis v. Wells Fargo*, 824 F.3d 333, 346 (3d Cir. 2016); *Constitution Party of Pa. v. Aichele*, 757 F.3d 347, 358 (3d Cir. 2014) (same); *see Dickerson v. Bank of Am.*, 2013 WL 1163483, at *2 (D.N.J. Mar. 19, 2013).

deference provided under" a Rule 12(b)(1) facial challenge. *Hartig Drug Co.*, 836 F.3d at 268; *see id.* ("[N]o presumptive truthfulness attaches to the plaintiff's allegations.") (citation omitted).

When challenging jurisdiction as a factual matter, the defendants may "present competing facts," *id.*, with which they "essentially mak[e] the argument that the allegations supportive of jurisdiction are not true." *Byrd*, 14 F. Supp. 3d at 679. The Court may then consider such extrinsic evidence as "affidavits, depositions, and testimony to resolve factual issues bearing on jurisdiction." *Gotha v. United States*, 115 F.3d 176, 179 (3d Cir. 1997). Once the defendants present evidence challenging jurisdiction, the Court "must permit the plaintiff to respond with evidence supporting jurisdiction." *Gould Elec., Inc.*, 220 F.3d at 177. The Court is then "free to weigh the evidence," *Hartig Drug Co.*, 836 F.3d at 268, "to determine if it has jurisdiction," *Gould Elec., Inc.*, 220 F.3d at 178. Consistent with the requirements of Article III, however, the "plaintiff has the burden of persuasion to convince the court it has jurisdiction," *id.*, and must establish the facts supporting jurisdiction "by admissible evidence," *Meridian Sec. Ins. Co. v. Sadowski*, 441 F.3d 536, 540, 542 (7th Cir. 2006) (quoting *McNutt v. Gen. Motors Acceptance Corp.*, 298 U.S. 178, 189 (1936) (if plaintiff's "allegations of jurisdictional facts are challenged by his adversary in any appropriate manner, he must support them by competent proof.")). *See also, e.g., McPhail v. Deere & Co.*, 529 F.3d 947, 954 (10th Cir. 2008); *Elofson v. Bivens*, 2017 WL 566323, at *15 (N.D. Cal. Feb. 13, 2017); *In re Enron Corp. Secs., Derivative & "ERISA" Litig.*, 279 F.R.D. 395, 403 (S.D. Tex. 2011).

II. PLAINTIFF CANNOT DEMONSTRATE HIS STANDING BECAUSE PRISM COLLECTION DOES NOT ENTAIL BULK COLLECTION OF ALL ONLINE COMMUNICATIONS SENT OR RECEIVED IN THE UNITED STATES.

A. Plaintiff's Allegation That PRISM Encompasses the Internet-Based Communications of All or Substantially All U.S. Persons Is Untrue.

The Third Circuit recognized that the "linchpin" of Plaintiff's standing claim is his allegation that PRISM collects "'all or substantially all of the e-mail sent by American citizens.'"

Schuchardt, 839 F.3d at 354 n.13. "Aside from this sweeping allegation, [Plaintiff] has supplied no facts suggesting" that the Government would collect online communications of his. *Id.* at 349. Therefore, in order to demonstrate a cognizable injury in fact that would establish his standing, Plaintiff bears the "burden of persuasion to convince the court," *Gould Elec., Inc.*, 220 F.3d at 178, that PRISM is the "virtual dragnet" he alleges, *see Schuchardt*, 839 F.3d at 349, so that he can establish that he was "among the injured." *Defenders of Wildlife*, 504 U.S. at 563.

