UNITED STATES DISTRICT COURT
DISTRICT OF COLUMBIA

SHARYL THOMPSON ATTKISSON, et al., Plaintiffs, vs. ERIC HOLDER, et al., Defendants.	)	Civil Action No. 1:15-cv-238(EGS)
SHARYL THOMPSON ATTKISSON, et al., Plaintiffs, vs. UNITED STATES OF AMERICA, et al., Defendants.	)	Civil Action No. 1:15-cv-1437(EGS)

PLAINTIFFS' MEMORANDUM IN OPPOSITION TO DEFENDANTS' AMENDED MOTION TO DISMISS

COME NOW the Plaintiffs, by counsel, and hereby submit their memorandum in opposition to Defendants' Amended Motion to Dismiss (Dkt. No. 74).

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Rules

Treatises

PRELIMINARY STATEMENT

Defendants' motion to dismiss is a true "kitchen sink" approach, and includes a hodge-podge of arguments that mix attacks on subject matter jurisdiction with challenges to venue, sovereign immunity, pleading standards, and an attempt to claim qualified immunity if all else fails. The one common thread that weaves its way throughout the motion is the extremes to which Defendants go to avoid discussing, or even acknowledging, the plethora of evidence outlined in the Complaint showing that illegal surveillance was used to conduct a cyber-attack on a high-profile member of the media from a government-owned and operated IP address during the very time period that Defendant Holder, the FBI, the DOJ, the Administration, and other agencies of the government were publicly admitting that such tactics were in fact being used to chill reporting on controversial topics that were critical to the reputational and political interests of the Obama Administration, the Defendants, and the very agencies that are now at the heart of this suit.

While ignoring the details and depth of the Complaint, Defendants take aim at the pleading using language like "167 paragraphs, but short on substance and legally infirm"; "rather verbose"; "fantasy"; and other pejorative descriptors all designed to try and deflect attention from the forensic evidence, public admissions, internal communications admitting motive, and the overwhelming temporal facts that go well beyond simple "plausibility" and establish a convincing and very worrisome pattern, practice, and policy of these government officials and agencies to violate clearly defined constitutional rights that have existed for decades.

As will be demonstrated in the following pages, the Court has subject matter jurisdiction over Counts 1-6; venue is appropriate in the District of Columbia; sovereign immunity is not an issue; qualified immunity does not apply to these officials given the facts; and finally the factual pleadings include explicit factual allegations that are convincing rather than simply "plausible.".

STANDARD OF REVIEW

Fed. R. Civ. P. 8(a) does not "require heightened fact pleading of specifics." *Bell Atl. Corp v. Twombly*, 550 U.S. 544, 570 (2007). The Complaint's sufficiency is still construed "in the light most favorable to the [P]laintiff[s], accepting as true all well-pleaded facts alleged, and drawing all possible inferences in [their] favor." *Tamayo v. Blagojevich* 526 F.3d 1074, 1081 (7th Cir. 2008).

Rule 12(b)(1) allows a party to move to dismiss "for lack of subject-matter jurisdiction." Fed. R. Civ. P. 12(b)(1). When a defendant moves to dismiss under Rule 12(b)(1), the plaintiff bears the burden of proving by a preponderance of the evidence that the Court has subject matter jurisdiction. *See Biton v. Palestinian Interim Self-Gov't Auth.*, 310 F. Supp. 2d 172, 176 (D.D.C. 2004); *see also Lujan v. Defenders of Wildlife*, 504 U.S. 555, 561 (1992). A court considering a Rule 12(b)(1) motion must assume the truth of all material factual allegations in the complaint and construe the complaint liberally, granting a plaintiff the benefit of all inferences that can be derived from the facts alleged.' *Am. Nat'l Ins. Co. v. FDIC*, 642 F.3d 1137, 1139 (D.C. Cir. 2011) (quoting *Thomas v. Principi*, 394 F.3d 970, 972 (D.C. Cir. 2005)).

FACTUAL ALLEGATIONS

A. THE ILLEGAL SURVEILLANCE

The Complaint alleges that Defendants, agents of the United States government acting under color of law, illegally installed sophisticated spyware on various electronic devices belonging to Plaintiffs between 2011 and 2014 in direct violation of their Constitutional rights. As alleged in the Complaint, the illegal surveillance occurred during the same period that Ms. Attkisson was extensively reporting on a number of critical domestic news stories, including *Fast and Furious* and *Benghazi*. Ms. Attkisson's reporting revealed information – much of which came

from confidential sources – that certain parties within the federal government clearly found embarrassing, and which suggested that Ms. Attkisson was communicating with well-placed sources/whistleblowers providing information that the federal government preferred not be revealed.[1] As a result, the individual defendants authorized or permitted certain persons connected to their respective agencies to conduct illegal surveillance on Plaintiffs, including electronic intrusion into personal and business computers and other electronic devices, in direct violation of Plaintiffs' constitutional, statutory, and common law rights.

The names of the individuals involved on the ground have not yet been identified because the attack was concealed and covert, and names of participants are in the exclusive control of Defendants. Forensic analysis identified unauthorized communications channels on Plaintiff's laptop directly connected to an Internet Provider (IP) address owned and operated by the United

[1] Ms. Attkisson's first "Fast and Furious" reporting was on or about February 22, 2011. http://www.cbsnews.com/stories/2011/02/23/eveningnews/main20035609.shtml. Shortly thereafter, representatives within the ATF authored an internal email that stated: "*Given the negative coverage by CBS Evening News last week and upcoming events this week, the bureau should look for every opportunity to push coverage of good stories. Fortunately, the CBS story has not sparked any follow up coverage by mainstream media and seems to have fizzled….It was shoddy reporting…ATF needs to proactively push positive stories this week, in an effort to preempt some negative reporting, or at minimum, lessen the coverage of such stories in the news cycle by replacing them with good stories about ATF*." http://www.cbsnews.com/8301-31727_162-20039251-10391695.html\. On March 3, 2011, Ms. Attkisson (and CBS) aired the landmark "Fast and Furious" story with whistleblower ATF Agent John Dodson. http://www.cbsnews.com/video/watch/?id=7358401n&tag=mncol;1st;5. That same month, March, 2011, Defendant Holder's office was communicating with CBS News about Ms. Attkisson's reporting. By May, 2011, the White House recruited Eric Schultz to publicly address investigations into the "Fast and Furious" scandal, including Congress' efforts to investigate. http://www.conservativecommune.com/wp-content/uploads/2011/10/Converted_file_8fc47fc1.jpg

States Postal Service, which is known to partner and coordinate with the FBI and DOJ in related matters.[2]

B. THE CONSTITUTIONAL VIOLATION CLAIMS

Plaintiffs' brought suit under the Federal Tort Claims Act ("FTCA"), 28 U.S.C. § 2671, the United States Constitution, and certain laws of the Commonwealth of Virginia. *See* Complaint, Dkt. No. 1 at p. 2. Defendants include former Attorney General Eric Holder, former Postmaster General and head of the United States Postal Service, Patrick R. Donahoe, and unknown named agents of the Department of Justice, United States Postal Service, and the United States. The Complaint alleges misconduct in exceeding restraints on the exercise of governmental power imposed by our country's Constitution, laws, and traditions, including illegal surveillance and cyber-attacks of personal computers and phone systems through the remote installation of sophisticated spyware and the use of an IP address owned, controlled and operated by the federal government, which is in direct violation of the First Amendment, Fourth Amendment, and a collection of statutes ranging from federal to the Commonwealth of Virginia[3]. *Id*. at p. 8, ¶27.

