IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA
Alexandria Division

SHARYL THOMPSON ATTKISSON, et al.,	)	
	)	
Plaintiffs,	)	
	)	
v.	)	No. 1:17-cv-364 (LMB/JFA)
	)	
ERIC HIMPTON HOLDER, JR., et al.,	)	
	)	
Defendants.	)	

MEMORANDUM OPINION

Before the Court is defendants Eric Holder ("Holder") and Patrick Donahoe's ("Donahoe") (collectively, "defendants") Motion to Dismiss, in which they argue that all eight counts in the Complaint should be dismissed under Fed. R. Civ. P. 12(b)(1) or 12(b)(6) or, in the alternative, on the basis of qualified immunity. For the reasons that follow, Count 4 will be dismissed under Rule 12(b)(6) as to all defendants, Counts 7 and 8 will be dismissed under Rule 12(b)(1) as to all defendants, and Counts 1-3 and 5-6 will be dismissed under Rule 12(b)(6) only as to defendants Holder and Donahoe. Because the Court finds that the Rule 12(b)(1) and 12(b)(6) grounds provide a sufficient basis for dismissal, the Court declines to address defendants' immunity arguments.

I. BACKGROUND

In this civil action, plaintiffs Sharyl Attkisson ("Attkisson"), James Attkisson, and Sarah Attkisson (collectively, "plaintiffs") claim that defendants Holder, Donahoe, and Unknown Named Agents of the Department of Justice, United States Postal Service, and the United States

("John Does" or "John Doe agents")[1] violated a variety of their constitutional, statutory, and common law rights by conducting unauthorized electronic surveillance of plaintiffs' home and electronic devices. See Compl.[2] ¶¶ 1-2.

During the time relevant to this action, Attkisson was an investigative reporter for CBS News who covered, among other stories, the federal gun-trafficking investigation known as "Fast and Furious" and the attack on the American diplomatic compound in Benghazi. Id. ¶ 6. Plaintiffs James and Sarah Attkisson, both of whom live with Attkisson, are Attkisson's husband and daughter, respectively. Id. ¶¶ 7-8. Defendants Holder and Donahoe were, at the relevant time, the Attorney General and Postmaster General of the United States. Id. ¶¶ 9-10. In those positions, Holder oversaw the Department of Justice ("DOJ"), including the Federal Bureau of Investigation ("FBI") and the Bureau of Alcohol, Tobacco, Firearms, and Explosives ("ATF"), and Donahoe oversaw the United States Postal Service ("USPS").

In 2011, Attkisson, who had been a reporter with CBS for twenty years, began investigating a story about the ATF allowing firearms dealers to sell weapons to straw purchasers to enable the ATF to track the firearms back to higher-up figures in Mexican drug cartels. See id. ¶ 14 & n.2. Attkisson's first report on this story, which eventually became known as the "Fast

[1] It is unclear from the Complaint exactly how the John Does are being sued. In the caption, all defendants are specifically described as being sued "Individually" or "in their individual capacities," Compl. [Dkt. No. 117] 1, and Counts 1 and 2 are brought "against Defendants in their individual capacity and not their official capacity," id. ¶ 1; however, the Complaint does not specify whether Counts 3 through 8 are brought against defendants individually or in their official capacities, see id. ¶ 2. The Complaint alleges that plaintiffs "are unaware of the true names and capacities, whether individual or otherwise, of the Unknown Federal Agents referenced in the caption." Id. ¶ 11. Because defendants' attorneys have only noticed an appearance on behalf of Donahoe and Holder (and the United States of America, although it is no longer a defendant), the present Motion to Dismiss applies only to the claims against Holder and Donahoe.

[2] All references to the "Complaint" and citations to "Compl." are to plaintiffs' "Consolidated Complaint," filed on September 15, 2017 [Dkt. No. 117], which is the only operative complaint in this civil action.

and Furious" story, aired on CBS on February 22, 2011. Id. ¶ 15. The story relied on a variety of confidential sources critical of the program. Id. Throughout 2011, Attkisson continued reporting on the program, allegedly in the face of considerable efforts from the ATF, FBI, and DOJ to stymie her reporting.[3] Over the year, the story expanded to include apparent discrepancies in the FBI's accounting of evidence in a related murder of a Border Patrol agent, id. ¶¶ 18-21, alleged problems with Holder's "sworn testimony" (presumably before Congress), id. ¶ 22, and the DOJ's retraction of a letter it had previously sent to Congress that contained misinformation about the program, id. ¶ 24.

In October 2012, Attkisson began reporting on the attacks in Benghazi that resulted in the deaths of Ambassador Christopher Stevens and three other American officials. Id. ¶ 34. Attkisson's reports on the situation were generally critical of the Executive Branch and included information derived from a variety of confidential sources within the federal government or with links to intelligence agencies, including a public interview with whistleblower Colonel Andrew Wood. Id. ¶¶ 34-35.

In "mid-to-late 2011," plaintiffs "began to notice anomalies in numerous electronic devices at their home," including a laptop and desktop "turning on and off at night," the "house

[3] Attkisson alleges that the ATF "instigated an orchestrated campaign against" her initial report, although the news story about this "campaign" to which Attkisson cites just describes an internal ATF memorandum saying the ATF should look to "proactively push positive stories" to "preempt some negative reporting" or "lessen the coverage of such stories." See Compl. ¶ 16 & n.3. She also alleges that DOJ officials "persisted in their denial of the allegations" when contacted for comment, id. ¶ 17, and that her sources told her that the ATF was "actively seeking to identify government insiders who were providing information or 'leaking' to her," id. Similarly, with respect to her later reporting on Benghazi, Attkisson alleges that her confidential sources told her that "efforts were being made by the Executive Branch to clamp down on leaks and to track the leaking of information to specific reporters regarding the Benghazi affair." Id. ¶ 35. In general, Attkisson alleges that "several sources with close ties to the intelligence community approached [her] privately and informed her that the government would likely be monitoring her electronically in an effort to identify her confidential sources." Id. ¶ 38.