Plaintiff cannot carry that burden because his "linchpin" allegation is wrong as a matter of fact. As detailed in the declaration of the NSA Director of Operations, PRISM collection involves targeted—not bulk—collection. *See* Murphy Decl. ¶¶ 4, 11-14, 16. Specifically, Section 702 of FISA authorizes only the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information." 50 U.S.C. § 188la(a), (g); *see* Murphy Decl. ¶¶ 4, 10-11. Consistent with the limits of that authority, the NSA conducts PRISM collection by acquiring "targeted electronic communications associated with an approved target's selector," such as an e-mail address for a member of a foreign terrorist organization, "directly from compelled electronic communication service providers." Murphy Decl. ¶ 14; *see also id.* ¶¶ 4, 5, 23. For example, if the selector is an e-mail address, that e-mail address is "sent to the provider of that email service and the provider would then be compelled to facilitate acquisition of electronic communications to or from the email address of the target." *Id.* ¶ 14. "PRISM collection is therefore not, as Plaintiff alleges," "a program in which the NSA collects in bulk (or stores) all or substantially all of the e-mail and other Internet-based communications of all U.S. persons." *Id.*; *see also id.* ¶ 4.

This understanding of PRISM's targeted nature is supported not only by the sworn testimony of the NSA's Director of Operations, but also, as the Third Circuit noted, *see Schuchardt*, 839 F.3d at 353, by a number of other authorities, including 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 ("PCLOB Report"), https://www.pclob.gov/library/702-Report.pdf, at 7, 32-34 (describing process of targeted collection under PRISM). The PCLOB is an "independent agency" that was asked by a "bipartisan group of U.S. Senators" to review and report on the NSA intelligence programs authorized by Section 702 of FISA, including PRISM. *See* PCLOB Report at 1. And as Director Murphy confirms, the PCLOB's description of PRISM's operation and its independent assessment of PRISM as a program of targeted collection are both correct. *See* Murphy Decl. ¶ 17.[10/] As the Third Circuit also observed, the authorities that have examined PRISM and agree that the program is targeted are "substantial." *Schuchardt*, 839 F.3d at 353. That consensus, which is accurate, "undermine[s] [Plaintiff's] ability to show that his own electronic communications were seized by the PRISM program." *Id.*

That conclusion is unchanged by Plaintiff's erroneous contention that the NSA is "doing the bulk of [the] collection under the purported authority of Executive Order 12333." 2d Am. Compl. ¶ 63. As Director Murphy attests, the allegation that PRISM is conducted under authority of Executive Order 12333 is "incorrect." Murphy Decl. ¶ 5. "PRISM collection is conducted exclusively under authority of FISA section 702," *id.*, not Executive Order 12333, *id.* ¶ 23. Moreover, it would make no difference even if Plaintiff were correct, and PRISM in fact operated under authority of that order. Executive Order 12333 authorizes the NSA, *inter alia*, to collect signals intelligence information for foreign-intelligence and counterintelligence purposes.

[10/] *See also United States v. Mohamud*, 843 F.3d 420, 440 (9th Cir. 2016) (citing the PCLOB Report for targeted nature of PRISM); *United States v. Hasbajrami*, 2016 WL 1029500, at *6 (E.D.N.Y. Mar. 8, 2016); *Wikimedia Found. v. NSA*, 143 F. Supp. 3d 344, 348-49 (D. Md. 2015); *Klayman v. Obama*, 957 F. Supp. 2d 1, 8 n.6 (D.D.C. 2013) ("'PRISM' program" "targets non-U.S. persons located outside the U.S."), *vacated on other grounds and remanded by Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015).

Id. ¶ 21. While the "specific sources and methods" of intelligence-gathering collection under "Executive Order 12333 are classified," "the NSA does not, under Executive Order 12333, collect in bulk (or store) all or substantially all of the emails or other Internet-based communications of all United States persons." *Id.* ¶ 22. Indeed, the NSA does not "engage in such bulk collection (or storage) of all or substantially all U.S. persons' online communications under any other authority." *Id.*; *see also id.* ¶¶ 4-5.

And so, deprived of the exclusive factual basis upon which his claim that his Internet-based communications are collected under PRISM (or any other intelligence program), *see Schuchardt*, 839 F.3d at 349, Plaintiff is unable to carry his burden of proving that he personally has suffered a cognizable injury attributable to PRISM collection, and thus "that jurisdiction does in fact exist." *Hartig Drug Co.*, 836 F.3d at 268 (citation omitted).[11/]

B. Plaintiff's Second Amended Complaint Identifies No Competent Support for the Allegation That the NSA Collects the Online Communications of Virtually All Americans.

