UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LARRY KLAYMAN, *et al.*,

Plaintiffs,

v.

NATIONAL SECURITY AGENCY, *et al.*,

Defendants.

Civil Action Nos. 13-851 (RJL)
13-881 (RJL)

st

MEMORANDUM OPINION

November 21, 2017 [Dkts. ##178, 123]

These two actions are yet another chapter in a multi-year saga, during which our three co-equal branches of government have struggled to strike the appropriate balance between protecting the citizens of our Nation and the individual liberties of those very citizens. Although the Judiciary will surely be called upon in the future to ensure that the balance struck is constitutionally sound, this Court's role in assessing the Government's conduct in these two cases ends today.

Plaintiffs filed these two related actions, *Klayman v. Obama*, No. 13-cv-851 (D.D.C. filed June 6, 2013) ("*Klayman I*"), and *Klayman v. Obama*, No. 13-cv-881

(D.D.C. filed June 12, 2013) ("*Klayman II*"), in June of 2013,[1] challenging the constitutionality and statutory authorization of certain intelligence-gathering practices of the United States Government. Plaintiffs are six individuals and one law firm, who bring these suits as U.S. citizens or entities, and who are all subscribers, customers, or users of certain telecommunications and Internet service providers that allegedly participated in these Government surveillance programs. *See Klayman I*, 4th Am. Compl. ¶¶ 7–18 [Dkt. #145-1]; *Klayman II*, 3d Am. Compl. ¶¶ 4–23 [Dkt. #112]. In the operative complaints, plaintiffs challenge the Government's wholesale collection and analysis of the phone and Internet metadata of U.S. citizens. Plaintiffs allege that these surveillance programs violated—and continue to violate—their First, Fourth, and Fifth Amendment rights. *See Klayman I*, 4th Am. Compl. ¶¶ 49–69; *Klayman II*, 3d Am. Compl. ¶¶ 55–75.

In the actions as filed, defendants are several federal agencies and departments, executive and judicial officials, and telecommunications and Internet service providers and their executive officers.[2] *See Klayman I*, 4th Am. Compl. ¶¶ 19–25; *Klayman II*, 3d Am. Compl. ¶¶ 24–35. To remedy defendants' alleged constitutional infractions, plaintiffs seek three distinct forms of declaratory and injunctive relief: (1) an injunction against future bulk collection of metadata about their calls; (2) an injunction against NSA

---

[1] Plaintiff Larry Klayman has also filed two additional related cases, *Klayman v. Obama*, No. 14-cv-92 (D.D.C. filed Jan. 23, 2014), and *Montgomery v. Comey*, No. 17-cv-1074 (D.D.C. filed June 5, 2017). This memorandum opinion, however, addresses only *Klayman I* and *Klayman II*.

[2] The individual defendants in both cases have since been dismissed. *See Klayman I*, 9/19/16 Mem. Order [Dkt. #175]; *Klayman II*, 9/19/16 Mem. Order [Dkt. #120]. And while the original complaints in these actions named as defendants several telecommunications and Internet service providers and their executive officials, the newest versions of the complaints in both actions omit these defendants. *Compare Klayman I*, Compl. ¶ 9, and *Klayman II*, Compl. ¶¶ 20–42, *with Klayman I*, 4th Am. Compl. ¶¶ 19–24, and *Klayman II*, 3d Am. Compl. ¶¶ 13–18.

queries of plaintiffs' metadata that may have been collected under the program; and (3) an accounting, expungement from federal Government records, and return of any collected data pertaining to plaintiffs' communications. *See Klayman I*, 4th Am. Compl. ¶ 71; *Klayman II*, 3d Am. Compl. ¶ 77. They also seek a multi-billion dollar award for compensatory, actual, and punitive damages and for attorneys' fees and costs. *Klayman I*, 4th Am. Compl. ¶ 70; *Klayman II*, 3d Am. Compl. ¶ 76.

These cases are before the Court on defendants' consolidated Motion to Dismiss. *See Klayman I* [Dkt. #178]; *Klayman II* [Dkt. #123]. Upon consideration of the parties' submissions, and the entire record herein, defendants' motion is GRANTED and plaintiffs' complaints are DISMISSED with prejudice.

BACKGROUND

Because the controversy surrounding the Government's challenged conduct in these cases has featured prominently in the news media over the last four years, familiarity with this case is likely.[3] I nonetheless will provide a brief background of these two related suits.

A. The Section 215 Bulk Telephony Metadata Program

Section 215 of the USA PATRIOT Act, which governs access to certain "business records," authorizes the Government to apply to the Foreign Intelligence Surveillance Court ("FISC") for an order requiring the "production of any tangible things . . . for an

[3] *See, e.g.*, Ellen Nakashima & Ann E. Marimow, *Judge Says NSA's Call Tracking is Probably Illegal*, WASH. POST, Dec. 17, 2013, A1; Charlie Savage, *Judge Curbs N.S.A. Data Collection*, N.Y. TIMES, Nov. 10, 2015, at A17; *see also infra* p. 12 & n.9.

investigation to protect against," among other things, "international terrorism." Pub. L. No. 107-56, 115 Stat. 272, 287 (2001) (codified at 50 U.S.C. § 1861(a)(1)). In May 2006—after the Government sought and received authorization from judges of the FISC—the NSA began the bulk telephony metadata program that plaintiffs challenge today. *See Klayman I*, Decl. of Acting Assistant Dir. Robert J. Holley, FBI, ¶ 6 [Dkt. #25-5]; *Klayman I*, Decl. of Teresa H. Shea, Signals Intelligence Dir., NSA, ¶ 13 [Dkt. #25-4]. As part of this program, the NSA conducted daily bulk collection, storage, and analysis of telephony metadata. *See id.* From May 2006 until the termination of the program in November 2015, the Government obtained FISC orders directing certain telecommunications service providers to produce, in bulk, call-detail records, which contained metadata about telephone calls, including the time and duration of a call and the dialing and receiving numbers. *Klayman I*, Decl. of Wayne Murphy, Dir. of Operations, NSA, ¶¶ 6–7 ("Murphy Decl.") [Dkt. #178-2]; Murphy Decl. Ex. A ("Aug. 27, 2015 FISC Order"). The FISC orders expressly excluded the content of the call as well as "the name, address, or financial information of a [telephone] subscriber or customer." *See* Aug. 27, 2015 FISC Order at 3 n.1. In total, the FISC authorized the program forty-three times, under orders issued by at least nineteen different FISC judges. *See* Murphy Decl. ¶ 7.

Under the program, once the data was collected, the Government created a repository where data could be accessed and queried by NSA analysts for the purpose of detecting and preventing terrorist attacks. *Id.* ¶¶ 6, 8–9. Among other minimization

procedures[4] designed to protect privacy interests of U.S. citizens, FISC orders authorizing the program required that metadata obtained through the program be destroyed within five years of collection. *Id.* ¶ 11. Beginning in March 2014, however, the FISC authorized the NSA to delay the destruction of metadata that had passed the five-year mark. *Id.* This retention was authorized as a means of allowing the Government to comply with its obligation to preserve potentially relevant evidence under orders issued in two civil cases involving challenges to the legality of the Section 215 program. *See Jewel v. Nat'l Sec. Agency*, No. 4:08-cv-4373-JSW (N.D. Cal. filed Sept. 18, 2008); *First Unitarian Church of L.A. v. Nat'l Sec. Agency*, No. 4:13-cv-3287-JSW (N.D. Cal. filed July 16, 2013); Murphy Decl. ¶ 11.

B. The Bulk Internet-Metadata Program Under FISA's Pen-Trap Provision

Although the surveillance scheme conducted pursuant to FISA's pen-trap provision features less prominently in this litigation than the Section 215 program, a brief history of that program would likely be helpful at this point.