---

[2] In passing, Defendants faintly attempt to question the forensic evidence by noting that the government-owned and operated IP address was "not associated with any web server or website used by the USPS", as if that is favorable to Defendants. (Doc. 72-1, page 16). To the contrary, the fact that the USPS IP address linked to the illegal invasion was not being used on an active web server or website is proof positive that the IP address was not susceptible to being hacked, and that the perpetrator came from inside the USPS. An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves as (a) a host or network interface identification and (b) a location addressing mechanism. The Internet Assigned Numbers Authority (IANA) manages the IP address space allocations globally and delegates five regional internet registries to allocate IP address blocks to local registries and other entities. IP addresses (at least static addresses) are manually assigned to a computer by an Administrator.

[3] Defendants make a "tongue-in-cheek" criticism of the Complaint for failing to identify the Agencies or people actually involved in the intrusion (Dkt. 72-1, pg. 16), and for "curiously" failing to even consider that other agencies might have actually been engage in the illegal surveillance (Dkt. 72-1, pg. 17, fn 5). The criticism is ironic given that the government uniquely possesses the missing information, has repeatedly fought limited discovery to identify this very

Plaintiffs include Sharyl Attkisson, an investigative reporter for CBS News, and her family residing in Virginia. Ms. Attkisson served CBS for twenty (20) years, the majority of which was devoted to investigating and reporting on national news stories from Washington, D.C. *Id*. at p. 6, ¶14. During the 2011-2013 timeframe, Ms. Attkisson was tasked to investigate high profile investigations of government misconduct, including Fast and Furious and the Benghazi tragedy. *Id*. at p. 6, ¶14. Each of the stories included the use of informants, confidential government sources, whistleblowers, and officials of the government who were upset with the manner in which the government and Administration had carried out their responsibilities under the law. *Id*. at p. 8, ¶20; p. 10, ¶35. The reporting was likewise critical of the Attorney General, the Administration, and specifically reported on documented misrepresentations made by Mr. Holder to Congress about the FBI's knowledge of certain events, some of which resulted in public retractions and corrections as well as illegal surveillance targeting of the press in an effort to silence whistleblowers who were sharing information with Plaintiff Attkisson and other members of the media about the misconduct. Id. at p. 7, ¶21; p. 7, ¶22; p. 10, ¶ 35; and p. 18, ¶72.

Contrary to Defendants' criticism that the Complaint is full of "bare bones" and "conclusory allegations", the Complaint combines forensic evidence from multiple independent sources with public admissions of Defendant Holder, internal email correspondence released into the public domain, and whistleblower facts all of which not only make Plaintiffs' Complaint "plausible", but sets forth a compelling factual setting demonstrating intentional and reckless behavior by agents at high levels of the federal government. For instance, the Complaint sets forth concrete facts showing sophisticated illegal intrusion using cyber-attack software that is not

---

point, and that illegal surveillance by nature is covert, secret, and done to conceal what is being done.

commercially available and all of which was remotely installed from an IP address owned, controlled, operated, and closely monitored by the USPS.

For instance, the forensic evidence demonstrating government intrusion from an IP address owned, controlled and operated by the USPS is clear, factual, and documented from the computers by multiple sources. *Id*. at p. 13, ¶47; p. 14, ¶48-49, 55; p.; p. 15, ¶56. Even CBS in Washington, D.C., Ms. Attkisson's employer, confirmed that forensics evidenced the referenced attack. *Id*. at p. 14, ¶55. Factual evidence from the mouth of Attorney General Holder and his top staff likewise conceded the existence of this unprecedented surveillance program targeted at the media in an effort to silence whistleblowers and thus sensor Ms. Attkisson's First Amendment rights, including Deputy Attorney General Cole's public admission that Attorney General Holder created a policy of targeting members of the press with illegal surveillance when responding to very public objections submitted by the *Associated Press* in response to having been targeted by the Attorney General. *Id*. at p. 19, ¶72, as well as an admission in a November 11, 2013 interview wherein Attorney General Holder admitted knowledge of improper surveillance techniques combined with a promise to reexamine his own policies. *Id*. at p. 20, ¶72. Other publicly available evidence further supporting the existence of a policy and practice of illegal surveillance consistent with that described by forensic evidence by Defendants included the concession that the USPS publicly admitted a "working relationship" with the FBI and DOJ on electronic surveillance (*Id*. at p. 16-17, ¶63); Inspector General reporting of DOJ and the NSA recommending changes in the surveillance programs (*Id*. at p. 19, ¶72); the public release by Mr. Snowden of internal records showing that the very same agencies involved in the illegal surveillance here were similarly involved in illegal surveillance of news media member *Al Jazeera* (*Id*. at p. 24, ¶72), and, most critically, internal communications from the Administration itself published in unrelated litigation

specifically referring to the need to "muzzle" Ms. Attkisson's reporting. *Id*. at p. 20, ¶72. The foregoing mountain of facts established from forensic evidence, admissions, public reports, and internal communications was further compounded when Judge Napolitano judicially described Attorney General Holder's conduct as intrusive and designed to silence the government's critics, including a comparison of the conduct to former President Richard M. Nixon. *Id*. at p. 23, ¶72.

Plaintiffs' Complaint further alleges that the illegal conduct caused Plaintiffs to incur unreasonable and unnecessary out of pocket expenses; resulted in an invasion of their privacy; caused each of them to fear for their well-being and safety; interfered with their ability to use their telephones, computer, and television; caused fear for Ms. Attkisson's sources' well-being and safety, as well as her own; interfered with Ms. Attkisson's ability to maintain necessary contacts with sources to perform her professional investigative reporting duties as a member of the press; directly affected Ms. Attkisson's sources' willingness to communicate with her; distracted her from her duties as an investigative reporter and chilled her First Amendment rights; and resulted in irreparable tension in Ms. Attkisson's relationship with her employer (CBS), and that the illegal surveillance violated Plaintiffs' Constitutional rights. And specifically, the Complaint alleges that by subjecting Plaintiffs to illegal surveillance, Defendants sought to abridge the freedom of the press and chill the exercise of free speech and freedom of the press in a reckless manner with objective unreasonableness, and with the intent to violate Constitutional rights. *Id*. at p. 17, ¶66.

ARGUMENT

Defendants seek to dismiss the consolidated cases for (a) lack of subject matter jurisdiction; (b) improper venue; and (c) failure to state a claim for which relief may be granted.

1. SUBJECT MATTER JURISDICTION

The Defendants claim that a plaintiff may not base a FTCA claim on violations of a federal statute, citing *Art Metal-U.S.A., Inc. v. United States of America*, 753 F.2d 1151 (D.C. Cir. 1985). Defendants cite *Art Metal* for the general proposition that a violation of a federal statute by government officials does not of itself create a cause of action under the FTCA. *See Canadian Transport Co. v. United States*, 663 F.2d 1081, 1091 (D.C. Cir. 1980) ("Not every violation by the government of its regulations will give rise to an action under the Tort Claims Act.").

What Defendants leave out is the principle that FTCA liability attaches where state law recognizes comparable private liability and/or explicitly recognizes a private cause of action for violation of a statute. *Art Metal*, citing *Zabala Clemente v. United States*, 567 F.2d 1140, 1149 (1st Cir. 1977) cert. denied, 435 U.S. 1006, 98 S. Ct. 1876, 56 L. Ed. 2d 388 (1978); *United States v. Smith*, 324 F.2d 622, 624-25 (5th Cir. 1963) The pertinent inquiry is whether the duties set forth in the federal laws are analogous to those imposed under local tort law. *See Art Metal*, citing *Indian Towing Co. v. United States*, 350 U.S. 61, 76 S. Ct. 122, 100 L. Ed. 48 (1955); *Rayonier, Inc. v. United States*, 352 U.S. 315, 77 S. Ct. 374, 1 L. Ed. 2d 354 (1957).