In support of his contrary allegation that PRISM collection encompasses virtually all electronic communications sent or received in the United States, Plaintiff cites an amalgamation of media reports, statements by one-time Government employees, and a set of exhibits he refers

[11/] While the Government has officially acknowledged the existence of and some facts about PRISM collection, *see* Murphy Decl. ¶¶ 4, 10-17, the operational details of PRISM collection, such as the identities of targets and participating providers, remain classified to protect sensitive intelligence sources and methods, and cannot be disclosed without compromising ongoing intelligence operations and thus placing national security at risk. *See id.* ¶¶ 6, 15, 24-27, 29. The same is true for the "specific sources and methods employed by the NSA to collect signals intelligence information pursuant to Executive Order 12333." *Id.* ¶ 22; *see also id.* ¶¶ 6, 24-29. The Government is therefore entitled, under the state secrets doctrine, to protect these sources and methods and additional details from public disclosure. *See ACLU v NSA*, 493 F.3d 644 (6th Cir. 2007); *see also Mohamed v. Jeppesen Dataplan, Inc.*, 614 F.3d 1070, 1090 (9th Cir. 2010); *El–Masri v. United States*, 479 F.3d 296, 308-311 (4th Cir. 2007); *Halkin v. Helms*, 690 F.2d 977, 994-95 (D.C. Cir. 1982). The NSA's sources and methods are also protected by section 6 of the National Security Agency Act of 1959, 50 U.S.C. § 3605, which provides that no law shall be construed to require the disclosure of any information regarding NSA's intelligence-gathering activities. *See Larson v. Dep't of State*, 565 F.3d 857, 868 (D.C. Cir. 2009); *Linder v. NSA*, 94 F.3d 693, 698 (D.C. Cir. 1996).

to as "Snowden's documents." The Court of Appeals held that on Defendants' facial challenge to Plaintiff's standing he was "entitled to any inference in his favor that may be reasonably drawn" from these sources, *Schuchardt*, 839 F.3d at 352, but the legal terrain has since shifted. Now that jurisdiction has been contested on factual grounds, Plaintiff can no longer rest on the presumption of truth. *Hartig Drug Co.*, 836 F.3d at 268. Instead, he must prove the facts necessary to establish the Court's jurisdiction, *Gould Elec. Inc.*, 220 F.3d at 178, and do so on the basis of admissible evidence, *Meridian Sec. Ins. Co.*, 441 F.3d at 540, 542; *see supra*, at 14. The sources cited by Plaintiff, however, contain no admissible evidence to support his mistaken claim that PRISM involves the collection of all Americans' online communications.

1. The So-Called "Snowden Documents"

Plaintiff principally relies on a series of documents, Exhibits D-I to his First Amended Complaint, which he describes as showing that the NSA is collecting "massive quantities of e-mail and other data created by United States citizens." *See* 2d Am. Compl. ¶¶ 36-44, citing 1st Am. Compl., Exhs. D-I. To the contrary, however, as evidence that PRISM collection encompasses the online communications of virtually all Americans, these exhibits are valueless.

First, these exhibits have not been authenticated. As a condition of admissibility the 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). The evidence on which a party relies for this purpose "must itself be admissible." *In re Japanese Elec. Prods. Antitrust Litig.*, 723 F.2d 238, 285 (3d Cir. 1983), *rev'd on other grounds* by 475 U.S. 574 (1986). Plaintiff does not explain what he claims Exhibits D-I to be, other than referring to them as "Snowden's documents." 2d Am. Compl. ¶ 35. Perhaps he means to suggest that these exhibits are part of a classified Powerpoint presentation about PRISM that the *Guardian* newspaper claimed to have obtained in a June 6,