From July 2004 until December 2011, the NSA also engaged in the bulk collection of Internet metadata, authorized by FISC orders issued pursuant to Section 402 of FISA, otherwise known as FISA's pen-register and trap-and-trace provision. *See* 50 U.S.C. § 1842; Murphy Decl. ¶¶ 19–20. Under section 402, the Government collected data from the "to" and "from" lines of e-mails, and the date and time the e-mails were sent, but not

[4] Section 215 requires the Government to comply with FISC-approved procedures that "minimize the retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons consistent with the need . . . to obtain, produce, and disseminate foreign intelligence information." 50 U.S.C. § 1861(b)(2)(B), (c)(1), (g)(2)(A), (h).

the e-mails' content or the "subject" line. *See* Murphy Decl. ¶¶ 19–20. Like the Section 215 program, the Section 402 program allowed the Government to query and analyze the bulk data, with the goal of obtaining foreign intelligence information. *Id.* ¶ 20. Critically, however, the FISC orders required compliance with minimization procedures that limited the retention of the metadata and required "reasonable, articulable suspicion" that the selection terms used in queries were, in fact, associated with foreign terrorist organizations. *Id.* The Section 402 program was ultimately discontinued because it did not meet the Government's operational expectations, and on December 7, 2011, the NSA destroyed all bulk Internet metadata collected as part of the program. *Id.* ¶¶ 20–21. Importantly, the Government has never "disclosed the scope on which the [Section 402] program operated or any of the identities of the providers that received orders from the FISC." *Id.* ¶ 20.

C. Targeted PRISM Collection of Communications Content Under FISA Section 702

As with the surveillance program pursuant to FISA Section 402, a brief overview of the PRISM program is in order.

In 2008, Congress added a new Section 702 to FISA to "supplement[] 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 the communications of non-U.S. persons located abroad." *Clapper v. Amnesty Int'l USA*,

568 U.S. 398, 404 (2013). Under Section 702, upon the FISC's approval[5] of a "certification" by the Government, the Attorney General and Director of National Intelligence may jointly authorize the "targeting of persons reasonably believed to be located outside the United States to acquire foreign intelligence information" for a period of up to one year. 50 U.S.C. § 1881a(a), (g); Murphy Decl. ¶ 23. The text of Section 702, however, expressly prohibits the Government from intentionally targeting a U.S. person overseas or any person known to be in the United States. *See* 50 U.S.C. § 1881a(b); Murphy Decl. ¶¶ 22–23. Section 702 also requires the Government to conduct the data acquisition with the assistance of an electronic communication service provider, and the Government must do so "in a manner consistent with the [F]ourth [A]mendment." 50 U.S.C. § 1881a(b)(5), (g)(2)(A)(vi), (b); Murphy Decl. ¶¶ 22–23.

Unlike the surveillance programs under Section 215 of the USA PATRIOT Act or Section 402 of FISA, Section 702 of FISA is a targeted content-collection program, *not* a bulk collection program. *See* Murphy Decl. ¶¶ 23, 26. As such, PRISM collection can *only* target non-U.S. persons located abroad who possess or are likely to receive or communicate foreign intelligence information authorized for acquisition. *Id.* ¶¶ 22–23.

---

[5] Before the FISC approves a Section 702 certification, it must find that: (1) the Government's targeting procedures are "reasonably designed" to ensure that any acquisition of data is limited to "persons reasonably believed to be located outside the United States" and will not intentionally acquire communications known at the time of acquisition to be purely domestic, 50 U.S.C. § 1881a(b), (i)(2)(B)(i); (2) the Government's certification contains all statutorily required elements, including, *inter alia*, an attestation that a significant purpose of the acquisitions is to obtain foreign-intelligence information, *id.* § 1881a(g)(2)(A)(v), (i)(2)(A); (3) the Government's minimization procedures meet FISA's requirements, *id.* § 1881a(i)(2)(C); and (4) the Government's targeting and minimization procedures are consistent with both FISA and the Fourth Amendment, *id.* § 1881a(i)(3)(A).

The identities of persons targeted under this program are classified, as are the identities of the electronic communications service providers that assist in the acquisition. *Id.* ¶ 27.

D. The Initial Litigation

Shortly after Edward Snowden's disclosure of classified material—which revealed some of the NSA's surveillance programs for the first time[6]—plaintiffs filed suit in both of these cases. *See Klayman I*, Compl., June 6, 2013 [Dkt. #1]; *Klayman II*, Compl., June 12, 2013 [Dkt. #1]. As relevant here, Snowden's "leaks" revealed, among other things, that a FISC order dated April 25, 2013 compelled Verizon Business Network Services ("VBNS") to produce to the NSA on "an ongoing daily basis . . . all call detail records or 'telephony metadata' created by Verizon for communications (i) between the United States and abroad; or (ii) wholly within the United States, including local telephone calls." *Klayman I*, Defs.' Opp'n Pls.' Mots. Prelim. Inj. Ex. F ("Apr. 25, 2013 FISC Order") [Dkt. #25-7]; *see also Klayman I*, Defs.' Opp'n Pls.' Mots. Prelim. Inj. 21 n.9 [Dkt. #25] ("The Government has acknowledged the authenticity of an unlawfully disclosed Secondary Order of the FISC dated April 25, 2013, which listed Verizon Business Network Services, Inc. (VBNS) as a recipient of that order at that time."). As

[6] *See, e.g.*, Glenn Greenwald, *NSA Collecting Phone Records of Millions of Verizon Customers Daily*, THE GUARDIAN (LONDON) (June 5, 2013), https://www.theguardian.com/world/2013/jun/06/nsa-phone-records-verizon-court-order.

subscribers of Verizon, plaintiffs alleged that their communications were likely among those collected through the Government's program.[7]

In general, plaintiffs' original complaints alleged that the Government uses the information collected through the surveillance programs I outlined above to create comprehensive profiles on U.S. citizens, including intimate details about their lives and personal associations. *See, e.g.*, *Klayman II*, 3d Am. Compl. ¶¶ 1–3. According to plaintiffs, the NSA's use of their personal information restricts their "abilities to communicate via telephone, e-mail, social media and otherwise on the Internet, out of

---

[7] The parties to both cases largely overlap, but there are some differences. Larry Klayman ("Klayman"), Charles and Mary Ann Strange ("the Stranges"), and J.J. Little ("Little") and his law firm, J.J. Little & Associates, P.C. (collectively referred to as "the Little Plaintiffs"), are parties to both complaints. *See Klayman I*, 4th Am. Compl. ¶¶ 9–18; *Klayman II*, 3d Am. Compl. ¶¶ 11–19, 22. Klayman, an attorney, is no stranger to the courtroom, having served as a former prosecutor at the U.S. Department of Justice. *Klayman I*, 4th Am. Compl. p. 2. He is also the chairman and general counsel of Freedom Watch, a public interest and advocacy organization. *Id.* ¶ 9. Klayman alleges that he has been a subscriber and user of Verizon Wireless ("Verizon") at all material times, and that because of his public criticism of the Obama administration and his international communications, he believes his communications have "inevitably" been accessed by the Government. *Id.* ¶¶ 9–16.

The Stranges are the father and stepmother of a Navy SEAL who was killed in Afghanistan in 2011. *Id.* ¶ 17. Like Klayman, the Stranges are subscribers of Verizon, and they believe defendants have accessed their phone, Internet, and computer records because they have been vocal about their criticism of President Obama, his administration, and the U.S. military. *Id.* Little is a criminal defense lawyer who has litigated against the Government, which he believes places him "in the line of fire of Government surveillance by the Government Defendants." *Id.* ¶ 18. Little alleges that surveillance of him and his law firm implicates "breaches of attorney-client privilege and work product." *Id.* Little and his firm are subscribers of Verizon Business Network Services ("VBNS") and Verizon.