alarm chirping daily at different times, often indicating 'phone line trouble,'" and television interference. Id. ¶ 23. These various devices all used the Verizon FiOS line installed in the home, and Verizon was unable to cure the problems. Id. In January 2012, plaintiffs noticed problems with their Internet service; although Verizon installed a new router, the problems continued. Id. ¶ 25. In March 2012, Verizon replaced the router again and, this time, also replaced the entire FiOS service box; this too failed to resolve the issues. Id. ¶ 29. By November 2012, plaintiffs' phone line was "nearly unusable because of anomalies and interruptions," problems which also extended to Attkisson's mobile phones. Id. ¶ 40. In December 2012, Attkisson began discussing these problems with friends and contacts and decided to log the dates and times that the computers in her house turned on. Id. ¶ 41. Soon thereafter, the "computer nighttime activity stopped." Id.

Also in December 2012, plaintiffs asked a contact "with U.S. government intelligence experience" to examine their home. Id. ¶ 43. During this examination, the consultant discovered an extra fiber optics line dangling from plaintiffs' Verizon FiOS box. Id. Attkisson contacted Verizon to ask about this line. Verizon disclaimed any knowledge of the line and suggested Attkisson contact law enforcement. Id. Soon thereafter, a person called Attkisson, identified herself as a Verizon supervisor, and said she would dispatch a technician to the house. Id. The next day, which happened to be New Year's Day, a person "represented to be a Verizon technician" removed the cable. Id. ¶ 44. Attkisson asked the technician to leave the cable by the box and he did so; however, when Attkisson's husband arrived home later, the cable was missing. Id. Attkisson then "repeatedly" attempted to contact the technician to ask about the now-missing cable; he never returned her calls. Id. ¶ 45. In addition, throughout January and

February 2013, plaintiffs continued to experience phone and internet issues; although Verizon was notified about these problems, it was unable to fix them. Id. ¶ 46

These various anomalies convinced Attkisson to have an expert conduct a forensic analysis of her laptop. Id. ¶ 47. After the expert found evidence of sustained intrusions (including using "sophisticated software" whose "fingerprint indicated the software was proprietary to the federal government"), Attkisson reported this finding to CBS, which retained an expert to examine the laptop and desktop computers. Id. ¶¶ 48-49. Plaintiffs allege, based on the expert analysis, that their computers were the "targets of unauthorized surveillance efforts" beginning as early as June 2011 and that both plaintiffs' desktop and Attkisson's work laptop, as well as plaintiffs' Blackberry, were targeted, giving the intruder "complete control of the system." Id. ¶ 27. The forensic analysis also revealed that somebody "installed sophisticated surveillance spyware" on Attkisson's work laptop some time in February 2012 and "remotely 'refreshed' the ongoing surveillance" in July 2012. Id. ¶¶ 27, 32. Then, in December, the intruders "executed remote actions" to "remove evidence of the intrusion" from the various electronics. Id. ¶ 42. Finally, in March 2013, after the forensic examination, plaintiffs' desktop "began malfunctioning and, after several days of it freezing and emitting a burning odor, it shut down." Id. ¶ 50. Plaintiffs have been unable to turn the computer back on. Id.[4] Plaintiffs allege least some of these intrusions were apparently executed "via an IP address owned, controlled, and operated by the" USPS. Id. ¶ 27.

In mid-2013, Attkisson and CBS began publicly commenting on the alleged intrusions and Attkisson filed a complaint with the DOJ Inspector General. Id. ¶¶ 51, 53, 55. In response,

[4] Attkisson also alleges that a third computer, her personal MacBook Air, was "accessed remotely, controlled, and the data deleted." Compl. ¶ 57. She noticed this problem in September 2013. Id. The Complaint does not indicate that there have been any expert analyses conducted on this device.

the FBI and DOJ privately and publicly stated that they had no knowledge of any such intrusions. Id. ¶¶ 52-53. In addition, the DOJ Inspector General requested the ability to examine the affected computers. Id. ¶ 60. CBS refused to release the laptop, but Attkisson gave her desktop to the DOJ. Id. In early 2015, before Attkisson testified in front of a Senate panel, the Inspector General released a "partial report upon Congressional request" that "noted a great deal of advanced mode computer activity not attributable to" plaintiffs but concluded that there was "no evidence of intrusion" into the desktop. Id.

The Complaint alleges a variety of facts to support plaintiffs' belief that Holder, Donahoe, and unknown government employees were involved in the alleged electronic intrusions.[5] First, plaintiffs point to various policy-level initiatives taken by the DOJ in the realm of electronic surveillance. These include a DOJ and FBI public announcement in 2012 of "a new effort to vastly expand cyber related efforts to address alleged 'national security-related cyber issues'" and, around the same time, the DOJ secretly seizing "personal and phone records belonging to journalists from the Associated Press," including Attkisson. Id. ¶¶ 30, 72(C).[6] This action was reportedly criticized by a variety of news organizations but defended by Deputy Attorney General James Cole, allegedly at Holder's direction. Id. ¶¶ 72(C)-(E). The DOJ also "designated U.S. Attorneys' offices to act as 'force multipliers' in its stepped-up cyber efforts in the name of national security." Id. ¶ 31. In addition, around the same time, "internal emails from

[5] The Complaint also includes a variety of bare allegations about Holder's and Donahoe's personal involvement. See, e.g., Compl. ¶ 72(G) ("Defendant Holder, through his own conduct, likewise promulgated a policy that required or encouraged the violation of Plaintiffs' rights, and personally gave instruction to employees and agents to violate the constitution, including Plaintiffs' rights, through the use of illegal surveillance and computer intrusions."). Because the Court may not consider such conclusory allegations even at the motion to dismiss stage, see Ashcroft v. Iqbal, 556 U.S. 662, 675 (2009), they are not recounted here.

