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

ELLIOTT SCHUCHARDT,	)	
	)	
Plaintiff,	)	
v.	)	Civil Action No. 14-705
	)	
BARACK H. OBAMA, *et al*.,	)	Judge Cathy Bissoon
	)	
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 underpins each of Plaintiff's claims, and he purports to represent a "nationwide class" of "American citizens" similarly-situated. Id. at ¶ 76.

[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).

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 [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

[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.

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**.

September 30, 2015

s\Cathy Bissoon
Cathy Bissoon
United States District Judge

cc (via ECF email notification):

All Counsel of Record

[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).