The complaint in *Klayman II* adds Michael Ferrari ("Ferrari") and Matt Garrison ("Garrison") as additional parties. *Klayman II*, 3d Am. Compl. ¶¶ 20–21. Ferrari and Garrison are private investigators who claim that their communications were certainly monitored by defendants because they frequently engage in e-mail and telephone communications with foreign countries. *Id.* Ferrari alleges that he is a subscriber, consumer, and user of Sprint, Google/Gmail, Yahoo!, and Apple, while Garrison alleges that he is a consumer and user of Facebook, Google, YouTube, and Microsoft products. *Id.*

fear that their confidential, private, and often privileged communications are being and will be overheard by the NSA's surveillance program." *Id.* ¶ 49.

In the most recent versions of the complaints in these two consolidated cases, plaintiffs challenge the NSA's bulk collection of telephony metadata under Section 215, the Section 402 program, the PRISM program, and another program plaintiffs refer to as MUSCULAR.[8] *See Klayman I*, 4th Am. Compl. ¶¶ 44, 46, 51, 54, 59–60, 67; *Klayman II*, 3d Am. Compl. ¶¶ 10, 58, 63–64, 70, 73. In both cases, plaintiffs claim that the challenged surveillance programs violated—and continue to violate—their First, Fourth, and Fifth Amendment rights. *Klayman I*, 4th Am. Compl. ¶¶ 51–53, 58–60, 66–67; *Klayman II*, 3d Am. Compl. ¶¶ 57–58, 62–64, 70–72. With respect to their First Amendment rights, plaintiffs insist that defendants' actions "chill, if not 'kill,' speech by instilling in Plaintiffs and over a hundred million of [sic] Americans the fear that their personal and business conversations with other U.S. citizens and foreigners are in effect tapped and illegally surveyed." *Klayman I*, 4th Am. Compl. ¶ 59; *see also Klayman II*, 3d Am. Compl. ¶ 63. Plaintiffs further allege that their freedoms of expression and association were chilled because they refrained from contacting other people via cell

[8] The record contains little information on the so-called MUSCULAR program, but in *Klayman II*, plaintiffs allege that defendants "authorized broad and intrusive collections of records of individuals through the PRISM and MUSCULAR surveillance programs, thereby giving Defendants authority to obtain telephone and Internet data for a specified amount of time." *Klayman II*, 3d Am. Compl. ¶ 58. They also allege that "through a government program entitled 'MUSCULAR,' the FBI, CIA, and NSA have been intercepting information of the entirety of American citizenry from Internet companies such as Google and Yahoo! as it travels over fiber optic cables from one data center to another." *Id.* ¶ 8. Because plaintiffs treat the MUSCULAR program together with the PRISM program, I will do so as well. *See id.* ¶ 54 ("The Government Defendants, through the use of the continuing PRISM and MUSCULAR programs, illegally and unconstitutionally surveilled each of the Plaintiffs' telephone, Internet and social media communications.").

phone out of fear of retaliation by the Government defendants. *Klayman I*, 4th Am. Compl. ¶ 60; *Klayman II*, 3d Am. Compl. ¶ 64. To support their claim of a Fourth Amendment violation, plaintiffs allege that the challenged surveillance programs constituted unreasonable searches and seizures of their phone records without reasonable suspicion, particularity, or probable cause. *Klayman I*, 4th Am. Compl. ¶¶ 51–53; *Klayman II*, 3d Am. Compl. ¶¶ 70–72. The allegations supporting plaintiffs' Fifth Amendment claim are relatively sparse, but plaintiffs appear to suggest that they have a liberty interest—guaranteed by the Fifth Amendment—in being free from intrusion into their phone records. *Klayman I*, 4th Am. Compl. ¶¶ 65–67; *Klayman II*, 3d Am. Compl. ¶¶ 56–58.

As a result of these alleged violations, plaintiffs assert that they have suffered "severe emotional distress and physical harm, pecuniary and economic damage, loss of services, and loss of society." *Klayman I*, 4th Am. Compl. ¶¶ 55, 61, 68; *Klayman II*, 3d Am. Compl. ¶¶ 59, 65, 74. To remedy these harms, plaintiffs seek compensatory and punitive damages, and attorneys' fees and costs, in excess of $12 billion in *Klayman I*, and in excess of $20 billion in *Klayman II*. *Klayman I*, 4th Am. Compl. ¶ 70; *Klayman II*, 3d Am. Compl. ¶ 76. Both complaints also request injunctive relief that (1) enjoins the challenged surveillance activities; and (2) requires the Government to prepare an accounting of, expunge from Government records, and return to the service providers any

data collected that pertains to plaintiffs' communications. *Klayman I*, 4th Am. Compl. ¶ 71; *Klayman II*, 3d Am. Compl. ¶ 77.

In October 2013, four months after filing their complaints, plaintiffs moved for preliminary injunctions in both cases. *See Klayman I*, Pls.' Mot. Prelim. Inj. [Dkt. #13]; *Klayman II*, Pls.' Mot. Prelim. Inj. [Dkt. #10]. And in December of that year, I enjoined the Government from further collecting plaintiffs' call records. *Klayman v. Obama*, 957 F. Supp. 2d 1, 43–44 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015) (per curiam). In so ruling, I held that plaintiffs Klayman and Charles Strange had standing to challenge both the bulk collection of metadata under these programs and the analysis of that data through the NSA's electronic querying process. *Id.* at 8, 26–29. On the merits, I found it significantly likely that plaintiffs would be able to show that these programs violated their reasonable expectation of privacy and therefore constituted a Fourth Amendment search, and that the searches were unreasonable. *Id.* at 30–42. But in light of the "significant national security interests at stake," I voluntarily stayed my order pending the Government's appeal. *Id.* at 43. To say the least, that opinion unleashed a firestorm of press and public discussion.[9]

E. The USA FREEDOM Act

While my December 2013 injunction in *Klayman I* was stayed pending appeal, the other branches began to grapple with the significant constitutional questions raised by the

[9] *See, e.g.*, Spencer Ackerman, *NSA Collection of Phone Metadata Likely in Breach of Fourth Amendment – Read the Judge's Ruling*, THE GUARDIAN (LONDON) (Dec. 16, 2013), https://www.theguardian.com/world/interactive/2013/dec/16/nsa-collection-phone-metadata-district-court-ruling; Devlin Barrett, *Judge Deals Blow to NSA Phone Spying*, WALL ST. J. (Dec. 16, 2013), https://www.wsj.com/articles/nsa-phone-

NSA's surveillance programs, and they accordingly took steps to weigh in on the issue. In early 2014, President Barack Obama voiced many of the same concerns articulated in my December 2013 opinion. *See* Remarks on United States Signals Intelligence and Electronic Surveillance Programs, 2014 DAILY COMP. PRES. DOC. 30, 2 (Jan. 17, 2014) ("[I]n our rush to respond to a very real and novel set of threats, the risk of Government overreach—the possibility that we lose some of our core liberties in pursuit of security—also became more pronounced."). And in March of that year, he announced that he would seek legislation to replace the Section 215 program with "a mechanism to preserve the capabilities we need without the Government holding this bulk metadata," in order to "give the public greater confidence that their privacy is appropriately protected." Presidential Statement on the National Security Agency's Section 215 Bulk Telephony Metadata Program, 2014 DAILY COMP. PRES. DOC. 213, 1 (Mar. 27, 2014).