[6] The allegations in this paragraph are generally supported in the Complaint either by DOJ press releases, all of which appear to have been taken offline since the change in presidential administrations, or by emails published by Wikileaks.

a global intelligence company doing business with government agencies" were published by Wikileaks; these emails allegedly referenced White House "witch hunts of investigative journalists" who published negative stories about the White House. Id. ¶ 33 (internal quotation marks omitted). Later that year, in October and November, the DOJ provided "specialized training" for the National Security Cyber Specialists ("NSCS") network and the Computer Crime and Intellectual Property Section of the Criminal Division and Holder "hosted a national training conference" for NSCS. Id. ¶¶ 36, 39.[7] In addition, the USPS reportedly has a "working relationship with the FBI, Department of Homeland Security, and DOJ for domestic surveillance projects." Id. ¶ 63; see also id. ¶ 72(XX) (quoting a New York Times article that reported on the USPS's "mass surveillance program," which involved approving requests from a variety of agencies, including the DOJ, to "monitor the mail . . . for use in criminal and national security investigations").

With respect to Holder's personal involvement, the Complaint points to a variety of DOJ statements and interviews with Holder as a basis for claiming that Holder had some knowledge of illegal surveillance being carried out by the National Security Agency, including "overcollection" of domestic communications. Id. ¶¶ 72(M)-(O). It also cites a DOJ report that "included an admission of excessive intrusion in that it confirmed that significant revisions to

[7] The Complaint also alleges, without citation: "On November 13, 2012, the F.B.I. initiated a body of cyber security case investigations that would later relate to the illegal intrusions directed at Ms. Attkisson." Compl. ¶ 39. It is unclear to what this refers, although the Complaint later alleges (also without citation): "In June of 2013, though Plaintiffs were unaware at the time, the FBI had begun conducting inquiries of Ms. Attkisson's computer intrusions under the auspices of a national security issue, but the agency failed to contact or interview Plaintiffs. Ms. Attkisson only discovered the FBI inquiry in December, 2013, when she appealed denial of her Freedom of Information Act request to the FBI and received some documents. The F.B.I. investigation involving Ms. Attkisson's computer intrusions was circulated to the DOJ's national cyber security group and included with a set of cases opened in November, 2012, during the DOJ's expansion of its cyber team and the announcement of its intention to use 'new tools' in its arsenal." Id. ¶¶ 58-59.

Department policies were being made," id. ¶ 72(P), and a report that Holder was working on "new guidelines on dealing with news media," including "a dictate that records of a journalist w[ould] only be collected if that person is the focus of a criminal investigation and DOJ will forego the opportunity to use search warrants to obtain journalists' emails or other work product," id. ¶ 72(Z). The Complaint describes Holder as personally involved in illegal surveillance conducted on journalist James Rosen in 2010, see id. ¶¶ 72(AA)-(DD), and as "'signing-off' on search warrants as far back as 2009-2010, under the false representation that [various] media members were involved as 'possible co-conspirators' in carrying out violations of the Espionage Act," id. ¶ 72(EE).

The Complaint also alleges that Holder was personally involved in discussions that centered on Attkisson's Fast and Furious reporting, that he directed Tracy Schmaler ("Schmaler"), one of his aides, to call CBS anchor Bob Scheiffer "to get a 'handle' on [Attkisson's] reporting," and that Holder and Schmaler "began using the DOJ assets to regularly work with smear machines like Media Matters to attack reporters," including Attkisson. Id. ¶¶ 72(Q)-(T), 72(W). Schmaler is depicted as having "yelled and screamed" at Attkisson over her reporting. Id. ¶ 72(X).

With respect to defendant Donahoe, the Complaint alleges that he was ultimately responsible for the use of the USPS network and that the USPS has participated to varying degrees with the DOJ and FBI in assisting with investigations and in unconstitutionally monitoring mail as part of a mass surveillance program. Id. ¶¶ 72(OO)-(YY).

Based on this alleged misconduct, plaintiffs originally filed suit against Holder, Donahoe, and the John Doe Agents in the Superior Court of the District of Columbia, from which Holder and Donahoe removed the complaint to the United States District Court for the District of

Columbia on February 18, 2015. [Dkt. No. 1]. This original action included only the Bivens claims that are now Counts 1 and 2. In September 2015, plaintiffs filed a separate suit against the United States of America, Holder, Donahoe, and the John Doe agents, alleging the statutory and common law claims that are now Counts 3 through 8 and realleging the Bivens claims. In July 2016, the two actions were consolidated into one action, and, in March 2017, the consolidated action was transferred to this district. See Dkt. Nos. 82 & 83.

After defendants filed the present Motion to Dismiss [Dkt. No. 99] and plaintiffs filed a timely Opposition [Dkt. No. 109], the Court ordered plaintiffs to file a single consolidated complaint to clear up inconsistencies created by the previous consolidation of the two actions [Dkt. No. 114]. The revised Complaint was filed on September 15, 2017. [Dkt. No. 117]. Rather than refiling their Motion to Dismiss, defendants elected to proceed with their already-filed motion. See Dkt. No. 118.

The revised Complaint dropped the United States of America as a defendant, leaving five defendants, all of whom are sued in their individual capacities: Eric Holder, Patrick Donahoe, Unknown Named Agents of the DOJ, Unknown Named Agents of the USPS, and Unknown Named Agents of the United States. The Complaint includes eight counts, with all counts brought against all defendants. Counts 1 and 2 are brought under Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics, 403 U.S. 388 (1971), and allege violations of plaintiffs' First and Fourth Amendment rights, respectively. The remaining counts respectively allege violations of the Electronic Communications Privacy Act ("ECPA") (Count 3), violations of the Stored Communications Act ("SCA") (Count 4), violations of the Computer Fraud and Abuse Act ("CFAA") (Count 5), violations of the Foreign Intelligence Surveillance Act ("FISA") (Count 6), violations of the Virginia Computer Crimes Act ("VCCA") (Count 7), and common

law trespass to land and chattel (Count 8). Plaintiffs request compensatory, punitive, and statutory damages; an injunction; a declaration that defendants' actions were illegal; and attorney's fees and costs.