Contrary to Defendants' argument, Section 1983 provides a cause of action for "the deprivation of any rights, privileges, or immunities secured by the Constitution and laws" of the United States, as well as providing a cause of action for violations of federal statutes. *See Maine v. Thiboutot*, 448 U.S. 1, 4 (1980). The burden is on the government to show "by express provision or other specific evidence from the statute [496 U.S. 498, 521] itself that Congress intended to foreclose such private enforcement." *Id*. The government not only fails to do this, it fails to even discuss the specific statutes.

Here, not only are Plaintiffs direct beneficiaries of the statutes in question in that they are persons protected under the words and/or purpose of each, the misconduct alleged involves illegal surveillance and intentional trespass of Plaintiffs' home, electronics, phones, and personal information by sophisticated electronic surveillance devices as well as invasion of privacy. The alleged intentional misconduct occurred in both Virginia and in the District of Columbia. The District of Columbia Court of Appeals has defined trespass as "an unauthorized entry onto property that results in interference with the property owner's possessory interest therein." *Sarete v. 1344 U Street Ltd. P'ship*., 871 A.2d 480, 490 (D.C. 2005). Trespass also applies to chattels. *Pearson v. Dodd*, 410 F.2d 701, 706-707 (D.C. Cir. 1969). As for invasion of privacy, in 2009, the Court of Appeals reaffirmed that the District of Columbia has "adopted the *Restatement* formulation of the 'right of privacy.'" *Bean v. Gutierrez*, 980 A.2d 1090, 1095 no. 6 (D.C. 2009) (citing *Vassiliades v. Garfinckel's, Brooks Bros*., 492 A.2d 580, 587 (D.C. 1985)). Virginia likewise recognizes the tort of trespass, which includes unlawful entry of plaintiff's premises without consent, including the right to recover damages for emotional distress even in absence of physical injury. *Johnson v. Marcel,* 251 Va. 58, 465 S.E.2d 815 (1996). Virginia also recognizes computer invasion of privacy, codified at Va. Code § 18.2-152.5. The thrust of all of these claims is that the wrongdoer intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs, provided that the intrusion would be considered highly offensive to a reasonable person.

Each of these causes of action involve lack of consent, interference or invasion with possessory interest, and intentional misconduct. The statutes at issue impose similar prohibitions. For instance, the ECPA was designed to protect private citizens from unauthorized government access into private electronic communications. 18 U.S.C. § 2510 *et seq.* The SCA was designed to

protect private citizens from unauthorized government access to stored private communications. The CFAA was designed to protect private citizens from the unauthorized attack on their computers and cell phones or by accessing someone's computer without authorization. FISA was created for purposes of intelligence gathering and establishes clear duties and limitations on surveillance and collection of data and information from private citizens. Lastly, the Virginia Computer Crimes Act ("VCCA") was designed to protect private citizens from unauthorized access to private computers. The Defendants breached those duties by violating the clear requirements of the statutes thus causing Plaintiffs to suffer damages. Given that the statutes in question were clearly designed to protect private citizens like Plaintiffs against the very harm caused, violation of those statutes is actionable.

As the court in *Art Metal* also noted, however, even where the statutes may not serve as a direct basis for FTCA liability, the statutes may nevertheless be important in determining whether the government may be liable under the FTCA. *Id*. By way of example, the statutes may provide evidence that the government assumed duties analogous to those recognized by local tort law. Where the statutes impose a duty analogous to state law, the regulations may also provide a duty and standard of care against which the government's conduct may be assessed. *See Art Metal*, citing *Canadian Transport*, 663 F.2d at 1091 (breach of tort duty "may be proven in an action against the United States by reference to standards applicable to federal employees").

Here, Plaintiffs allege that the government trespassed by illegally conducting surveillance in direct violation of their Constitutional and personal liberty rights. There can be no good faith argument that a cause of action for such conduct does not exist in either the District of Columbia or Virginia. Trespass, illegal tapping of computers and phones, invading privacy, and harming personal property are all valid claims under every state's laws.

2. COUNTS 1-6 – SOVEREIGN IMMUNITY

Defendants next contend that sovereign immunity precludes the present action as to Counts 1-6. The Government's analysis is simply wrong.

A. COUNT 1 – THE ELECTRONIC COMMUNICATION PRIVACY ACT CLAIM

While Defendants are correct that Count I (violation of the ECPA) does not lie against the United States, it does lie against each of the individual defendants. *Burkhart v. Saxbe*, 397 F. Supp. 499, 501 (E.D. Pa. 1975); *see also Smith v. Nixon*, 606 F.2d 1183 (D.C. Cir., 1979). The government may have preserved its own sovereign immunity, but it did not extend that protection to its agents or employees in their individual capacity.

B. COUNT 2 – THE STORED COMMUNICATIONS ACT CLAIM

The only way to argue that the United States is immune from violations of the SCA is to ignore the existence of 18 U.S.C. § 2712:

> Any person who is aggrieved by any willful violation of this chapter [18 U.S.C. §§ 2701 *et seq*.]…may commence an action in United States District Court against the United States to recover money damages.

The statute goes on to describe the means by which such suit is instituted:

> Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act…

Id.; *see also Jewel v. NSA*, 965 F. Supp. 2d 1090, 1108 (N.D. Cal. 2013) ("Accordingly, the Court finds that Section 2712 waives sovereign immunity for Plaintiffs' claims for damages under the Wiretap Act and the SCA.")

Given the language of the statute, there is no basis to claim (as Defendants do) that Count II "cannot form a proper basis for Plaintiffs' FTCA claims." Dkt. No. 74-1 at p. 8.

C. COUNT 3 – COMPUTER FRAUD AND ABUSE ACT

18 U.S.C. § 1030(g), the Computer Fraud and Abuse Act ("CFAA"), provides that:

> [a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.

The language of the statute, which subjects any "violator" to a civil action, stands in sharp contrast to the language of the ECPA:

> " … 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**, which engaged in that violation such relief as may be appropriate."

18 U.S.C. § 2520.

In adopting 18 U.S.C. § 1030, Congress elected not to exclude the United States from the class of potential defendants. In so doing, it waived sovereign immunity and chose to subject the United States to liability. *Sosa v. Alvarez-Machain*, 542 U.S. 692, 711 n.9 (2004) ("when the legislature uses certain language in one part of the statute and different language in another, the court assumes different meanings were intended.")

D. COUNT 4 – FOREIGN INTELLIGENCE SURVEILLANCE ACT

As with Count 2 – the SCA claim – the same analysis holds true for violations of the Foreign Surveillance Intelligence Act ("FISA"). 18 U.S.C. § 2712 specifically identifies "405(a) of the Foreign Intelligence Surveillance Act of 1978," and provides that it is similarly subject to the FTCA.

E. COUNT 5 – VIRIGINA'S COMPUTER CRIMES ACT

Despite Defendants' assertion to the contrary, the question of whether the federal government can be liable for violation of the Virginia Computer Crimes Act ("VCCA") is not

whether the statute is characterized as a penal or criminal statute under state law. Instead, and as the Defendants note in their brief:

> The FTCA grants a limited waiver of sovereign immunity for "tort claims against the United States…under circumstances where the United States, if a private person, would be liable to the claimant in accordance with the law of the place where the act or omission occurred."

Dkt. No. 74-1 at p. 8 (internal citations omitted), *quoting* 28 U.S.C. § 1346(b)(1) (2016). If Virginia law recognizes a cause of action under the VCCA as one which arises in tort, the FTCA would necessarily apply.

Va. Code § 18.2-152.4 regards a violation of the VCCA as a "computer trespass," and Virginia law generally treats violations of criminal statutes for which a civil remedy has been provided as actions in tort. *See, e.g.*, Va. Code § 18.2-499 and -500. Virginia law also treats non-contractual injuries to property as actions arising in tort. *Sensenbrenner v. Rust, Orling & Neale*, 236 Va. 419 (1988). Finally, Virginia law recognizes that a "private person" may be held civilly liable for violation of the VCCA. VCCA. *Physicians Interactive v. Lathian Sys.*, 2003 U.S. Dist. LEXIS 22868, at *20 (E.D. Va. Dec. 5, 2003); *McGladrey & Pullen, L.L.P. v. Shrader*, 62 Va. Cir. 401, 410 (Cir. Ct. 2003). Taken together, these cases demonstrate that a civil action for violation of the VCCA is one which arises in tort, and to which the FTCA applies.