---

spying-8216almost-certainly8217-unconstitutional-judge-says-1387222634; Max Ehrenfreund, *Snowden Claims NSA Surveillance 'Collapsing,'* WASH. POST (Dec. 17, 2013), https://www.washingtonpost.com/world/****-security/snowden-claims-nsa-surveillance-collapsing/2013/12/17/7f8f577c-6726-11e3-ae56-22de072140a2_story.html?utm_term=.03094e93ade7; Josh Gerstein, *Judge: NSA Program Likely Unconstitutional*, POLITICO (Dec. 17, 2013), https://www. politico.com/story/2013/12/national-security-agency-phones-judge-101203; David Ingram & Mark Hosenball, *U.S. Judge Says Phone Surveillance Program Likely Unlawful*, CHICAGO TRIBUNE (Dec. 16, 2013), http://articles.chicagotribune.com/2013-12-16/news/sns-rt-us-usa-security-ruling-20131216_1_phone-surveillance-program-metadata-collection-program-u-s-surveillance-court; Kevin Johnson & Richard Wolf, *Federal Judge Rules Against NSA Spying*, USA TODAY (Dec. 16, 2013), https://www.usatoday.com/story/news/nation/2013/12/16/judge-nsa-surveillance-fourth-amendment/4041995/; Charlie Savage, *Judge Questions Legality of N.S.A. Phone Records*, N.Y. TIMES (Dec. 16, 2013), http://www.nytimes.com/2013/12/17/us/politics/federal-judge-rules-against-nsa-phone-data-program.html; David G. Savage, *Judge Says NSA Phone Data Collection Is Probably Unconstitutional*, L.A. TIMES (Dec. 16, 2013), http://www.latimes.com/nation/la-na-nsa-lawsuit-20131217-story.html; Alexandra Sifferlin, *Judge Says NSA Program Likely Unconstitutional*, TIME (Dec. 16, 2013), http://swampland.time.com/2013/12/16/judge-says-nsa-program-likely-unconstitutional/.

Congress, too, responded in kind. On June 2, 2015, it enacted the USA FREEDOM Act, Pub. L. No. 114-23, 129 Stat. 268, which prohibits the Government from obtaining telephony metadata in bulk. *See id.* § 103, 129 Stat. at 272. The President quickly signed the USA FREEDOM Act into law, making the bulk collection of metadata unlawful, effective November 29, 2015. *See id.* §§ 103, 109, 129 Stat. at 272, 276. Importantly, the USA FREEDOM Act amends both Section 402 of FISA *and* Section 215 of the USA PATRIOT Act to prevent bulk collection by the Government. *Id.* § 101, 129 Stat. at 269 ("Additional Requirements for Call Detail Records"); *id.* § 103, 129 Stat. at 272 ("Prohibition on Bulk Collection of Tangible Things"); *id.* § 201, 129 Stat. at 277 ("Prohibition on Bulk Collection"); *see* 50 U.S.C. §§ 1861(b)(2), 1842(c).

In place of bulk collection under Section 215, the USA FREEDOM Act requires targeted searches, whereby the Government must submit an application to the FISC identifying "a specific selection term," such as a telephone number, "to be used as the basis for production" of the call-detail records sought. *See* USA FREEDOM Act §§ 101(a)(3)(C)(i), 103(a), 129 Stat. 270, 272; *see* Murphy Decl. ¶ 14. As part of the NSA's transition to this new targeted collection program, the Government sought authority for—and the FISC approved—the following minimization procedures: (1) the Government would retain certain data in order to comply with its evidence preservation obligations; and (2) the Government would retain a three-month period of technical access, ending on February 29, 2016, so that NSA technical personnel could verify the

accuracy of productions under the new targeted system. *See* Murphy Decl. ¶ 16; Murphy Decl. Ex. B ("Nov. 24, 2015 FISC Order").

F. The Litigation on Remand

Although I enjoined the NSA's surveillance program in December 2013, the Court of Appeals did not issue its opinion until August 28, 2015. When it finally did, it vacated my preliminary injunction on the ground that plaintiffs, as subscribers of Verizon, rather than VBNS—the sole provider the Government has acknowledged as participating in the surveillance program—had not shown a substantial likelihood of standing to pursue their claims. *See Obama v. Klayman*, 800 F.3d 559, 564 (D.C. Cir. 2015) (Brown, J.); *id.* at 565, 568–69 (Williams, J.). As such, the Circuit did *not* address my ruling that the surveillance program likely constituted an unconstitutional search under the Fourth Amendment.

With little time left before the intermediate bulk collection program was set to lapse, plaintiffs moved for—and I granted—leave to file amended complaints to address the standing issue. *See Klayman I*, Min. Entry, Sept. 16, 2015; *Klayman II*, Min. Entry, Feb. 11, 2016. As relevant here, these complaints added the Little Plaintiffs—both of whom allege they have been subscribers to VBNS at all material times—as parties to both actions. *See Klayman I*, 4th Am. Compl. ¶ 18; *Klayman II*, 3d Am. Compl. ¶ 22. Plaintiffs also bolstered the complaint in *Klayman I* by pleading additional facts to support their allegation that Verizon was a participating telecommunications service provider in the challenged surveillance programs. *Klayman I*, 4th Am. Compl. ¶¶ 47–48.

With the Section 215 bulk-collection program set to expire on November 29, 2015, I warned plaintiffs at a status conference on September 2, 2015 that, if they wanted to litigate their Fourth Amendment claims, it was "time to move" because "the clock is running. And there isn't much time . . . ." *Klayman I*, Status Hr'g Tr. 23:6, 15:5–6, Sept. 2, 2015 [Dkt. #143]. Accordingly, on September 21, 2015, plaintiffs renewed their motion for a preliminary injunction against the programs, and also sought to prohibit the Government from destroying "any records relating to the Plaintiffs until this case is tried and all appeals are heard, and only then to purge them from government retention." *Klayman I*, Pls.' Renewed Mot. Prelim. Inj., Proposed Order ("Pls.' Proposed Order") [Dkt. #149-3]. On November 9, 2015, I granted the Little Plaintiffs a preliminary injunction barring bulk collection of records about their calls under Section 215, but I denied relief to the other plaintiffs. *Klayman v. Obama*, 142 F. Supp. 3d 172, 178 (D.D.C. 2015). This time, however, I did not stay my injunction. *Id.* at 198. Not surprisingly, the Government immediately appealed, and our Circuit granted their request for a stay of my injunction pending appeal. Order, *Klayman v. Obama*, No. 15-5307 (D.C. Cir. Nov. 16, 2015), 2015 WL 9010330.

Less than ten days later, the USA FREEDOM Act went into effect, and the Government accordingly moved to vacate the injunction and dismiss their appeal as moot. In an unpublished order dated April 4, 2016, the Court of Appeals granted the Government's motion, vacating the injunction and dismissing the appeal as moot. *See* Order, *Klayman v. Obama*, No. 15-5307 (D.C. Cir. Apr. 4, 2016), Doc. No. 1606954. Once again on remand to this Court, the individual-capacity defendants moved to dismiss

the claims against them for plaintiffs' failure to effect service, and I granted their motions on September 20, 2016. *Klayman I*, 9/20/16 Mem. Order [Dkt. #175]; *Klayman II*, 9/20/16 Mem. Order [Dkt. #120].

Because plaintiffs' complaints have been amended several times since defendants' motions for partial dismissal were filed in January of 2014, I ordered defendants to brief a renewed dispositive motion. *See Klayman I*, 9/20/16 Mem. Order at 4–5. The Government accordingly filed a consolidated motion to dismiss both *Klayman I* and *Klayman II* for lack of jurisdiction. The Government's motion is now ripe for my decision.