Defendants' Motion to Dismiss seeks dismissal of all eight counts with respect to Holder and Donahoe. Because their arguments vary by count, each count will be discussed in turn below.

II. DISCUSSION

A. Standard of Review

Under Rule 12(b)(1), a civil action must be dismissed whenever the court lacks subject matter jurisdiction. Although the plaintiff has the burden of establishing subject matter jurisdiction, Demetres v. East West Constr., Inc., 776 F.3d 271, 272 (4th Cir. 2015), a court should accept "as true the jurisdictionally significant facts claimed" by the plaintiff, Motley v. Va. State Bar, 403 F. Supp. 2d 468, 471 (E.D. Va. 2005). After accepting those facts as true, the court must determine "whether those facts are sufficient as a matter of law to establish subject matter jurisdiction." Id.

Under Rule 12(b)(6), a civil action must be dismissed if the complaint does not "contain sufficient facts to state a claim that is 'plausible on its face.'" E.I. du Pont de Nemours & Co. v. Kolon Indus., Inc., 637 F.3d 435, 440 (4th Cir. 2011) (quoting Bell Atl. Corp. v. Twombly, 550 U.S. 544, 570 (2007)). Although the court must assume for the purposes of deciding the motion that all "well-pleaded allegations" are true and must "view the complaint in the light most favorable to the plaintiff," Philips v. Pitt Cty. Mem'l Hosp., 572 F.3d 176, 180 (4th Cir. 2009), allegations that are merely conclusory need not be credited, see Iqbal, 556 U.S. at 678 (2009).

B. Bivens Claims (Counts 1 and 2)

Defendants' Motion to Dismiss argues that Bivens should not be extended into this new context and that even if Bivens were extended, defendants would be entitled to qualified immunity[8] because plaintiffs have failed to plausibly allege personal involvement on behalf of either Holder or Donahoe in the alleged violations of plaintiffs' rights. Def. Mem. [Dkt. No. 100] 5-14.

Before examining plaintiffs' factual allegations in more detail, the Court must first determine whether there exists a Bivens cause of action to address the type of misconduct plaintiffs allege. The analytic framework for determining the availability of a Bivens action in a given factual situation was clarified by the Supreme Court earlier this year in Ziglar v. Abbasi, 137 S. Ct. 1843 (2017). In Abbasi, aliens who had been detained in harsh conditions for months after the September 11th attacks brought Bivens claims against former Attorney General John Ashcroft, former FBI Director Robert Mueller, former Immigration and Naturalization Service Commissioner James Ziglar, and the warden and associate warden of the facility in which they were detained. See id. at 1853-54. The detainees argued that the officials had detained them in harsh conditions for a punitive purpose, in violation of their substantive due process rights; had done so because of their race, religion, or national origin, in violation of their equal protection rights; and that the warden and associate warden had subjected them to punitive strip searches, in violation of the Fourth and Fifth Amendments. See id.[9] After the Second Circuit allowed the

[8] The qualified immunity defense applies to both the Bivens claims and also to the various statutory claims. Def. Mem. 17 (citing Behrens v. Pelletier, 516 U.S. 299, 305 (1996)).

[9] The detainees brought additional claims against the warden and associate warden, arguing that those officials allowed guards to abuse them, in violation of their Fifth Amendment rights. See Abbasi, 137 S. Ct. at 1853-54. The Supreme Court's treatment of these claims, which were analyzed separately from the claims brought against the higher-level defendants, is not relevant to the present case.

detainees' claims to proceed under Bivens, the Supreme Court reversed in a 4-2 decision,[10] holding that a Bivens remedy was not available to the detainees. See id. at 1863. In declining to extend Bivens, the Supreme Court clarified that the first step in this analysis is to determine whether the plaintiff seeks to extend Bivens to a "new" or "novel" context. If so, the court must perform a "special factors analysis" to determine whether a Bivens action should be available in that new context. See id. at 1854-63.

Under this direction, the Court must first determine whether plaintiffs' allegations would extend Bivens to a new context. As the Supreme Court has explained, when determining whether a context is new, a court must examine whether the "case is different in a meaningful way from previous Bivens cases decided by [the Supreme] Court." Id. at 1859. Although not an exhaustive list, the Abbasi decision cites as examples of meaningful differences "the rank of the officers involved; the constitutional right at issue; the generality or specificity of the official action; the extent of judicial guidance as to how an officer should respond to the problem or emergency to be confronted; the statutory or other legal mandate under which the officer was operating; the risk of disruptive intrusion by the Judiciary into the functioning of other branches; or the presence of potential special factors that previous Bivens cases did not consider." Id. at 1860.