2013, article that Plaintiff attached to his First Amended Complaint. *See* 2d Am. Compl. ¶ 35 & n.9, citing 1st Am. Compl., Exh. C. But Plaintiff offers no evidence either (i) that Exhibits D-I are in fact part of the Powerpoint presentation that the *Guardian* said it had obtained; or (ii) that the suite of Powerpoint slides the *Guardian* obtained are in fact official Government documents describing PRISM, as would both be necessary to establish the authenticity of these exhibits.[12/] Absent such evidence, Exhibits D-I are entitled to no evidentiary weight.[13/]

Second, even if Exhibits D-I could be authenticated, they constitute written out-of-court statements regarding PRISM's operation that Plaintiff offers for the truth of the matters asserted. As such, they would remain inadmissible unless Plaintiff could also show that they fall under a hearsay exception or exclusion enumerated under the Federal Rules of Evidence. *See Browne*, 834 F.3d at 415-16, citing *United States v. McGlory*, 968 F.2d 309, 331 (9th Cir. 1992); *United States v. Console*, 13 F.3d 641, 656 (3d Cir. 1993). Plaintiff has made no such showing.

Third, even if Exhibits D-I could be rendered admissible as evidence, they would not support Plaintiff's contention that PRISM collection includes everyone's online communications in the United States. The first two of these Exhibits, D and E, purport to identify Internet service providers from which the NSA collects communications, and the types of communications

---

[12/] The *Guardian* article asserts that the paper "has verified the authenticity of the document," 2d Am. Compl., Exh. C at 2, but that conclusory assertion is itself unsubstantiated double hearsay—an unsworn, out-of-court statement by the authors of the *Guardian* article to the effect that they were told by other, unidentified individuals (whose own personal knowledge of the pertinent facts is unshown, *see* Fed. R. Evid. 602), that the document is genuine. As such the *Guardian's* assertion that it "verified the authenticity" of the Powerpoint document is itself inadmissible, and does not meet the pre-requisites of authentication, unless Plaintiff "demonstrate[s] that both layers of hearsay would be admissible" under an application exception. *Smith v. City of Allentown*, 589 F.3d 684, 693 (3d Cir. 2009); *see* Fed. R. Evid. 805.

[13/] The Government has neither confirmed nor denied the authenticity of these documents, and does not do so here. Courts do not consider national-security information that has been allegedly leaked to the press to be a matter of public knowledge unless its authenticity has been officially acknowledged by authorized Government personnel. *Cozen O'Connor v. U.S. Dep't of the Treasury*, 570 F. Supp. 2d 749, 788 (E.D. Pa. 2008); *see also EPIC v. NSA*, 678 F.3d 926, 933 n.5 (D.C. Cir. 2012); *Wilson v. CIA*, 586 F.3d 171, 186-87 (2d Cir. 2009).

collected. But neither exhibit says anything to suggest that the named companies provide the NSA with the communications of all persons who subscribe to their services, rather than just those whose communications are targeted in accordance with the limitations of Section 702. 1st Am. Compl. Exhs. D, E. Next is an exhibit that refers to "Sniff[ing] it All," "Know[ing] it All," and "Collect[ing] it All," and another noting "possibilities" that could "bring[ ] our enterprise one step closer to collecting it all." 1st Am. Compl. Exhs. F, G. According to Plaintiff these exhibits "confirm" that NSA PRISM collection encompasses "*all* of the content" stored by the named providers. 2d Am. Compl. ¶¶ 40, 41. In fact, neither exhibit refers to PRISM, or even the NSA, at all. And neither exhibit, when referring to "collecting it all," specifies "all" what. If, as Plaintiff maintains, the exhibits purport to describe PRISM collection under Section 702, then they would more obviously be explained as references to collecting "all" the online communications of only those non-U.S. persons targeted for surveillance in accordance with Section 702's terms and limitations, not of "all" U.S. persons generally.