STANDARD OF REVIEW

Article III of the Constitution limits the judicial power of the United States to adjudicating "cases" and "controversies." *Valley Forge Christian Coll. v. Ams. United for Separation of Church & State, Inc.*, 454 U.S. 464, 471 (1982). "Three inter-related judicial doctrines—standing, mootness, and ripeness, ensure that federal courts assert jurisdiction only over '[c]ases' and '[c]ontroversies'" consistent with their authority under Article III. *Williams v. Lew*, 77 F. Supp. 3d 129, 132 (D.D.C. 2015) (internal quotation marks omitted). Importantly here, the Supreme Court has noted that the standing inquiry is "especially rigorous when reaching the merits of the dispute would force [the judiciary] to decide whether an action taken by one of the other two branches of the Federal Government was unconstitutional." *Raines v. Byrd*, 521 U.S. 811, 819–20 (1997). This is, of course, because "[r]elaxation of standing requirements is directly related to the expansion of judicial power." *United States v. Richardson*, 418 U.S. 166,

188 (1974) (Powell, J., concurring). And regardless of whether a plaintiff had standing to sue when he initially filed his complaint, the doctrine of mootness bars a federal court from adjudicating that plaintiff's claim if "events have so transpired that the [court's] decision will neither presently affect the parties' rights nor have a more-than-speculative chance of affecting them in the future." *Chamber of Commerce v. EPA*, 642 F.3d 192, 199 (D.C. Cir. 2011) (quoting *Clarke v. United States*, 915 F.2d 699, 701 (D.C. Cir. 1990)).

Here, defendants have filed a motion to dismiss pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure, and thus they seek dismissal of plaintiffs' complaints based on lack of subject matter jurisdiction. Under Rule 12(b)(1), "[a] defendant may make a factual attack on the Court's subject matter jurisdiction . . . as opposed to a facial attack based solely on the complaint." *Finca Santa Elena, Inc. v. U.S. Army Corps of Eng'rs*, 873 F. Supp. 2d 363, 368 (D.D.C. 2012). When a defendant makes a factual attack on jurisdiction—as defendants do here—"no presumption of truthfulness applies to the factual allegations" in the plaintiff's complaint. *Richards v. Duke Univ.*, 480 F. Supp. 2d 222, 232 (D.D.C. 2007) (quoting *Ohio Nat'l Life Ins. Co. v. United States*, 922 F.2d 320, 325 (6th Cir. 1990)). I therefore am "not obliged to accept [plaintiffs'] allegations as true and may examine evidence to the contrary and reach [my] own conclusion on the matter." *Finca Santa Elena, Inc.*, 873 F. Supp. 2d at 368 (quoting 5B Charles Alan Wright & Arthur Miller, *Federal Practice and Procedure* § 1350 (3d ed. 2004)).

ANALYSIS

A. Plaintiffs' Challenge to Section 215 Surveillance

1. Plaintiffs' Claims for Declaratory and Prospective Injunctive Relief

Defendants argue that the statutorily mandated cessation of the Section 215 bulk collection program has mooted plaintiffs' claims for declaratory and prospective injunctive relief. *See Klayman I*, Defs.' Reply Supp. Mot. Dismiss *Klayman I & Klayman II* for Lack of Subj. Matter Jurisdiction 3 [Dkt. #184]. Because the Government's challenged conduct is now prohibited—both by federal statute and by an order of the FISC—I agree with defendants that plaintiffs' challenge to the Section 215 program no longer presents an Article III case or controversy.

As discussed above, the USA FREEDOM Act—which was largely motivated by the same concerns I articulated in my December 2013 opinion in this case[10]—expressly prohibits the bulk collection of telephony metadata under Section 215. *See* USA FREEDOM Act §§ 103, 109, 129 Stat. at 272, 276; 50 U.S.C. § 1861(c)(3). Effective November 29, 2015, the bulk collection of telephony metadata authorized under Section 215 was replaced by a process for targeted production of call-detail records by telecommunications service providers, pursuant to FISC order. USA FREEDOM Act § 101, 129 Stat. at 269–70; Murphy Decl. ¶ 13. In accordance with Congress's directive

[10] *See, e.g.*, Mark Coppenger, *Snowdenism: A Moral Assessment*, PROVIDENCE, Spring 2017, at 37, 39 ("Although Judge Leon's ruling was later overturned by an appeals court on a technicality, Congress enacted major reforms to the program based on many of the same concerns."); Alan Rubel, *Legal Archetypes and Metadata Collection*, 34 WIS. INT'L L.J. 823, 837–38 (2017) ("The legislation was inspired by the controversy surrounding the bulk metadata program, and makes important modifications to the business records provisions upon which the program was based.").

in the USA FREEDOM Act, the final FISC order authorizing bulk collection of telephony metadata under Section 215 expired on November 28, 2015. *See* Aug. 27, 2015 FISC Order at 4. Despite the November 29, 2015 deadline, on November 24, 2015, the FISC authorized temporary, limited access to the collected metadata by NSA personnel through February 29, 2016, but it did so "solely for the purpose of verifying the completeness and accuracy of call detail records produced under the targeted (i.e., non-bulk) production orders" issued by the FISC under the USA FREEDOM Act's targeted collection program. Nov. 24, 2015 FISC Order at 6. And even this limited access ended over twenty months ago. *Id.*

Both of plaintiffs' requests for declaratory and prospective injunctive relief are accordingly mooted by this change in law. First, plaintiffs' request for a "cease and desist order to prohibit" the bulk collection of their telephony metadata under Section 215 is moot because the USA FREEDOM Act prohibits bulk collection. *See Klayman I*, 4th Am. Compl. ¶ 71. Indeed, "[i]t is well established that a case must be dismissed as moot if new legislation addressing the matter in dispute is enacted while the case is still pending." *Am. Bar Ass'n v. Fed. Trade Comm'n*, 636 F.3d 641, 643 (D.C. Cir. 2011). Second, plaintiffs' request for a "cease and desist order to prohibit" the NSA from querying plaintiffs' metadata allegedly collected pursuant to Section 215 is also moot because the FISC has prohibited the NSA from accessing this data for intelligence analysis purposes. *See Klayman I*, 4th Am. Compl. ¶ 71; *Klayman II*, 3d Am. Compl. ¶ 47; Nov. 24, 2015 FISC Order at 6; Murphy Decl. ¶ 17. Because of this intervening action by Congress and the FISC, it is clear that a decision by this Court would "neither

presently affect" plaintiffs' rights nor "have a more-than-speculative chance of affecting them in the future," and thus plaintiffs' claims no longer present a live Article III case or controversy. *Chamber of Commerce*, 642 F.3d at 199 (quoting *Clarke*, 915 F.2d at 701).

Plaintiffs rejoin that the voluntary-cessation exception to the mootness doctrine applies here, and thus that their claims are not moot. *Klayman I*, Pls.' Opp'n to Defs.' Mot. Dismiss *Klayman I & Klayman II* for Lack of Subj. Matter Jurisdiction 14–15 ("Pls.' Opp'n") [Dkt. #182]. I disagree. "The rationale supporting voluntary cessation as an exception to mootness is that, without an order from the Court preventing [the defendant] from continuing the allegedly illegal practice, the defendant [would be] free to return to its old ways—thereby subjecting the plaintiff to the same harm but, at the same time, avoiding judicial review." *Jackson v. U.S. Parole Comm'n*, 806 F. Supp. 2d 201, 207-08 (D.D.C. 2011) (internal quotation marks omitted). Here, defendants are plainly not "free" to reinstitute the Section 215 bulk collection program because the USA FREEDOM Act expressly bars them from doing so. *Cf. Am. Bar Ass'n*, 636 F.3d at 648 ("[When] intervening legislation simply nullifie[s] the [agency program] . . . . [, t]his scenario is not within the compass of the voluntary cessation exception to mootness."); *Campbell v. Clinton*, 203 F.3d 19, 34 n.14 (D.C. Cir. 2000) ("The President's cessation of the attack on Yugoslavia was not 'voluntary' within the [Supreme] Court's meaning [of voluntary cessation]; the war ended because the United States won, not because the President sought to avoid litigation."). And even if the Government attempted to restart the program by seeking FISC approval of a bulk collection of telephony metadata, the FISC could not grant the request. *See* Nov. 24, 2015 FISC Order at 3 (noting that the