To date, the Supreme Court has recognized the availability of Bivens actions in only three discrete factual scenarios. First, in Bivens itself, the Court found an implied cause of action to enforce Fourth Amendment search and seizure rights against line-level FBI officers who searched plaintiff's home and arrested him without a warrant. Bivens, 403 U.S. at 389-90. Second, in Davis v. Passman, the Court found an implied cause of action under the Fifth Amendment's Due Process Clause that allowed an administrative assistant to sue a Congressman

[10] Justices Sotomayor, Kagan, and Gorsuch took no part in considering or deciding the case. See Abbasi, 137 S. Ct. at 1851.

for firing her because of her gender. 442 U.S. 228, 248-49 (1979). Finally, in Carlson v. Green, the Court found an implied cause of action under the Eighth Amendment that allowed a federal prisoner's estate to sue prison guards for failing to treat the decedent's asthma. 446 U.S. 14, 19 (1980).[11]

The claims in plaintiffs' Complaint differ meaningfully from the claims in each of these other cases. As an initial matter, only Bivens itself allowed a claim to proceed under the Fourth Amendment, which makes both Carlson and Davis meaningfully different from either of plaintiffs' constitutional claims and all three cases meaningfully different from plaintiffs' First Amendment claim. Beyond that, Bivens only allowed the plaintiff to sue line-level FBI agents, whereas plaintiffs wish to sue a former Attorney General and Postmaster General. Therefore, the ranks of the officials are a meaningful difference between the two contexts. In addition, plaintiffs' claims involve a significantly different factual setting (electronic surveillance), a different level of generality (broad policy decisions rather than individual unconstitutional actions), and a connection to national security that was not present in any of the previous three

[11] Plaintiffs contend that the Supreme Court has also "impliedly confirmed that individuals could seek damages against government officials who retaliated against them for exercising their constitutional right to freedom of speech." Pl. Opp. [Dkt. No. 109] 16 (citing Hartman v. Moore, 547 U.S. 250, 256 (2006)). They are incorrect. In Hartman, the plaintiff attempted to bring a Bivens claim under the First Amendment, claiming that the government had initiated a prosecution against him in retaliation for protected speech. See Hartman, 547 U.S. at 254-55. The Court held only that the absence of probable cause to support the underlying criminal charge is an element of such a retaliation claim. Id. at 265-66. Although it implicitly assumed for the purposes of argument that a First Amendment Bivens claim would be cognizable, it did not hold (or "impliedly confirm[]") that such a claim is available. Cf. Abbasi, 137 S. Ct. at 1855 ("These three cases—Bivens, Davis, and Carlson—represent the only instances in which the Court has approved of an implied damages remedy under the Constitution itself."); Reichle v. Howards, 132 S. Ct. 2088, 2093 n.4 (2012) ("We have never held that Bivens extends to First Amendment claims.").

cases.[12] As such, it is clear that plaintiffs' claims are meaningfully different from any previously recognized Bivens claim.[13]

Once a court has recognized that an action presents a new context, it must then determine whether Bivens should be extended into that context. As the Supreme Court has made clear, courts should exercise "caution" before such an extension and, in particular, should not recognize a Bivens remedy if there are "special factors counselling hesitation in the absence of affirmative action by Congress." Abbasi, 137 S. Ct. at 1857 (internal quotation marks omitted). Although the Supreme Court has not provided an exhaustive list of such "special factors," it has identified a few common factors that should make courts hesitate, including if a context involves "a host of considerations that must be weighed and appraised," id. (internal quotation marks omitted), if Congress has "designed its regulatory authority in a guarded way" (e.g., in cases involving the military or federal land), id. at 1858, or if there "is an alternative remedial structure present in a certain case," id.

---

[12] Indeed, in many ways, this case is to Bivens what Abbasi was to Carlson. Even though the Abbasi plaintiffs, like the Carlson plaintiff, were alleging unconstitutional actions related to confinement (although, as preconviction detainees, the Abbasi plaintiffs were proceeding under the Fifth rather than the Eighth Amendment), their claims challenging conditions imposed "pursuant to a high-level executive policy created in the wake of a major terrorist attack on American soil" were against high-ranking officials, Abbasi, 137 S. Ct. at 1860. As such, the Abbasi majority had little trouble holding that the plaintiffs' claims presented a new context, to which Bivens would not be extended.

[13] In addition to the Supreme Court cases, plaintiffs cite two Fourth Circuit cases that have also recognized a Bivens claim: Tobey v. Jones, 706 F.3d 379 (4th Cir. 2013), where plaintiffs argue that the court found a First Amendment claim for retaliatory arrest cognizable under Bivens, and Covey v. Assessor of Ohio County, 777 F.3d 186 (4th Cir. 2015), where the court allowed for a Bivens suit in a case where the officers improperly entered the plaintiffs' curtilage without a warrant. But in both cases, the Fourth Circuit did not explicitly address whether the particular Bivens claim was cognizable; instead, it was assumed that Bivens applied. Even assuming plaintiffs correctly characterized these holdings and these decisions survive after the Abbasi decision, this action still presents a new context for all of the reasons described above.

In Abbasi, the Supreme Court appeared to identify four additional "special factors necessarily implicated" by the claims. Id. at 1860-63. First, the Court observed that the plaintiffs' claims were brought against high-level officials to challenge the "formulation and implementation of a general policy." Id. at 1860. As such, resolving the claims would require discovery "into the whole course of the discussions and deliberations that led to the policies" being challenged, would "require courts to interfere in an intrusive way with sensitive functions of the Executive Branch," and would not serve a particularly acute deterrence function. Id. at 1860-61. The Court also found that the plaintiffs' claims implicated "sensitive issues of national security," an area in which the Congress and the President deserve deference from the courts. Id. at 1861. In addition, the Court found that although Congress's interest in the federal government's response to the September 11th attacks was "frequent and intense," including with respect to the conditions of confinement over which plaintiffs were suing, it had not chosen to extend a federal remedy to the plaintiffs, indicating that it did not intend for there to be such a remedy. Id. at 1862 (internal quotation marks omitted). Finally, the Court pointed to alternative avenues available to the plaintiffs to challenge the conditions of confinement, including a suit for injunctive relief and possibly a habeas action. Id. at 1862-63.