Defendants also contend that a FTCA claim may not be based on the Virginia statute citing the Supremacy Clause and *Blackburn v. U.S.*, 100 F.3d 1426 (9th Cir. 1996). Defendants' reliance on *Blackburn* is misplaced. In *Blackburn*, the plaintiff filed a FTCA claim alleging that the Government was negligent in failing to warn of the danger of diving off a bridge in Yosemite National Park. As part of his claim, plaintiff argued that the Government was required to comply with the California Resort Act, and that the failure to comply subjected it to suit under the FTCA.

In essence, the plaintiff was arguing that the California Resort Act created a standard of care, and that the government's failure to meet that standard was negligent. In rejecting the argument, the Ninth Circuit, relying on *Missouri Pac. R.R. Co. v. Ault*, 256 U.S. 554 (1921), noted that absent a waiver of immunity, the United States is not subject to liability under state statutes that are penal in nature. Defendants' reliance on *Blackburn* for the blanket proposition that no FTCA claim may be based on a state statute is simply an incorrect reading and interpretation of the case and the law.

That a state statute is characterized as "penal" has no effect on the analysis under the FTCA. Instead, the question is whether or not state law recognizes a private cause of action (i.e. in tort) for violation of that statute by a private actor. If the answer is yes - that is, an individual could be liable in tort for violation of the statute - then the government can be liable under the FTCA unless one of the exceptions contained in 28 U.S.C. §2680 applies.

The Court's decision in *Blackburn* was based entirely on one of the enumerated exceptions to the FTCA, the "discretionary function" exception in 28 U.S.C. §2680:

> The FTCA's waiver of immunity is limited, however, by the discretionary function exception, which bars claims 'based upon the exercise or performance or the failure to exercise or perform a discretionary function or duty on the part of a federal agency or an employee of the Government, whether or not the discretion involved be abused.'

Blackburn, 100 F.3d at 1429, quoting 28 U.S.C. §2680. There is no argument that violating a state law against computer hacking is a "discretionary function", and not even the Government is arguing that any of the FTCA exceptions apply. Accordingly, *Blackburn* is inapposite.

The Virginia Computer Crimes Act is located at Title 18.2, Chapter 5, Article 7.1 of the Virginia Code. Section 18.2-152.12 of the Act provides that any person whose property or person is injured by reason of a violation of any provision of the Act may sue and recover damages, including costs of the suit. Damages includes lost profits. Included within the conduct proscribed

by the Act is "computer trespass", which is defined as any temporary or permanent removal of computer data, computer programs, or computer software from a computer; causing a computer to malfunction; alter or erasing computer data, programs or software; causing physical injury to the property of another; or causing to be made an unauthorized copy, in any form, of data, programs, or software residing on or in a computer. Any person who uses a computer without authority and with the intent to do any of the following is subject to both civil and criminal liability. Unlike *Blackburn*, the statute does not purport to regulate federal government operations or property at all, but is aimed to prohibiting illegal intrusions into a private citizen's computer.

That the holding in *Blackburn* does not preclude an FTCA claim based on a violation of the VCCA is in line with the language which appears in *Blackburn* in the immediately preceding paragraph, and which the Defendants themselves quote: "[T]he Government can be sued 'under circumstances where the United States, if a private person, would be liable to the claimant in accordance with the law of the place where the act or omission occurred.'" *Blackburn*, quoting 28 U.S.C. § 1346(b). If the John Does in question were private citizens who committed an act of computer hacking, they would be liable under the VCCA.

Here, Plaintiffs are not suing for a "penalty". Plaintiffs are suing for compensation under the Virginia statute, which is neither penal in nature nor does it contain any penalty whatsoever. Plaintiffs are not prosecutors attempting to prosecute. They are simply private citizens seeking compensation for intentional violations of their rights under Virginia and federal law.

F. COUNT 6 – ADMINISTRATIVE REMEDIES WERE, IN FACT, EXHAUSTED

Defendants next contend that Plaintiffs failed to exhaust administrative remedies as required under 28 U.S.C. § 2675 with regard to Count 6 of the FTCA Complaint. Defendants concede that Plaintiffs timely submitted SF-95 forms to both the DOJ and the USPS. Those

forms are attached to the Defendants' motion as Exhibits A and B (Dkt. Nos. 74-2, 74-3). In those forms, Plaintiffs provided DOJ and USPS with an extensive narrative of the factual basis for each of their claims. Nevertheless, Defendants argue that the SF-95 forms were insufficient as to Count 6 because the terms "common law trespass" were not specifically used. This argument relies upon a hyper-technical reading of 28 U.S.C. § 2675 that is not supported by this Court's case law.

There is simply no support for the proposition that 28 U.S.C. § 2675 is a "magic words" statute such that if a plaintiff does not say something in a specific way, she is forever barred from court. Rather, case law makes clear that "to exhaust administrative remedies, a plaintiff must have presented the agency with '(1) a written statement sufficiently describing the injury to enable the agency to begin its own investigation and (2) a sum-certain damages claim.'" *Slate v. D.C.*, 79 F. Supp. 3d 225, 233 (D.D.C. 2015). This formulation of the exhaustion requirement focuses on providing sufficient notice of the injury to enable the agency to begin an investigation. It is a notice requirement, not a magic words requirement. Indeed, the statute does not even require that the notice come on an SF-95 form, or in any particular form. Rather, "[a]ll that is necessary [under the FTCA's presentment requirement] is that a claim be specific enough to serve the purposes intended by Congress in enacting § 2675(a)—to ease court congestion and avoid unnecessary litigation, while making it possible for the Government to expedite the fair settlement of tort claims …" *Johnson v. United States*, 788 F.2d 845, 848 (2d Cir. 1986) (citations omitted).

Common law trespass includes any wrongful interference with a person's actual possessory rights in property. *See, e.g., Sarete, Inc. v. 1344 U Street Ltd. Partnership*, 871 A.2d 480, 490 (D.C. 2005). The rule was designed to address any situation where an owner's control or enjoyment over his or her chattel or land was diminished by wrongful conduct.

Here, the administrative claim (Schedule B) submitted to the government placed the government on clear notice of Plaintiffs' contention that employees or agents of the Department of Justice conducted unauthorized and illegal surveillance of Ms. Attkisson's laptop computers and telephones from 2011-2013. (Schedule B at p. 1) This intrusion produced operational anomalies in numerous electronic devices at their home in Virginia. These anomalies included a work Toshiba laptop computer and a family Apple desktop computer turning on and off at night without input from anyone in the household, the house alarm chirping daily at different times, often indicating "phone line trouble," and television problems, including unexplained interference. All of the referenced devices use the Verizon FiOS line installed in Ms. Attkisson's home. Verizon was unable to cure the problems despite multiple attempts over a period of more than a year. (Schedule B at p. 2) The surveillance required obtaining new equipment due to the problems associated with the electronics. (Schedule B at p. 2) The damage done to the property included interference and an inability to even use the equipment at times, including malfunctions that impaired her ability to operate the equipment. (Schedule B at pp. 4-5, 7)

In summary, the SF-95 forms filed went above and beyond in terms of informing the Government of the nature of the injuries claimed—intrusion upon their privacy and damage to their property. They therefore properly exhausted their administrative remedies under 28 U.S.C. § 2675, and the Government's motion should be denied.