USA FREEDOM Act "clearly forecloses the issuance [of orders permitting] additional bulk collection after November 28, 2015" (emphasis omitted)). The voluntary cessation exception to the mootness doctrine therefore does not apply in this case.[11]

Plaintiffs again counter that the USA FREEDOM Act is "riddled with loopholes" that would "allow the intelligence agencies to collect all kinds of personal data without prior court approval." Pls.' Opp'n 13, 26. As an example of a loophole that "create[s] plenty of 'wiggle room' for the intelligence agencies to continue to operate unchecked," plaintiffs cite Section 102 of the USA FREEDOM Act. *Id.* at 12. That Section provides that the Attorney General may require the "emergency production" of documents or other tangible things without a FISC order, for a period not to exceed seven days, if he "reasonably determines that the factual basis for the issuance of [a FISC] order under [Section 215] to approve such production of tangible things exists." USA FREEDOM Act § 102, 129 Stat. at 271; 50 U.S.C. § 1861(i)(l)(B); Pls.' Opp'n 13. But even under this emergency exception, the statute is clear that the Attorney General has no authority to require bulk collection; he may authorize collection based only on specific selection terms that he reasonably determines to be associated with foreign terrorist activity. *See* USA FREEDOM Act § 102, 129 Stat. at 271; 50 U.S.C. § 1861(i)(l)(B). And the

[11] Plaintiffs also insist that the Government has engaged in a "pattern and practice of deception and disregard for the law," such that "[p]laintiffs have clearly established at minimum 'reasonable probability' that future harm will arise." Pls.' Opp'n 17. Plaintiffs have not, however, identified any factual basis to support their claim that defendants have engaged in a pattern of deception. And this Court must "presume that government officials will conduct themselves properly and in good faith." *In re Navy Chaplaincy*, 850 F. Supp. 2d 86, 94 (D.D.C. 2012). But as I have already noted, even if defendants were attempting to deceive this Court, and even if they tried to resurrect the Section 215 bulk collection program in the future, the FISC could *not* sanction bulk surveillance. *See* Nov. 24, 2015 FISC Order at 3. Plaintiffs' argument accordingly fails on this point.

Attorney General's determinations are, of course, subject to mandatory review by the FISC. *See* USA FREEDOM Act § 102, 129 Stat. at 271; 50 U.S.C. § 1861(i)(1)(C). Thus, plaintiffs' fear that the USA FREEDOM Act "in many ways actually *expands* the scope of wide-scale unconstitutional surveillance" is unsupported by the text of the statute. Pls.' Opp'n 12.

Plaintiffs' final argument on this point is that they should at least be permitted to engage in jurisdictional discovery in order to show that their telephony metadata was collected and queried as part of the Section 215 program. *Id.* at 17. Unfortunately for plaintiffs, the facts they seek to obtain through discovery cannot possibly establish jurisdiction in this case. To obtain jurisdictional discovery, plaintiffs are required to make a "detailed showing" that "include[s] *some* facts about what additional discovery could produce" to establish jurisdiction. *Shaheen v. Smith*, 994 F. Supp. 2d 77, 89 (D.D.C. 2013). Without such a showing, it would be "'inappropriate to subject [defendants] to the burden and expense of discovery'" before dismissing this case on jurisdictional grounds. *App Dynamic ehf v. Vignisson*, 87 F. Supp. 3d 322, 329 (D.D.C. 2015) (quoting *Atlantigas Corp. v. Nisource*, 290 F. Supp. 2d 34, 53 (D.D.C. 2003)). Here, plaintiffs have identified the discovery they wish to pursue: evidence showing whether their metadata was collected as part of the Section 215 bulk collection program. Pls.' Opp'n 6, 17–18. But even if plaintiffs were able to establish—through jurisdictional discovery—that the NSA had, in fact, collected their telephony metadata, they still would not be able to overcome the jurisdictional defect in this case. Because bulk collection under Section 215 is now prohibited by statute, plaintiffs' claims for injunctive relief

against bulk collection are moot, regardless of whether the Government *actually* collected and queried plaintiffs' telephony metadata pursuant to the Section 215 program in the past. Plaintiffs' request for jurisdictional discovery is accordingly denied, and their claims for declaratory and prospective injunctive relief related to the Section 215 bulk collection program must be dismissed as moot.

2. Plaintiffs' Claim for Expungement

In addition to their request for injunctions against further bulk collection and querying of their telephony metadata, plaintiffs also request that any of their metadata that was collected pursuant to Section 215 be "expunged from federal government records." *Klayman I*, 4th Am. Compl. ¶ 71; *Klayman II*, 3d Am. Compl. ¶ 77. Because I conclude that plaintiffs lack standing to pursue this injunctive relief, their request must also be denied.

To establish Article III standing, plaintiffs must show, among other things, that their injury is "'fairly trace[able] . . . to the challenged action' of [defendants]." *Bhd. of Locomotive Eng'rs v. Surface Transp. Bd.*, 457 F.3d 24, 28 (D.C. Cir. 2006) (quoting *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992)). Importantly, an Article III court may only redress injury "'that fairly can be traced to the challenged action of the defendant, and not injury that results from the independent action of some third party not before the court.'" *Nw. Airlines, Inc. v. Fed. Aviation Admin.*, 795 F.2d 195, 203–04 (D.C. Cir. 1986) (quoting *Simon v. E. Ky. Welfare Rights Org.*, 426 U.S. 26, 41–42 (1976)). Similarly, our Circuit has "consistently held that self-inflicted harm doesn't

satisfy the basic requirements for standing." *Nat'l Family Planning & Reprod. Health Ass'n v. Gonzales*, 468 F.3d 826, 831 (D.C. Cir. 2006).

Here, defendants have retained the remaining call-detail records at the request of plaintiffs—in this litigation—and third parties in other similar cases. As discussed above, the FISC's November 24, 2015 order required the Government to destroy all bulk telephony metadata produced under the Section 215 program once its preservation obligations in civil litigation had been lifted. *See* Murphy Decl. ¶ 18; Nov. 24, 2015 FISC Order at 8. And as of the date of this opinion, the only metadata that the Government still retains from its bulk collection under Section 215 is metadata that is subject to a preservation obligation in this and other litigation. Murphy Decl. ¶ 18. Indeed, it was plaintiffs who explicitly requested that this Court enter an order that would prohibit defendants from "destroy[ing] any records relating to the Plaintiffs until this case is tried and all appeals are heard." *Klayman I*, Pls.' Renewed Mot. Prelim. Inj. Proposed Order [Dkt. #149-3]. And the same is true in the other civil litigation concerning the Government's challenged surveillance programs. *See, e.g.*, Preservation Order A, D, *Jewel*, No. 4:08-cv-4373-JSW (N.D. Cal. Nov. 16, 2009); Preservation Order A, E, *First Unitarian Church*, No. 4:13-cv-3287-JSW (N.D. Cal. Mar. 21, 2014).[12] As such, any injury plaintiffs may suffer as a result of this retention is either self-inflicted or traceable

[12] But even without such an order, defendants are correct that they have "a duty 'to preserve potentially relevant evidence,'" and that they run the risk of sanctions if they fail to do so. *Zhi Chen v. District of Columbia*, 839 F. Supp. 2d 7, 12 (D.D.C. 2011) (quoting *D'Onofrio v. SFX Sports Grp., Inc.*, No. 06-687, 2010 WL 3324964, at *5 (D.D.C. Aug. 24, 2010)). Plaintiffs are essentially requesting that this Court order defendants both to preserve the remaining metadata they collected under Section 215 for the purposes of this litigation, and to destroy that very same metadata. Particularly in light of defendants' court-ordered preservation obligations, I will not grant this seemingly contradictory demand.

to the actions of third parties who are not before this Court. Plaintiffs accordingly lack standing to pursue their claims for expungement of the remaining bulk telephony metadata.