Exhibit H purports to discuss PRISM collection of Microsoft Skydrive data, but nothing in the exhibit states that the NSA is "literally storing every single document … on Microsoft's Skydrive" service, as Plaintiff alleges. 1st Am. Compl., Exh. H; *see* 2d Am. Compl. ¶ 42. To the contrary, Exhibit H purports to state that Skydrive data would become a standard part of PRISM collection "for a tasked selector," which would be consistent with targeted collection of data only from user accounts and communications associated with tasked selectors, *see supra*, at 5-6, and not bulk collection of data from all accounts. Finally, Exhibit I simply states that unspecified "collection" of some kind is "outpacing the NSA's ability to ingest, process and store" data in accordance with prior "norms." 1st Am. Compl., Exh. I. But absent quantifiable benchmarks regarding the amount of data collected, or the NSA's storage capabilities, that observation provides no springboard for concluding that collection under PRISM (which the

document does not mention) includes the online communications of all U.S. persons. Thus, even if Exhibits D-I were admissible to support Plaintiff's jurisdictional claims, they do not support his claim that all Americans' online communications, including his, are collected under PRISM.

2. The *Guardian* Newspaper Articles

Relatedly, Plaintiff also relies on statements appearing in three *Guardian* articles, including claims that the NSA, through PRISM, obtains "direct access to the servers of several large internet companies," and assertions by Edward Snowden that when employed as an NSA contractor he could "wiretap anyone" and "search for, seize, and read … [a]nyone's communications at any time." 2d Am. Compl. ¶¶ 35, 45, 46, citing 1st Am. Compl., Exhs. C, J, K. These articles also are of no evidentiary worth. "Newspaper articles are considered hearsay and may be used as evidence "only in very exceptional circumstances." *Corner Pocket, Inc. v. Travelers Indem. Co.*, 2014 WL 657615, at *2 (W.D. Pa. Feb. 20, 2014) (citations omitted). The statements in these articles "by individuals other than [their] author[s]"—such as those attributed to Edward Snowden in Exhibits J and K—"constitute double hearsay." *Id.* (citation omitted).

Moreover, none of the statements contained in these articles, even if admissible, describe PRISM as a bulk collection program that sweeps in all online communications in the United States. The *Guardian's* June 6, 2013, article asserting that the NSA "has obtained direct access to the systems" of various Internet service providers, 1st Am. Compl., Exh. C at 1-2, states that the NSA obtained this access under a law that "allows for *the targeting* of any customers of participating firms *who live outside the U.S. or those Americans whose communications include people outside the U.S.*" *Id.* at 2-3 (emphasis added). Thus, the activity described by the *Guardian* is not one of mass surveillance of all Americans' communications, but resembles more closely (albeit imperfectly) the targeted surveillance directed at non-U.S. persons located outside the United States that is authorized under Section 702.

The second and third of the *Guardian* articles, published in July 2013, respectively discuss a purported NSA program called "XKeyscore," and reproduce a transcript of a public statement made by Mr. Snowden. 1st Am. Compl., Exhs. J, K. Neither makes any reference whatsoever to PRISM, much less substantiates Plaintiff's claims about PRISM's scope. And even if the statements in these articles attributed to Mr. Snowden were credited—that while "sitting at [his] desk" he "could wiretap anyone," and "had the capability … to search for, seize, and read [anyone's] communications," 1st Am. Compl., Exh. J at 2, Exh. K at 2—they speak only to a capability of surveilling any given individual's communications. They do not remotely suggest that the NSA actually collects every U.S. person's communications, whether under PRISM or any other intelligence-gathering program.

3. The Binney, Drake, and Wiebe Declarations

In addition to the materials appended to Plaintiff's First Amended Complaint, the Second Amended Complaint also cites declarations submitted by three former NSA employees in *Jewel v. NSA*, No. 4:08-cv-4373-JSW (N.D. Cal.), a self-described "challenge[to] an [alleged] illegal and unconstitutional program of dragnet communications surveillance conducted by the [NSA] and other Defendants …." 2d Am. Compl. ¶¶ 8-12, 18-21, citing Decls. of William E. Binney, Thomas A. Drake, & J. Kirk Wiebe, *Jewel* ECF Nos. 86-88 (attached as Exhibits 2-4, hereto); *see* Complaint for Constitutional & Statutory Violations ¶ 2, *Jewel* ECF No. 1. But none of these declarants supplies competent evidence that the NSA, whether under PRISM, or otherwise, collects information about the telecommunications of all Americans.