3. VENUE IS PROPER IN THE DISTRICT OF COLUMBIA

Defendants next contend that the District of Columbia is an improper venue for Plaintiffs' FTCA claims because Plaintiffs reside in Virginia and because there was insufficient "meaningful conduct" in the District of Columbia. Although the Government again recites the general law

correctly, the flaw in Defendants' analysis is in the application of that law to the facts set forth in the Complaint.

Venue in the FTCA context is a two-pronged analysis. Venue is proper in an FTCA claim either where the Plaintiff resides or where the act or omission complained of occurred. 28 U.S.C. § 1402(b). As Defendants concede, in analyzing whether venue is proper, the Court must consider all facts alleged in the Complaint as true, must draw all reasonable inferences in Plaintiffs' favor, and must resolve any factual conflicts in Plaintiffs' favor. (Dkt. No. 74-1 at 14 (quoting *Darby v. U.S. Dep't of Energy*, 231 F. Supp. 2d 274, 276-77 (D.D.C. 2002)).

The first prong is not at issue because Plaintiffs do not live in this District, so the basis for venue in this District for the FTCA claims is that the acts or omissions complained of occurred in this District. As this Court has explained, an act or omission occurs in a district where "sufficient activities giving rise to the plaintiff's cause of action took place." *Zakiya v. United States*, 267 F. Supp. 2d 47, 58 (D.D.C. 2003). So the question is how much of the conduct set forth in the Complaint occurred in this District, and how meaningful was that conduct. Defendants arrive at the conclusion that there was insufficient "meaningful conduct" in this District only by misstating and minimizing the facts alleged in the Complaint.

The FTCA Complaint, which was the Complaint filed in Case No. 1:15cv1437, advances three parallel narratives that overlap to form the basis for Plaintiffs' claims. First, the Complaint lays out a detailed chronology of Mrs. Attkisson's journalistic work at CBS News in Washington that was critical of the Obama Administration and exposed certain scandals in which the Administration was involved. Her reporting, all of which was carried out in the District of Columba, relied heavily on confidential sources within the Administration. (1:15cv1437 Dkt. No. 1 (Compl.) ¶¶ 14-15, 17-22, 24, 26, 34-35).

Second, the Complaint alleges that in reaction to her reporting, as well as the work of other investigative journalists, the DOJ and FBI—from their headquarters in the District of Columbia—undertook efforts to discredit these stories and also to identify and shut-down the confidential sources being used in the reporting due to the politically sensitive nature of the issues. The efforts, Plaintiffs contend, included programs aimed specifically at discovering the source of the leaks via electronic means, all in the name of "cybersecurity." (*E.g., id.* ¶¶ 16, 30-31, 36, 38-39).

Third, the Complaint overlays these first two narratives with allegations concerning how, at the same time, Mrs. Attkisson and her family began experiencing problems with their communications devices and computers and their internet connectivity, which were used in both Virginia and the District of Columbia because, as is quite common, the devices are mobile thus permitting work to be done both in the District of Columbia and at home in Virginia. (*E.g.*, *id.* ¶¶ 23, 25, 28-29, 37, 40, 41, 43-46, 50). The Complaint alleges how forensic investigation revealed that a computer with an IP address owned by the US Postal Service—also located in the District of Columbia—was used to access Plaintiffs' electronic devices, place programs and data on those devices, and also extract information from those devices back to the USPS IP address. (*E.g.*, *id.* ¶¶ 27, 32, 42, 47-49.) Given that the devices were transported daily to and from the District of Columbia, and given that the software used to infiltrate the mobile devices was contained within the software wherever the devices traveled, the infiltration occurred in both Virginia and the District of Columbia.

Thus, in sum, the Complaint alleges a scenario in which due to negative reporting and embarrassing investigation into Government activity, reporting which was done from her office in the District of Columbia, agents of the United States government operating in the District of Columbia used remote electronic means to access Plaintiffs' electronic devices in both Virginia

and the District of Columbia, for purposes of surveillance and extraction of information back to the District of Columbia for use in identifying the sources providing information to Ms. Attkisson. When the wrongful act originated from the District of Columbia and resulted in information being returned back to the District of Columbia, Plaintiffs' respectfully submit that "sufficient activities giving rise to plaintiff's cause of action took place" in this District and that venue for the FTCA claims is thus proper in this District. *Zakiya*, 267 F. Supp. 2d at 58. To argue otherwise ignores facts and cherry-picks in a manner that is unreasonable.

Defendants place primary reliance on *Sanchez v. United States*, 600 F. Supp. 2d 19 (D.D.C. 2009), to support the argument that venue is improper. In *Sanchez*, this Court confronted claims based on decisions allegedly made in Washington D.C. but which concerned solely actions in Puerto Rico and affected only Puerto Rico. Defendants specifically latch onto the Court's observation that "when conduct occurs in one district but has intended effects in another, the act 'occurs' in the jurisdiction where its effects are directed." *Id.* at 21 (internal quotations omitted). Defendants then portray Plaintiffs' Complaint as alleging that the wrongful acts were directed solely at Plaintiffs' home in Virginia, and that *Sanchez* thus means that the acts occurred in Virginia.

But this characterization of Plaintiffs' Complaint by Defendants focuses on only half of the story. Plaintiffs' Complaint does not merely concern decisions made in Washington, D.C., but effectuated somewhere else downstream. To the contrary, the Complaint alleges a course of conduct in which tangible concrete conduct occurred in Washington, D.C.—the use of the USPS IP address to remotely access Plaintiffs' electronic devices in both Virginia and the District of Columbia—that resulted in wrongfully obtained information coming back to Washington, D.C. for use by Government agents in Washington, D.C. to unmask leaks within the Government.

Washington, D.C. is therefore the center of gravity for Plaintiffs' Complaint, and so venue is proper in this District for Plaintiffs' FTCA claims.

4. INDIVIDUALS AS PLAINTIFFS

Defendants next incorrectly claim that a suit against individual government employees is forbidden under the FTCA. Although it is accurate to say that the FTCA does not create a statutory cause of action against individual government employees, individual employees may still be subject to a lawsuit in their individual capacities for violation of federal or state law. No less an authority than the November 2010 edition of the United States Attorneys' Bulletin recognizes that "some statutes create a private right of action which may be asserted against a federal employee in his individual capacity,"[4] citing *Quon v., Arch Wireless Operating Co., Inc*., 445 F.Supp.2d 1116, 1128 (C.D. Cal. 2006).

While individual defendants may have absolute immunity, such immunity only attached when the Attorney General certifies that the employee was acting within the scope of employment at the time of the incident out of which the claim arose. 28 U.S.C. § 2679(d)(1). If and when the Attorney General makes such a certification, the tort suit automatically converts to an FTCA action against the United States in federal court and the Government becomes the sole party defendant. If the Court disagrees with the Attorney General's determination, the state-law tort suit may proceed against the defendant government employee, individually, in his or her personal capacity. *See Harbury v. Hayden*, 522 F.3d 413 (D.C. Cir. 2008), citing *Gutierrez de Martinez v. Lamagno,* 515 U.S. 417, 423-24, 434, 115 S. Ct. 2227, 132 L. Ed. 2d 375 (1995); *Council on Am. Islamic Relations v. Ballenger,* 444 F.3d 659, 662 (D.C. Cir. 2006). Of course, the very existence

[4] Pgs. 11 and 12, available at https://www.justice.gov/sites/default/files/usao/legacy/2010/12/06/usab5806.pdf

of the Westfall Act further proves that individual liability may lie – otherwise, the Westfall Act would be entirely superfluous, as employees would be immune without the need for certification.