B. Plaintiffs' Challenge to FISA's Pen-Trap Provision

In addition to their challenges to the Government's now defunct surveillance program under Section 215 of the USA PATRIOT Act, plaintiffs seek a "cease and desist order to prohibit" the NSA from collecting or querying bulk Internet metadata pursuant to Section 402 of FISA, and an order requiring the "expunge[ment] from federal government records" of any data the NSA collected as part of this program. *Klayman II*, 3d Am. Compl. ¶ 77. Defendants insist that plaintiffs' claims do not present an Article III case or controversy because the NSA ceased FISC-authorized bulk collection of Internet metadata—and destroyed all metadata collected pursuant to Section 402—in December of 2011. *See Klayman I*, Defs.' Mem. Supp. Mot. Dismiss *Klayman I* & *Klayman II* for Lack of Subj. Matter Jurisdiction 31 ("Defs.' Mem.") [Dkt. #178-1]. Unfortunately for plaintiffs, defendants are correct.

Eighteen months *before* plaintiffs filed this suit, the NSA had already discontinued its bulk collection program under FISA and destroyed the accumulated metadata. *See* Murphy Decl. ¶¶ 19–21. And four years after the Section 402 program was discontinued, Congress enacted the USA FREEDOM Act, which prohibits bulk collection of metadata under FISA's pen-trap provision. USA FREEDOM Act § 201, 129 Stat. at 277; 50 U.S.C. § 1842(c)(3). Thus, even assuming that plaintiffs' Internet metadata had been collected pursuant to Section 402, this Court could not grant plaintiffs the relief they

request because that metadata was destroyed eighteen months prior to the filing of plaintiffs' complaints. As such, plaintiffs have failed to show an injury that could be redressed by the injunctive relief they request, and this Court accordingly lacks jurisdiction to hear their claim.[13]

Plaintiffs insist that this Court should not credit the evidence defendants have presented to show that bulk data collection under Section 402 ended in 2011. They assert that the declaration of Wayne Murphy, the Director of Operations of the NSA, "is hardly credible evidence, particularly since the NSA has a history of deceit, lying to this and other courts, and lawless conduct." Pls.' Opp'n 19. They insist that "[i]f Director of National Intelligence James Clapper is willing to lie and commit perjury, under oath, before Congress," I should not take Murphy's declaration at face value. *Id.* Unfortunately for plaintiffs, these accusations fall far short of satisfying their burden under Federal Rule of Civil Procedure 12(b)(1). Once the Government introduced Murphy's declaration, the burden shifted to plaintiffs to prove "by a preponderance of the evidence that the [C]ourt has subject matter jurisdiction to hear the case." *Harris v. Koenig*, 722 F. Supp. 2d 44, 49 (D.D.C. 2010). Plaintiffs, however, have not pointed to any evidence to contest Murphy's sworn statement that the bulk collection of Internet

[13] Plaintiffs alternatively argue that the voluntary cessation exception to the mootness doctrine applies here because defendants voluntarily discontinued the program and destroyed the related metadata. Pls.' Opp'n 19. But because defendants discontinued the program and destroyed the related metadata eighteen months *before* plaintiffs even filed these suits, the mootness doctrine—let alone the voluntary cessation exception to that doctrine—does not apply. *See, e.g.*, *Friends of the Earth, Inc. v. Laidlaw Envt'l Servs.*, 528 U.S. 167, 191 (2000) ("[B]y the time mootness is an issue, the case has been brought and litigated."). Additionally, there is no risk that defendants could reinstitute the bulk Internet metadata collection program because it has been prohibited by the USA FREEDOM Act. *See* USA FREEDOM Act § 201, 129 Stat. at 277; 50 U.S.C. § 1842(c)(3). Plaintiffs' argument on this point is accordingly of no avail.

metadata was discontinued in 2011. As such, plaintiffs have failed to refute the Government's Rule 12(b)(1) evidence, and they therefore have not established a live Article III case or controversy as to the surveillance program conducted under Section 402.

C. Plaintiffs' Challenge to the PRISM Program

Plaintiffs next challenge the PRISM program, which—unlike the Section 215 program or the bulk collection of Internet metadata pursuant to Section 402 of FISA—is an ongoing targeted collection program conducted under FISA Section 702. *See* 50 U.S.C. § 1881a. As discussed above, under the PRISM program, the Government uses selectors—like e-mail addresses of non-U.S. persons located abroad—to collect online communications. *See* Murphy Decl. ¶¶ 22–26. Plaintiffs generally allege that defendants unconstitutionally intercepted their telephonic and Internet communications pursuant to the PRISM program. *Klayman II*, 3d Am. Compl. ¶¶ 41, 53. And while plaintiffs' arguments on this point are slightly re-packaged, they are largely the same as those I addressed in my first opinion in this case.

In my December 2013 opinion granting plaintiffs' motion for a preliminary injunction, I rejected plaintiffs' challenges to the PRISM program on the ground that they did not allege sufficient facts to show that the NSA had actually targeted any of their communications. *Klayman*, 957 F. Supp. 2d at 8 n.6. I based my ruling on the Supreme Court's decision in *Clapper*, 568 U.S. at 398, in which the Court concluded that the plaintiffs in that case lacked standing to challenge the very same statutory provision as the one challenged here. That was so, according to the Court, because it was speculative

whether "potential future surveillance is certainly impending or is fairly traceable to § 1881a." *Clapper*, 568 U.S. at 414. In rejecting plaintiffs' claims, I noted that "plaintiffs here have not even alleged that they communicate with anyone outside the United States at all, so their claims under Section 702 are even less colorable than those of the plaintiffs in *Clapper*." *Klayman*, 957 F. Supp. 2d at 8 n.6 Although plaintiffs have since amended their complaint in *Klayman II* to bolster their claim of standing on this basis, I find that they still fail to allege facts sufficient to satisfy their Article III burden.

In the most recent version of their complaint in *Klayman II*, plaintiffs allege specific facts intended to show that they do, in fact, communicate with persons abroad who are likely to have been monitored under the PRISM program. Specifically, plaintiffs claim that "Klayman frequents and routinely telephones and e-mails individuals and high-ranking government officials in Israel, a high-conflict area where the threat of terrorism is always present." *Klayman II*, 3d Am. Compl. ¶ 12. Klayman proceeds to list various meetings and communications he has had with persons in Israel, Spain, the United Kingdom, and several other European nations "which have very large Muslim populations and where terrorist cells are located." *Id.* ¶¶ 12-17. He also recounts an occasion in which he was participating in a radio interview about the NSA, when the show experienced "a tech meltdown." *Id.* ¶ 16. Klayman states—in conclusory fashion—that this event made "clear that the NSA was attempting to harass him." *Id.* The Stranges have also bolstered their standing claim by alleging that they "make telephone calls and send and receive e-mails to and from foreign countries" and that they "have received threatening e-mails and texts from overseas, in particular Afghanistan."

Id. ¶19. The other remaining plaintiffs variously allege that they make and receive telephone calls and send and receive e-mails to and from foreign countries. *Id.* ¶¶ 20-21. Based on these new allegations, plaintiffs insist that they have "pled specific facts that strongly support [their] contention that their metadata was collected under the PRISM Program, and that it remains substantially at risk of such collection." Pls.' Opp'n 22. I disagree.