First, all three declarants lack personal knowledge about the scope and operation of PRISM. Messrs. Binney and Wiebe retired from the NSA in late 2001, and Mr. Drake no later than 2006. *See* Binney Decl. ¶ 6; Wiebe Decl. Exh. A at 2; Drake Decl. Exh. A at 2. By the time Section 702 was enacted in 2008, these gentlemen had not been employed by the NSA for years,

and could only speculate about the nature, scope, and focus of the NSA intelligence programs carried out under the statute's terms. They are not competent witnesses, therefore, to testify on such matters. Fed. R. Evid. 602; *United States v. Seals*, 566 F. App'x 121, 122 (3d Cir. 2014) ("A witness may not testify about an event s/he does not have personal knowledge of.").[14/]

Plaintiff specifically cites testimony by Messrs. Binney and Drake that while still employed at the NSA in late 2001 they were told by unnamed colleagues involved with the President's Surveillance Program (the "PSP") (a collection of intelligence activities initiated in the wake of the September 11, 2001, terrorist attacks) that the program "involved the collection of domestic electronic communications traffic." 2d Am. Compl. ¶¶ 19-20, citing Binney Decl. ¶ 5 & Drake Decl. ¶ 7. This testimony is not only hearsay, it is also irrelevant. Nothing in the Binney or Drake declarations even purports to describe the scope or scale on which the PSP was "collect[ing] … domestic electronic communications traffic," much less do they attest that the NSA was collecting all such traffic in the United States.[15/]

Plaintiff also places reliance on assertions by Messrs. Binney, Wiebe, and Drake that the NSA has the "capability to seize and store most electronic communications passing through its U.S. intercept centers," which Mr. Binney "estimate[s]" to number between ten and twenty, and,

---

[14/] The Supreme Court has made clear, also, that speculation about the scope and operation of Government surveillance programs will not support a finding, for standing purposes, that a litigant has been a subject of such surveillance. *Amnesty Int'l*, 133 S. Ct. at 1147-51.

[15/] In any event, evidence of surveillance activities conducted by the NSA in late 2001 would have no probative value regarding the scope of surveillance conducted by the agency today, nearly 16 years later, under authority of a statute not enacted until 2008. Evidence so remote in time from the events at issue cannot be considered relevant under Federal Rule of Evidence 401. *See, e.g.*, *Chertkova v. Conn. Gen. Life Ins. Co.*, 2000 WL 349277, at *4 (2d Cir. Apr. 4, 2000) (affirming exclusion of evidence "of events that had allegedly occurred 11 years before the relevant period"); *Bhasin v. Bluefield Reg'l Med. Ctr., Inc.*, 1995 WL 465796, at *4 (4th Cir. Aug. 8, 1995) (affirming exclusion of events from early 1980s as "too remote" from an employment discharge in 1992); *West v. Drury Co.*, 2009 WL 1532491, at *1 (N.D. Miss. June 2, 2009) (excluding medical record more than a decade old); *Dimas v. Mich. Dep't of Civil Rights*, 2004 WL 1397558, at *12 n.2 (W.D. Mich. Mar. 19, 2004) (excluding statements ten years prior to alleged discrimination as "too remote in time . . . to be probative").

based on media reports about the anticipated capacity of new NSA digital storage facilities, that the NSA "is, in fact, storing all [the electronic communications] that they are collecting." 2d Am. Compl. ¶¶ 19-21; Binney Decl. ¶¶ 7-13; Wiebe Decl. ¶¶ 8-9; Drake Decl. ¶¶ 8-9. Again, these gentlemen, who all retired from the NSA some 10-15 years ago (and years before they executed their June 2012 declarations), have no evident basis in personal knowledge from which to competently testify about the volume of communications the NSA has the capacity to collect or store. *Seals*, 566 F. App'x at 122. Moreover, even assuming the NSA were "stor[ing] most electronic communications passing through its U.S. intercept centers," nothing in the Binney, Wiebe, and Drake declarations even purports to suggest what fraction of Americans' electronic communications passes through the 10-20 "intercept centers" whose existence Mr. Binney posits, much less that they intercept the communications of all Americans.