The present action involves many of the same factors identified by the Supreme Court in Abbasi as a basis for declining to extend Bivens. Plaintiffs are attempting to sue high-level officials, including one of the same high-level officials sued in Abbasi, the Attorney General, for what were essentially policy-level decisions. As such, resolving the allegations in the Complaint would require inquiry into sensitive Executive Branch discussions and decisions, overstepping the judiciary's bounds. In addition, the policies in question here implicate potential national security concerns, as plaintiffs' allegations appear to be directed primarily toward policies

designed by the federal government to identify employees who were leaking sensitive information. Finally, as plaintiffs' reliance on several statutes in Counts 3 through 6 of their Complaint demonstrates, Congress has already legislated extensively in the areas of electronic surveillance and unauthorized intrusions into electronic communications, as plaintiffs identify no fewer than four federal statutory claims in addition to their constitutional claims. In fact, many of plaintiffs' allegations recognize that Congress was particularly concerned with the federal government's domestic surveillance activities, including those tactics employed by the FBI and DOJ, which were overseen by Holder. See, e.g., Compl. ¶¶ 14 n.2, 24, 60, 72(HH) & n.8, 72(JJ). Given Congress's attention to this area, either Congress has provided plaintiffs a federal statutory remedy and it is unnecessary to find an implied Bivens cause of action, or Congress has not provided plaintiffs a federal statutory remedy and this considered inaction weighs against the Court finding an implied Bivens cause of action in this context.

As explained above, plaintiffs' Bivens claims would require extending the implied right of action described in Bivens into a new context and a large number of special factors counsel hesitation in this area. For these reasons, the Court declines to extend Bivens to the allegations in this litigation and will grant defendants' Motion to Dismiss as to Counts 1 and 2.

C. Electronic Communications Privacy Act Claim (Count 3)

In Count 3, plaintiffs contend that defendants violated the ECPA, 18 U.S.C. §§ 2511, 2520. Section 2511 provides in pertinent part that

> any person who—(a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication; (b) intentionally uses, endeavors to use, or procures any other person to use or endeavor to use any electronic, mechanical, or other device to intercept any oral communication when [a jurisdictional element that is not in dispute here is met]; [or] (c) intentionally discloses, or endeavors to disclose, to any other person the contents of any wire, oral, or electronic communication, knowing or having reason to know that the information was obtained through the interception of

> a wire, oral, or electronic communication in violation of this subsection [has violated the statute].

18 U.S.C. § 2511. Section 2520 creates the private right of action under which plaintiffs are suing by providing that "any person whose wire, oral, or electronic communication is intercepted, disclosed, or intentionally used in violation of this chapter may in a civil action recover from the person or entity, other than the United States,[14] which engaged in that violation such relief as may be appropriate."

According to defendants, § 2520 bars plaintiffs' claims against Holder and Donahoe because the language of the provision only reaches the person or entity that intercepts, discloses, or intentionally uses communications—and not a person or entity that procures others to intercept, disclose, or use communications. Def. Mem. 18. Before a congressional amendment in 1986, § 2520 parroted § 2511 (and included the "procuring" language).[15] As such, under the canon of statutory construction that amendments should be given meaning, the removal of "procuring" should be given significance and the court should not allow an action to proceed under § 2520 on the basis of "procuring" liability. Def. Mem. 18-19.

Plaintiffs respond that although the 1986 amendment of § 2520 removed the procuring language, it replaced this language with a reference to § 2511, and that the incorporation of § 2511 into § 2520 necessarily includes all means of violating § 2511—including "procuring" a

---

[14] Defendants also argue (and plaintiffs agree) that this carve-out exempts the United States from liability under this section. Def. Mem. 18; Pl. Opp. 22. This concession appears irrelevant, as plaintiffs have only sued defendants in their individual capacities, but to the extent plaintiffs attempt to assert any claims against the United States or against agencies or officers in their official capacities, those claims would indeed be barred.

[15] Originally, § 2520 provided in pertinent part: "Any person whose wire or oral communication is intercepted, disclosed, or used in violation of this chapter shall (1) have a civil cause of action against any person who intercepts, discloses, or uses, or procures any other person to intercept, disclose, or use such communications . . . ." Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 223.

violation. Pl. Opp. 23. Plaintiffs argue that this is the more natural reading of the text, as the provision allows recovery against the person who "engaged in" the "violation of this chapter," and somebody who procures an interception has "engaged in" a "violation of" § 2511. Id. In addition, they argue that the legislative history does not suggest that Congress intended to eliminate procurer liability. Id.

Courts have split on whether a plaintiff may bring suit under § 2520 against a "procurer," and the Fourth Circuit has not yet ruled on the issue.[16] See, e.g., Buckingham v. Gailor, No. 00-cv-1568, 2001 WL 34036325, at *6 (D. Md. Mar. 27, 2001) (finding that the 1986 amendments eliminated the availability of a civil action against a procurer), aff'd, 20 F. App'x 243 (4th Cir. 2001) (per curiam);[17] Lonegan v. Hasty, 436 F. Supp. 2d 419, 427-28 (E.D.N.Y. 2006) (determining that a civil action based on procurement is still viable).

Based on the plain language of the statute, defendants have the better of the argument. The use of the phrase "that violation" (plaintiffs may recover from the person who "engaged in that violation") most naturally refers to the violation denoted earlier in the sentence: the interception, disclosure, or use of a communication. Moreover, the statute provides that a plaintiff may recover from "the person" who engaged in the violation—not from a person or

[16] Plaintiffs remark that "the Fourth Circuit has never explicitly overruled its holding in Flowers v. Tandy Corp., 773 F.2d 585 (4th Cir. 1985)." Pl. Opp. 24. To the extent that plaintiffs intend this to be an argument that this Court is bound on the procurement question by Flowers, they are wrong because Flowers was decided before the 1986 amendments, when § 2520 clearly provided for procurer liability. As such, it has nothing to say about whether the amended version of the section supports procurer liability. Moreover, neither party in Flowers argued that procurer liability was improper under § 2520; instead, they argued about what "procures" should mean in the context of the section. See Flowers, 773 F.2d at 590.