Notwithstanding these efforts to salvage their suit, plaintiffs' allegations remain plainly insufficient under the standard the Supreme Court articulated in *Clapper*. In *Clapper*, the plaintiffs alleged that the very fact that the PRISM program was operational gave them "no choice but to *assume* that any of [their] international communications *may* be subject to government surveillance, and [they] have to make decisions . . . in light of that *assumption*." 568 U.S. at 411. The Supreme Court rejected these allegations out of hand, reasoning that the plaintiffs had "set forth no specific facts demonstrating that the communications of their foreign contacts will be targeted." *Id.* at 412. The Court ultimately concluded that there were too many steps in the plaintiffs' speculative chain of causation for their claims to pass muster under Article III, especially because Section 1881a "at most *authorizes*—but does not *mandate* or *direct*—the surveillance that [plaintiffs] fear." *Id.*

The Court proceeded to set forth four additional breaks in the *Clapper* plaintiffs' chain of causation that doomed their standing. First, even if the plaintiffs could show that their foreign contacts would be targeted, they had no facts showing that the Government would use the PRISM program, rather than other methods of surveillance, to do so. *Id.*

Second, even if the plaintiffs could show that the Government would seek FISC authorization to surveil their foreign contacts under the PRISM program, they could do nothing more than speculate as to whether the FISC would actually authorize that surveillance. *Id.* at 413. Third, even if the Government were to obtain FISC approval, the plaintiffs set forth no facts to support the conclusion that the Government would succeed in obtaining the targeted communications. *Id.* at 414. And fourth, even if the plaintiffs could demonstrate that the Government would successfully obtain communications of their foreign contacts, they pleaded no facts suggesting that the plaintiffs' own communications with those foreign contacts would be incidentally collected. *Id.* Thus, the Court concluded that the *Clapper* plaintiffs' speculative chain of causation failed to satisfy Article III.

The same is true here. In fact, most of plaintiffs' allegations that they communicate with unidentified persons in foreign countries fall far short even of the *Clapper* plaintiffs' allegations, which the Supreme Court held to be inadequate. Among other defects, plaintiffs here have not alleged any facts tending to show that: (1) their foreign contacts would be targeted by the PRISM program; (2) defendants would seek FISC authorization to surveil their foreign contacts under the PRISM program; (3) defendants would actually succeed in obtaining communications from plaintiffs' foreign contacts; or (4) plaintiffs' communications with their foreign contacts would be among those collected pursuant to the PRISM program. *See Clapper*, 568 U.S. at 411–414. While Klayman has alleged more facts than the other plaintiffs to support his challenge to the PRISM program, his assertions that his foreign contacts have, in fact,

been targeted by the Government under the PRISM program "are necessarily conjectural," because the identities of PRISM targets are classified. *Id.* at 412; Murphy Decl. ¶27.

Plaintiffs take issue with this line of reasoning, arguing that, by classifying the identities of persons targeted by the PRISM program, the Government is able to "escape liability for [its] illegal activities," by depriving plaintiffs of the evidence they need to establish Article III standing. Pls.' Opp'n 23. But the Supreme Court expressly rejected this very same argument in *Clapper*. First, the Court noted that "[t]he assumption that if [plaintiffs] have no standing to sue, no one would have standing, is not a reason to find standing." *Clapper*, 568 U.S. at 420 (internal quotation marks omitted). Second, the Court recognized that the PRISM program was not insulated from judicial review because "Congress created a comprehensive scheme in which the [FISC] evaluates the Government's certifications, targeting procedures, and minimization procedures—including assessing whether the targeting and minimization procedures comport with the Fourth Amendment." *Id.* at 421. Therefore, while plaintiffs may disagree with Congress's decision to enact Section 1881a—and they may be dissatisfied with the FISC's rulings pursuant to that statute—these issues are irrelevant to my assessment of plaintiffs' standing in this case. *Id.* Plaintiffs' challenge to the PRISM program is accordingly dismissed.

D. Plaintiffs' Constitutional Claims for Damages

Finally, plaintiffs attempt to advance constitutional tort claims for compensatory and punitive damages. Specifically, they assert *Bivens* claims against both the individual

defendants—who have since been dismissed from this action—as well as the Government defendants for violations of their First, Fourth, and Fifth Amendment rights. *Klayman I*, 4th Am. Compl. ¶¶ 49–69; *Klayman II*, 3d Am. Compl. ¶¶ 55–75. The Government insists, however, that I lack jurisdiction to hear plaintiffs' claims because they are barred by sovereign immunity. Defs.' Mem. 38. I agree.

"[I]t is well established that '[a]bsent a waiver, sovereign immunity shields the Federal Government and its agencies from suit.'" *Debrew v. Atwood*, 792 F.3d 118, 124 (D.C. Cir. 2015) (quoting *FDIC v. Meyer*, 510 U.S. 471, 475 (1994)). The burden of proving that the Government has unequivocally waived its immunity belongs to plaintiffs, and that waiver must be "unequivocally expressed in the statutory text." *Tri-State Hosp. Supply Corp. v. United States*, 341 F.3d 571, 575 (D.C. Cir. 2003). Here, plaintiffs have identified no statutory waiver of sovereign immunity that would allow a claim for money damages against the Government in these circumstances.

And this omission in plaintiffs' briefing is not surprising, given the fact that "federal constitutional claims for damages are cognizable only under *Bivens*, which runs against individual governmental officials personally." *Loumiet v. United States*, 828 F.3d 935, 945 (D.C. Cir. 2016); *see also Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388 (1971). Although plaintiffs insist that they have plans to "file a motion . . . to serve the Individual Defendants, in their individual capacities" to "allow this crucial matter to proceed substantively," the fact remains that the individual defendants were dismissed from this case, and thus plaintiffs' constitutional claims

against them cannot proceed.[14] Pls.' Opp'n 26; *see Klayman I*, 9/20/16 Mem. Order ("[T]he complaint is DISMISSED as to the individual federal defendants."); *Klayman II*, 9/20/16 Mem. Order ("[T]he complaint is DISMISSED as to the government officials in their individual capacities."). Because "sovereign immunity is jurisdictional in nature"—and I conclude that the Government has not waived its sovereign immunity here—I lack jurisdiction to assess plaintiffs' constitutional damages claims. *Tri-State Hosp. Supply Corp.*, 341 F.3d at 575.

CONCLUSION

While the zeal and vigilance with which plaintiffs have sought to protect our Constitutional rights is indeed laudable, this Court, in the final analysis, has no choice but to dismiss these cases for plaintiffs' failure to demonstrate the necessary jurisdiction to proceed. I do so today, however, well aware that I will not be the last District Judge who will be required to determine the appropriate balance between our national security and privacy interests during this never-ending war on terror. Hopefully by the time these issues are next joined, our Supreme Court will have had the opportunity to provide us with further guidance on the parameters of our privacy interests in this era of ever-increasing electronic communication. If not, concerned citizens such as these will

[14] It is worth noting that, even if the individual federal defendants were properly before this Court as defendants, recent Supreme Court precedent makes it unclear whether plaintiffs could even maintain a *Bivens* action against them at all. *Cf. Ziglar v. Abbasi*, 137 S. Ct. 1843, 1857 (2017) ("[T]he Court has made clear that expanding the *Bivens* remedy is now a 'disfavored' judicial activity. This is in accord with the Court's observation that it has consistently refused to extend *Bivens* to any new context or new category of defendants. Indeed, the Court has refused to do so for the past 30 years." (internal citations and quotation marks omitted)).

continue to shoulder the heavy yoke that vigilance to our Constitutional liberties surely requires.

Thus, for all the reasons stated herein, Defendants' Motion to Dismiss is GRANTED. Plaintiffs' complaints are both DISMISSED with prejudice. A separate Order consistent with this decision accompanies this Memorandum Opinion.

RICHARD J. LEON
United States District Judge