5. COUNTS 7-8 – THE COMPLAINT STATES A VALID *BIVENS* CLAIM

A. THE "*POST HOC ERGO PROPTER HOC*" ARGUMENT FAILS

Choosing to ignore the detailed factual evidence presented in the Complaint, including forensic evidence showing that the IP address used to illegally invade Plaintiffs' privacy was owned, controlled, and operated by the USPS, Defendants argue that Plaintiffs' claims must be dismissed because they amount to little more than "an outline of a sequence of events", and that although temporally connected in a causal link, the Court should ignore the clear temporal connection and give it "little weight", citing *Arias v. DynCorp*, 928 F. Supp. 2d 10, 21 (D.D.C. 2013) and *Maduka v. Meissner*, 114 F.3d 1240 (D.C. Cir. 1997). The argument is without merit because it implies that the Complaint is entirely based on nothing but a timeline, which is a mischaracterization of significant proportion.

Contrary to Defendants' argument, Plaintiffs' entire case does not rest on a temporal connection between Ms. Attkisson's reporting and the illegal intrusion. Although the temporal connection is compelling circumstantial evidence in terms of motive, especially when combined with the forensic evidence, documentary evidence, government reports, and public records documenting admissions by the government, the guts of the claim, as set forth clearly in the Complaint, is that Defendants illegally invaded electronic systems using an IP address owned by the U.S. Government and left forensic evidence behind proving that the illegal invasion occurred. Although it is easy to see why Defendants would prefer to ignore the existence of this compelling proof, as well as the clear temporal connection establishing motive for the intrusion, it is disingenuous to argue one while ignoring the other.

The case law cited by Defendants is equally unconvincing. For instance, *Arias* was a toxic tort case involving 2,000 Ecuadorian citizens who brought claims of negligence (among others) against DynCorp alleging personal injuries caused by the spraying of herbicides over land in Ecuador. The issue before the Court was a motion under Rule 702 to exclude an expert witness because the opinions he proffered were unreliable. In addressing methods experts apply in toxic tort cases to draw conclusions about causation, the district court noted that "an expert may rely on a temporal relationship between exposure to the toxic and subsequent adverse health effects" to establish both general and specific causation, and in compelling circumstances, a temporal relationship alone is sufficient to establish general causation. Granted that the methodology used by a toxicologist to establish causation between a toxic chemical and injury is irrelevant to pleading a constitutional violation, even if it was relevant, *Arias* stands for the proposition that a temporal relationship can be compelling enough, standing alone, to establish cause and effect.

The other case cited by Defendants – *Maduka v. Meissner*, 114 F.3d 1240 (D.C. Cir. 1997) – is equally irrelevant to the issues. *Maduka* involved an attempt to obtain an administrative review of an INS decision to deny Maduka a visa, which was denied because he got married for the purpose of evading immigration laws. The only issue before the district court was whether Maduka was entitled to fees and costs because the filing of the complaint, it was alleged, caused the INS to approve the visa application. In rejecting the claim for fees and costs, the court noted that there was no proof that the filing of the lawsuit was a necessary or substantial factor in obtaining the result, and that although chronology is important in determining causation it is it is by no means dispositive. Here, Plaintiffs have plead proof, including forensic evidence, public admissions, internal documents and standards, and internal communications proving that the government was trying to "muzzle" Plaintiff Attkisson's reporting.

The argument that the entire Complaint fails because all that is plead is a "temporal" relationship in the form of a timeline mischaracterizes the Complaint and ignores reality.

B. ***ASHCROFT v. IQBAL*: THE COMPLAINT IS NOT ONLY PLAUSIBLE – IT IS FACTUALLY COMPELLING**

Referring to Plaintiffs' allegations as "fantastic", the Government next argues that the Complaint fails to survive the "plausibility" standard in *Iqbal* because *respondeat superior* does not apply and because the claims are simply, in their words, not plausible. Defendants' arguments fail.

Defendants' heavy reliance on *Iqbal* is misplaced. *Iqbal* was a *Bivens* action brought by a Pakistani national who alleged discriminatory treatment in the post-September 11, 2001, period by numerous federal officials while he was detained for allegedly defrauding the U.S. with regard to identification documents, charges to which he plead guilty prompting his deportation. *Ashcroft v. Iqbal*, 129 S. Ct. 1937, 1949 (2009). There was no dispute that the facts alleged by *Iqbal* stated a valid *Bivens* claim against all individuals involved in his treatment. *Id.* Rather, the narrow question in *Iqbal* was whether *Bivens* liability – which indisputably cannot be based on *respondeat superior* – attached under a theory of supervisory liability where the claim as plead only included a claim, unlike the present case, that the supervisor's mere knowledge of his subordinate's discriminatory purpose was sufficient to satisfy the pleading requirement.

A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. *Iqbal*, at 1949 (citing *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 556, 127 S.Ct. 1955, 167 L.Ed.2d 929 (2007)). The plausibility standard is not akin to a "probability requirement", but it asks for more than a sheer possibility that a defendant has acted unlawfully. *Id.* Where a complaint pleads facts

that are merely consistent with a defendant's liability, it stops short of the line between possibility and plausibility of entitlement to relief. *Id.* (Citing *Twombly*, 550 U.S. at 557 (brackets omitted).

As to the first point, Defendants confuse the concepts of *respondeat superior* and supervisory liability in a manner designed to blur a critical distinction in *Bivens* jurisprudence. Although Defendants are correct about the inapplicability of *respondeat superior*, Defendants' arguments are wrong on supervisory liability.

In order for a defendant to be liable under *Bivens*, there must be a constitutional duty imposed on the defendant that runs to the plaintiff that is breached. The breach of constitutional duty supplies the required threshold "fault" for liability to attach. The causation requirement follows from the "subjects, or causes to be subjected" language as well as the fundamental tort liability requirement for causation. Historically, the causation hurdle in *Bivens* was characterized as imposing a requirement of a showing of "personal involvement", which precluded responsibility based on *respondeat superior* liability. In simple terms, "personal involvement" translates into the notion of affirmative conduct constituting fault. As the Supreme Court noted in *Monell*, a mere "right to control without any control or direction having been exercised and without any failure to supervise is not enough" to support liability. *Monell v. Dep't of Social Services* 436 U.S. 658, 694 n.58. In plain language, the mere failure to act, standing alone, is insufficient to establish liability. That legal premise has no applicability to the present Complaint, which clearly goes far beyond a mere "failure to act".

Turning to supervisory liability, *Iqbal* did slightly modify one aspect of supervisory liability in that the Supreme Court made clear that personal involvement was required for supervisory liability to attach, and that the complaint must include plausible allegations that a *Bivens* defendant personally violated a constitutional right in order to be liable in a supervisory

capacity. Rather than focusing on state of mind, actual knowledge, or deliberate indifference, the key to supervisory liability after *Iqbal* is personal involvement. *Iqbal*, 129 S. Ct. 1954.

In the context of First Amendment claims under *Bivens*, a plaintiff is required to establish by a preponderance of the evidence that: (1) plaintiff was engaged in constitutionally protected conduct: herein, freedom of the press; (2) the Government took action that violated her constitutionally protected conduct; and (3) the plaintiff's protected conduct was a "substantial or motivating factor" for the defendants' illegal action. If the plaintiff makes this three-part showing, then the defendant must establish by a preponderance of the evidence that it would have conducted itself the same way even in the absence of the protected conduct. *See, e.g., Lakeside-Scott v. Multnomah County*, 556 F.3d 797, 803 (9th Cir. 2009) (citing *Mt. Healthy City Sch. Dist. v. Doyle*, 429 U.S. 274, 287, 97 S.Ct. 568, 50 L.Ed.2d 471 (1977)); *see also Garcetti v. Ceballow*, 547 U.S. 410, 126 S.Ct. 1951, 164 L.Ed.2d 689 (2006); *White v. State*, 131 Wn.2d 1, 11, 16–18, 20, 929 P.2d 396 (1997); *Bd. of County Comm'rs, Wabaunsee County v. Umbehr*, 518 U.S. 668, 675, 116 S.Ct. 2342, 135 L.Ed.2d 843 (1996).