[17] On appeal, the plaintiffs in Buckingham raised three issues, none of which implicated the procurement question. See 20 F. App'x at 244. As such, the Fourth Circuit affirmed the district court's grant of summary judgment to the defendants without discussing the availability of a civil action for procurement, see id., and defendants here do not argue that this affirmance binds this Court on the question of procurer liability.

from any person—and the use of the word "the" contemplates only a single person or entity engaged in a given violation. If so, then the violator being referred to must be the person who engaged in the actual interception, disclosure, or use of a communication. Given this plain reading, defendants' argument is correct: the 1986 amendments restricted liability in a private action only to those who personally intercept, disclose, or use communications in violation of the ECPA.[18] As such, defendants' Motion to Dismiss Count 3 will be granted.

D. Stored Communications Act Claim (Count 4)

In Count 4, plaintiffs allege that all defendants violated the SCA, 18 U.S.C. §§ 2701, 2707. The SCA provides in relevant part that whoever "intentionally accesses without authorization a facility through which an electronic communication service is provided . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage" has violated the statute. 18 U.S.C. § 2701(a). Section 2707 provides a private right of action against "the person or entity, other than the United States,[19] which engaged in" a violation of § 2701(a). Id. § 2707(a).

Preliminarily, defendants claim that the Complaint does not allege that any defendant accessed a "facility through which an electronic communication service is provided." Def. Mem. 21. As the relevant case law explains, the most natural reading of this provision is that it applies to third parties attempting to access "network services providers' own facilities," not "an

[18] Plaintiffs' only other argument on this point—that the legislative history is silent on whether Congress intended to eliminate procurer liability—does not overcome the plain text of the statute.

[19] Again, defendants argue that this carve-out exempts the United States from liability under the SCA. Def. Mem. 20. Plaintiffs argue that a different section, 18 U.S.C. § 2712, provides a cause of action against the United States for violations of the SCA, a point that defendants concede in their reply brief (and a point that was in fact suggested by defendants in their opening brief under their obligation of candor). Def. Reply 16. In any event, this discussion is irrelevant because plaintiffs are only suing defendants in their individual capacities.

individual's personal computing device." In re Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 145-46 (3d Cir. 2015) (internal quotation marks omitted); see also United States v. Steiger, 318 F.3d 1039, 1049 (11th Cir. 2003); In re iPhone Application Litig., 844 F. Supp. 2d 1040, 1057-58 (N.D. Cal. 2012). As such, defendants argue that plaintiffs' allegations that defendants intruded on various personal electronic devices, including a laptop, desktop, phone line, television, and house alarm, do not state a claim under the SCA. Def. Mem. 21.

Plaintiffs respond that the breadth of the provision "is the subject of some debate," Pl. Opp. 25, but do not attempt to defend a broad reading of the SCA. Instead, they argue that "[i]n order to access [p]laintiffs' computers and other devices, [d]efendants necessarily went through [p]laintiffs' service provider—Verizon—to access the [p]laintiffs' electronic devices," including making "physical alterations to the Verizon hardware located on [p]laintiffs' property." Id.; see also Compl. ¶¶ 43-44.

These arguments are weak. In all of the cases defendants cite for the proposition that end-user devices are not "facilities" under the SCA, the alleged intrusion would have gone through the service provider and there is no suggestion in this case that the intrusion accessed Verizon's facilities in some special manner.[20] As such, what those cases necessarily hold is that using a service provider's network to access an end-user's device is not a violation of the SCA; instead, the intrusion must be to a facility that the service provider itself uses to store data. In addition,

[20] Plaintiffs do allege, as discussed above, that one or more of the John Doe defendants physically accessed their Verizon box by inserting an unauthorized fiber-optic cable. Neither party discusses or cites to case law discussing how such a physical intrusion might be treated under the SCA. But as explained in this section, the SCA is concerned with unauthorized access of data stored by service providers, whereas plaintiffs' allegations about the Verizon box appear to be that there was some physical contact with the box to facilitate the electronic intrusion into plaintiffs' end-user devices, not that defendants somehow accessed data that Verizon had stored in the box. Therefore, the allegations of physical contact with the Verizon box are not sufficient to state a claim under the SCA.

this understanding aligns with the language of the statute, which focuses on facilities used by electronic communication providers to store electronic data—not on the portions of a service provider's network that merely connect the end user to the service provider.[21] Therefore, because plaintiffs do not appropriately allege that defendants accessed a "facility through which an electronic communication service is provided," defendants' Motion to Dismiss will be granted as to Count 4.[22]

E. Computer Fraud and Abuse Act Claim (Count 5)

In Count 5, plaintiffs allege that defendants violated the CFAA, 18 U.S.C. § 1030, which provides in relevant part[23]:

> Whoever . . . (4) knowingly and with intent to defraud, accesses a protected computer[24] without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value . . . ; [or] (5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer; (B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or (C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss [violates this provision].

---

[21] Though not discussed in more depth by either party beyond defendants' citation to the case generally, In re Google Cookie Placement includes a persuasive analysis of the legislative history and enactment context and concludes that the intent of the SCA was to reach individuals who intrude on information stored by third-party service providers, not to reach individuals who intrude on information stored on users' personal devices.

[22] Because the determination that plaintiffs' end-user devices are not "facilities" within the meaning of the SCA applies equally to the SCA claims against the John Doe agents, Count 4 will be dismissed as to all defendants.

[23] Defendants claim that plaintiffs do not specify which subsection(s) of § 1030 apply to their claim and that this "failure alone warrants dismissal." Def. Mem. 22. As plaintiffs correctly argue, their allegations make it clear that only §§ 1030(a)(4) and 1030(a)(5) are potentially applicable. For example, § 1030(a)(3) only encompasses intrusions into computers owned or used by the federal government. As such, defendants had appropriate notice of the nature of the claim in Count 5.