Messrs. Binney and Wiebe also concur that "[s]everal other circumstances support the conclusion that the NSA is storing all personal electronic communications." Binney Decl. ¶¶ 14-17; *see* Wiebe Decl. ¶¶ 11-14. But this testimony, too, lacks a foundation in personal knowledge. Rather, it is speculation based on public testimony about the Government's investigation of the 2011 killings at Fort Hood, Texas, and public reports of activities allegedly planned by British intelligence agencies, *id.*, none of which has anything to do with Plaintiff's allegations regarding the scope of communications collection conducted under PRISM.

4. The Tye Editorial

Finally, Plaintiff cites a July 2014 editorial by John Napier Tye,[16/] a former State Department employee, as support for the allegation that the Government "claim[s] the legal

[16/] *See* John Napier Tye, "Meet Executive Order 12333," *Washington Post* (July 18, 2014), https://www.washingtonpost.com/opinions/meet-executive-order-12333-the-reagan-rule-that-lets-the-nsa-spy-on-americans/2014/07/18/93d2ac22-0b93-11e4-b8e5-d0de80767fc2_story.html?utm_term=.f1b6f19e021c (Exh. 5, hereto).

authority to collect the nation's entire e-mail database under Executive Order, No. 12333." 2d Am. Compl. ¶ 60. The statements made in this editorial support no such claim.

According to the editorial, Mr. Tye "worked on global Internet freedom policy as a civil servant at the State Department," and in that capacity "was cleared to receive" classified information about NSA intelligence-collection activities. Exh. 5, at 2. He expresses concern that nothing in Executive Order 12333 prohibits the NSA from retaining the communications of U.S. persons that are "incidentally" collected "outside the United States in the course of a lawful foreign intelligence investigation." *Id*. at 2, 3. This out-of-court written statement is of course hearsay, *Console*, 13 F.3d at 656, and to the extent Plaintiff wishes to prove the truth of what Mr. Tye was told about NSA intelligence collection, it is double hearsay, *Corner Pocket, Inc.*, 2014 WL 657615, at *2. Moreover, the editorial does not assert that the NSA claims or purports to exercise authority under Executive Order 12333 to collect all e-mails sent or received by persons in the United States. It merely addresses the possibility, in Mr. Tye's view, that the NSA could be retaining some U.S. persons' communications that were incidentally collected in the course of lawful foreign-intelligence activities conducted overseas.

In sum, Plaintiff has advanced no competent evidence to support his allegation that PRISM involves the collection of information about all Americans' online communications. His contention that the NSA must be collecting communications of his, because it intercepts and collects information about all electronic communications sent or received in the United States, is simply not rooted in fact. It offers no ground on which Plaintiff can establish standing to maintain this suit. And because he has pled no other such grounds, *Schuchardt*, 839 F.3d at 349, 354 n.13, much less proven any, Plaintiff's claims must be dismissed.

CONCLUSION

For the reasons stated above, the Second Amended Complaint should be dismissed.

Dated: March 15, 2017

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General

ANTHONY J. COPPOLINO
Deputy Branch Director

JAMES J. GILLIGAN
Special Litigation Counsel

/s/ Rodney Patton
RODNEY PATTON
Senior Counsel

JULIA A. BERMAN
Trial Attorney

CAROLINE J. ANDERSON
Trial Attorney

TIMOTHY A. JOHNSON
Trial Attorney

U.S Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Ave., N.W., Room 7320
Washington, D.C. 20001
Phone: (202) 305-7919
E-mail: rodney.patton@usdoj.gov

Counsel for Defendants