As for Fourth Amendment claims, the causation inquiry is typically focused on the absence of probable cause. *See, e.g., Hartman v. Moore*, 547 U.S. 250, 259–66, 126 S.Ct. 1695, 164 L.Ed.2d 441 (2006); *Beck v. City of Upland*, 527 F.3d 853 (9th Cir. 2008).

Here, there can be no reasonable dispute that Ms. Attkisson, a national news reporter for CBS, was engaged in constitutionally protected conduct as part of her job as a journalist. The Complaint very clearly sets forth convincing evidence, including forensic, internal email, internal documents, and publicly-available direct quotes from the agents indicating that the Government took action that violated her constitutionally protected conduct in a manner designed to chill freedom of the press. The facts plead are not only plausible, they are convincing and supported by

forensics and documents. Lastly, the Complaint very clearly pleads facts demonstrating that Plaintiff's protected conduct was a "substantial or motivating factor" for the defendants' illegal action in that the internal correspondence from General Holder and his staff directly show the link between the two[5]. All of which was in direct violation of her Constitutional rights and the laws cited. Dkt. No. 1 at p. 8, ¶27.

Contrary to Defendants' skewed characterization of the Complaint as a "fallacy", the foregoing are examples of well-plead facts, not simply "temporal connections" or "fallacies," all of which include details, times, places, personal involvement, forensic evidence, documentary evidence, and oral admissions all demonstrating a clear violation of Constitutional rights that were a proximate and substantial cause in Plaintiffs' alleged damages. The supervisory liability claims, unlike *Iqbal*, focus on personal involvement rather than a "failure to act", and set forth facts showing that the individual defendants were intimately involved in creating and shaping policies, making public statements, and taking credit for a program of surveillance that was unprecedented and illegal, all in an effort to chill First Amendment privileges. Defendants' motion should be denied.

C. THE "PATENTLY INSUBSTANTIAL" DOCTRINE IS INAPPLICABLE

Citing *Tooley v. Napolatino*, Defendants next urge dismissal claiming that the allegations are "patently insubstantial" claims that are "essentially fictitious" and "absolutely devoid of merit." *Tooley v. Napolatino* 586 F.3d 1006, 1009-10 (D.C. Cir. 2009). The argument ignores forensic evidence; ignores publicly available evidence from the mouths of the Defendants conceding the

[5] The operative Complaint cites to clear factual evidence from internal correspondence of conversations, including General Holder and his staff, of a desire, intent, and plan to "muzzle" Ms. Attkisson's reporting, which is a direct link to the First Amendment rights trampled on in this case. (Dkt. No. 1 at p. 20, ¶ 72). The link could not be stronger.

existence of policies and practices designed to target members of the press with inappropriate surveillance techniques; and ignores internal documentation produced in other litigation as well as by third parties proving the intent to "muzzle" Ms. Attkisson's First Amendment rights due to reporting that placed the Administration and agencies at issue in a challenged position on a variety of topics. Rather than bizarre conspiracy theories of fantastic government manipulations of the mind or will of a *pro se* plaintiff, the facts plead are actual facts, specific details, and solid proof from a number of different forensic experts who found undisputed evidence that the electronic devices at issue were illegally invaded from an IP address owned and operated by the U.S. Government. So, while the Plaintiffs certainly agree that it is hard to believe that the U.S. Government would so blatantly violate so many constitutional and statutory rights, that is exactly what the evidence indicates occurred here. Conscience-shocking to be sure, but, unfortunately, not fantasy.

Contrary to Defendants' self-serving description of the Complaint, the "patently insubstantial" doctrine is reserved for use where "bizarre conspiracy theories of fantastic government manipulations of their will or mind" are put forth by typically *pro se* plaintiffs. *See, e.g., Hu v. U.S. Dep't of Def.*, No. 13-5157, 2013 WL 6801189, at *1 (D.C. Cir. Dec. 11, 2013) (district court properly dismissed complaint under Fed. R. Civ. P. 12(b)(1) where "its factual allegations were 'essentially fictitious,' involving a fantastic scenario of a vast government conspiracy to interfere in appellant's daily life, including through the implantation of a micro-tracker in her mouth and use of electromagnetic radiation weapons"), cert. denied sub nom., *Hu v. Dep't of Def.*, 135 S. Ct. 90 (Oct. 6, 2014); *Moore v. Bush*, 535 F. Supp. 2d 46, 48 (D.D.C. 2008) (dismissing case under Fed. R. Civ. P. 12(b)(1) where plaintiff alleged that a conspiracy "led to the implantation of a micro-chip in his head and use of brain wave technology to disrupt his life");

Bestor v. Lieberman, 03cv1470, 2005 WL 681460, at *1-2 (D.D.C. March 11, 2005) (dismissing case under Fed. R. Civ. P. 12(b)(1) where plaintiff alleged that two Senators were "involved in the irradiation of his brain and manipulation of his thought processes via devices surreptitiously implanted in his head").

Although not discussed at any length by Defendants, the accepted test for assessing the defense that a claim is "patently insubstantial" is to consider whether the claim is "flimsier than doubtful or questionable . . . essentially fictitious." *Best v. Kelly*, 39 F.3d at 228, 330 (internal quotation marks omitted); *see Hagans v. Lavine*, 415 U.S. 528, 536–1379) ("federal courts are without power to entertain claims otherwise within their jurisdiction if they are so attenuated and unsubstantial as to be absolutely devoid of merit, wholly insubstantial, [or] obviously frivolous") (internal citations and quotation marks omitted); *see, e.g., Peters v. Obama*, Misc. Action No. 10-298 (CKK), 2010 WL 2541066 , at *2 (D.D.C. June 21, 2010) (*sua sponte* dismissing complaint alleging that President Obama had been served with and failed to respond to an "Imperial Writ of Habeas Corpus" by the "Imperial Dominion of Amexem," requiring the plaintiff's immediate release from a correctional institution).

Here, Plaintiffs' claims are based on multiple-sourced forensic evidence, documentary admissions, documented reports, internal communications conceding an intent to "muzzle" Ms. Attkisson, and direct proof that the illegal invasion occurred from an IP address owned, operated and controlled by Defendants. This is not a case involving wild claims that the government implanted a multifunctional nano-chip that acts as a recorder and a transmitter in order to record thoughts, dreams, words, concepts, and behaviors, or claims of a vast government conspiracy to harm plaintiff with electromagnetic radiation, or wild fantasy stories involving fictitious planets taking control of government. Although Defendants clearly desire to use self-serving language to

mischaracterize the claims, Plaintiffs suffered what no American should ever have to suffer: an illegal intrusion into their home, electronics, and personal life by a Government charged with the responsibility to protect, not harm, them, all for political reasons and to chill free speech.

D. FIRST AMENDMENT PROTECTION AND *BIVENS*

Defendants next claim that a *Bivens* action does not exist for illegal surveillance of a news reporter under the First Amendment, and that even if one is available, they are entitled to qualified immunity. In plain terms, Defendants claim that no remedy exists for illegal surveillance carried out by the government of a news reporter's home, work, and personal electronic devices, all in direct violation of First Amendment rights that have existed since our founding fathers established our government. The fact that the government even makes such an argument is frightening.

Judge James E. Boasberg of the District of Columbia has already rejected Defendants' argument that a plaintiff has no *Bivens* claim against federal officers for violation of First Amendment free speech rights, including claims that qualified immunity likewise precluded the action. *See, e.g., Bloem v. Unknown Department of the Interior Employees*, 920 F.Supp.2d 154 (D.D.C. 2013). Although Judge Boasberg's ruling was unsurprising given the state of circuit law and the approach in other circuits to the question of whether a plaintiff may bring a First Amendment claim against federal officers, what is surprising is that the Government continues to urge the rejected notion that no such claim exists.