[24] A "protected computer" includes, among other devices, any computer "which is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B). Although not specifically pled, it is a plausible inference that plaintiffs' computers are used in interstate communication and defendants do not argue otherwise.

18 U.S.C. § 1030(a). Section 1030(g) provides a private right of action for "[a]ny person who suffers damage or loss by reason of a violation of this section," but limits the private right to situations where "the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i)" and limits "[d]amages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I)" to economic damages.[25] Id. § 1030(g).

Here, defendants' primary argument[26] is that "there are simply no non-conclusory allegations within the four corners of plaintiffs' complaint that would render plausible the conclusion that either" Holder or Donahoe "had any involvement in actually accessing plaintiffs' personal computing devices." Def. Mem. 23. In response, plaintiffs do not argue that § 1030(a)(5)(A), which reaches any person who "causes" the transmission of programs or code that harms a protected device, should be interpreted to reach individuals who allow or direct subordinates to engage in electronic intrusions without themselves personally accessing the protected device. Instead, plaintiffs' response[27] is, in its entirety, that "the substantive factual

---

[25] Subsection (c)(4)(A)(i) lists five factors, capturing offenses that caused: "(I) loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value; (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; [or] (V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security . . . ." Of these five factors, only (I) seems potentially applicable, and it is not at all clear that plaintiffs have pled sufficient facts to make out a large enough monetary loss to meet that factor (and, if they had, they would still be limited to economic damages under this Count); however, defendants do not make any argument that plaintiffs' claim is limited by this subsection.

[26] Defendants also argue, and plaintiffs contest, that this section does not waive sovereign immunity. Def. Mem. 22-23; Pl. Opp. 25-26. Again, in the revised Complaint, plaintiffs only sue defendants in their individual capacities, making the sovereign immunity defense irrelevant.

[27] This actually appears to be a response to defendants' argument that plaintiffs did not specifically identify which subsection of the statute they were bringing the claim under, but, generously construed, it is also the only statement that could possibly bear on defendants' "plausible claim" argument.

allegations clearly support violations of § 1030(a)(4) and (5)." Pl. Opp. 26. Although both parties' arguments are conclusory, defendants are correct: there is no plausible allegation that either Donahoe or Holder personally "accessed" plaintiffs' computers. Therefore, defendants' Motion to Dismiss will be granted as to Count 5.

F. Foreign Intelligence Surveillance Act Claim (Count 6)

An individual violates FISA when he (1) "engages in [unauthorized] electronic surveillance under color of law"; and (2) "discloses or uses information" obtained through that surveillance. 50 U.S.C. § 1809(a). Any "aggrieved person" has a "cause of action against any person who committed" a "violation" of § 1809. Id. § 1810.

Here, again, defendants' primary[28] argument is that the Complaint does not plausibly allege that either Holder or Donahoe actually engaged in the alleged unauthorized surveillance. Def. Mem. 25. Plaintiffs' brief is silent on this point. See Pl. Opp. 26-27 (discussing only sovereign immunity). As discussed above, defendants correctly argue that the Complaint fails to allege sufficient facts to make a plausible claim that either defendant personally engaged in the alleged surveillance and, in the absence of an argument from plaintiffs that "engages in" should be read more broadly, defendants' Motion to Dismiss will be granted as to Count 6.[29]

G. Virginia Computer Crimes Act Claim and Common Law Trespass Claim (Counts 7 and 8)

In Counts 7 and 8, both brought pursuant to the Federal Tort Claims Act, plaintiffs seek damages for violations of the Virginia Computer Crimes Act and for trespass to land and chattel

---

[28] As with the previous claims, the parties engage in some skirmishing over whether the United States has waived its sovereign immunity with respect to FISA. As defendants concede in their reply brief after initially suggesting the point in their opening brief, the United States has waived its sovereign immunity against FISA claims. Def. Reply. 18. This is again irrelevant.

[29] Defendants also correctly point out that the Complaint does not allege that either Holder or Donahoe disclosed or used the information allegedly obtained as a result of the surveillance.

under Virginia common law. Defendants argue that the "exclusive" remedy for damages "arising or resulting from the negligent or wrongful act or omission of any employee of the Government while acting with the scope of his office or employment" is a civil action against the United States of America (except for constitutional and federal statutory claims). 28 U.S.C. § 2679; see also Def. Mem. 25-28. As such, plaintiffs must sue the United States of America, not Holder and Donahoe in their individual capacities. Plaintiffs have not named the United States of America as a defendant and have not responded to this argument. See Pl. Opp. 27-30. Therefore, Counts 7 and 8 were dismissed during oral argument.

H. Defendants' Motion for Reconsideration or, in the Alternative, for a Protective Order

On October 27, 2017, defendants filed a motion in which they asked the Court to "reconsider its September 22, 2017 order . . . to the extent that it held [defendants'] motion to dismiss—on qualified immunity grounds—'in abeyance'" or, alternatively, to enter a "protective order staying discovery pending the resolution of their motion to dismiss." Dkt. Nos. 128 & 129. Because the Order to be issued with this Memorandum Opinion will fully resolve defendants' Motion to Dismiss, it will also moot defendants' new motion. Accordingly, defendants' Motion for Reconsideration or, in the Alternative, for a Protective Order will be denied as moot.

III. CONCLUSION

For the reasons stated in this Memorandum Opinion, defendants' Motion to Dismiss will be granted, defendants Donahoe and Holder will be dismissed from this civil action, Count 4 will also be dismissed as to all John Doe defendants, and defendants' Motion for Reconsideration will be denied as moot by an appropriate Order to be issued with this Memorandum Opinion.

Entered this 1st day of November, 2017.

Alexandria, Virginia

/s/
Leonie M. Brinkema
United States District Judge