In *Bloem,* plaintiff brought suit under *Bivens*[6] for the seizure and destruction of his property during the so-called "Occupy DC" protests, which he alleges violated his First, Fourth, and Fifth Amendment rights. Much as Defendants have done in the instant case, the defendants in *Bloem*

---

[6] *Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics*, 403 U.S. 388, 91 S.Ct. 1999, 29 L.Ed.2d 619 (1971).

moved to dismiss, arguing that a *Bivens* action did not exist under the First Amendment, and that even if one were available, defendants were entitled to qualified immunity. Both claims by the Government were rejected by Judge Boasberg, who found that Plaintiff could, in fact, pursue a *Bivens* remedy for the First Amendment claim and that defendants were not entitled to qualified immunity.

In addressing the issue of whether a *Bivens* action may lie for violations of First Amendment rights, Judge Boasberg first noted that both this Circuit and this Court have already held that a *Bivens* action may lie for violations of the First Amendment rights of demonstrators. *See Dellums v. Powell,* 566 F.2d 167, 194-196, 1977 U.S. App. LEXIS 12165, 184 U.S. App. D.C. 275, 24 Fed. R. Serv. 2d (Callaghan) 20 (D.C. Cir. 1977); *Hartley v. Wilfert,* 918 F.Supp.2d 45, 50-52, 2013 WL 266514, at *4-5 (D.D.C. January 24, 2013). The court likewise noted that in the ensuing 35 years, other courts reached precisely the same conclusion.[7] In *Paton v. La Prade,* 524 F.2d 862, 870 (3d Cir. 1975), for instance, the Third Circuit observed:

> Were there no cause of action for federal infringement of first amendment rights, an aggrieved individual could seek damages for violations of his first amendment rights by state officials, 42 U.S.C. § 1983, but not by federal officials. There is no reason to allow federal officials to act with impunity in this context and to bar state officials. The damage to the individual's first amendment interests is the same regardless of the perpetrator of the violation. *Id.* at 870; *see also Gibson,* 781 F.2d at 1342 n. 3 (noting that "[g]iven the availability of § 1983 relief against state agents who infringe First

---

[7] *See Mendocino Envtl. Ctr. v. Mendocino Cnty.,* 14 F.3d 457, 464 (9th Cir.1994)(plaintiffs stated *Bivens* claim where complaint contained specific factual allegations that tended to show FBI agents intended to interfere with plaintiffs' First Amendment rights); *Gibson v. United States,* 781 F.2d 1334, 1342 (9th Cir.1986) (allegation that "FBI agents acted with impermissible motive of curbing plaintiff's protected political speech cognizable through *Bivens*-type action directly under First Amendment"); *Paton v. La Prade,* 524 F.2d 862, 870 (3d Cir. 1975) (extending *Bivens* remedies "to violations of First Amendment rights where plaintiff can prove First Amendment rights were violated by a federal government employee,); *Jihaad v. Carlson,* 410 F.Supp. 1132, 1134 (E.D.Mich.1976) ("the rationale of *Bivens* may, in a proper case, be applied to violations of the first as well as the fourth amendment").

> Amendment rights, it is hard to see why *Bivens* relief should not be available to redress equivalent violations perpetrated by federal agents") (citing *McKinley v. City of Eloy,* 705 F.2d 1110 (9th Cir.1983)) (internal citation omitted). Indeed, just last month this Court held that a protester who was intimidated into leaving the White House sidewalk by Secret Service officers could bring a *Bivens* action for interference with her First Amendment rights. *See Hartley,* 918 F.Supp.2d at 50-51, 2013 WL 266514, at *4.

Lastly, Judge Boasberg rejected defendant's argument that a *Bivens* cause of action for First Amendment violations – as recognized in *Dellums* – did not survive the Supreme Court's decision in *Ashcroft v. Iqbal,* 556 U.S. 662, 129 S.Ct. 1937, 173 L.Ed.2d 868 (2009). Judge Boasberg noted that even if the Government was correct in predicting the Supreme Court's response to questions not yet before it, the District Court for the District of Columbia "cannot accept its invitation to depart from this Circuit's binding precedent." *See Critical Mass Energy Project v. Nuclear Regulatory Comm'n,* 975 F.2d 871, 876 (D.C.Cir.1992) (*en banc*) (decisions of D.C. Circuit are binding "unless and until overturned by the court *en banc* or by Higher Authority") (citation omitted); *Owens-Ill., Inc. v. Aetna Cas. & Sur. Co.,* 597 F.Supp. 1515, 1520 (D.D.C.1984) ("The doctrine of *stare decisis* compels district courts to adhere to a decision of the Court of Appeals of their Circuit until such time as the Court of Appeals or the Supreme Court of the United States sees fit to overrule the decision.").

Turning to the second issue presented in *Bloem* – the issue of whether a *Bivens* remedy was appropriate where a comprehensive statutory scheme (the federal small-claims statute) had been established to provide relief in a given area – Judge Boasberg likewise disposed of the Government's argument by noting that the constitutional interests at issue under the First Amendment – freedom of speech, among others – were a far cry from the interests safeguarded by the small-claims statute, which protects individuals from the government's negligent mishandling

of property. As noted by the Supreme Court, the FTCA supplements, but does not supplant, the availability of a *Bivens* action. In *Carlson v. Green,* 446 U.S. 14, 100 S.Ct. 1468, 64 L.Ed.2d 15 (1980), the Court noted a number of deficiencies in the Federal Tort Claims Act—in comparison to a *Bivens* action—that made the statute "[p]lainly ... not a sufficient protector of the citizens' constitutional rights." *Id.* at 23, 100 S.Ct. 1468. There, the Court observed that *Bivens* can be preempted only where "Congress has created what it views as an *equally* effective remedial scheme. Otherwise the two can exist side by side." *Id.* at 23 n. 10, 100 S.Ct. 1468 (emphasis in original). The small-claims statute here suffers from many of the same deficiencies the Court observed in *Carlson:* recovery is limited, punitive damages are not available, and the deterrent effect provided by personal liability under *Bivens* may be limited where damages are paid by the agency. *See id.* at 21-23. As a result, like the FTCA, the small-claims statute does not provide an adequate substitute for a *Bivens* remedy for the constitutional violations alleged here. *Cf. Hartley,* 918 F.Supp.2d at 56, 2013 WL 266514, at *10(finding Privacy Act did not preempt First Amendment *Bivens* claim).

Lastly, with respect to Defendants' claim that the operative Complaints fail to appropriately define the First Amendment rights violated, the claim is without merit and is in many ways disturbing given that it comes from the very Government who is supposed to be charged with the responsibility of protecting Constitutional rights.

One of the fundamental purposes of the First Amendment is to ensure that the public is well-informed about the functioning of its government, including the critical job of protecting the free discussion of governmental affairs. *See, e.g., Mills v. Alabama*, 384 U.S. 214, 218 (1966). Illegal and invasive surveillance programs implicate privacy rights of all Americans, and information pertaining to that surveillance naturally qualifies as a matter of profound significance

warranting First Amendment protection. *See, e.g., Connick v. Myers*, 461 U.S. 138, 145 (1983) (speech concerning public matters is more than self-expression; it is the essence of self-government). Allowing the public to make informed decisions about the operations of their government merits the highest degree of First Amendment protection. *McKinley v. City of Eloy*, 705 F.2d 1110, 1114 (9th Cir. 1983).

Under the First Amendment, the government has no power to restrict expression because of its message, its ideas, its subject matter, or its content. *Brown v. Entm't Merchs. Ass'n*, 131 S. Ct. 2729, 2733 (2011). This means the Government may not interfere with the distribution of information and opinions. During the time of the British colonies in America, prior to the signing of the *Declaration of Independence*, the media was subject to a series of regulations. British authorities attempted to prohibit the publication and circulation of information in which they did not approve. The Free Press Clause protects the right of individuals to express themselves through publication and dissemination of information, ideas and opinions without interference, constraint or prosecution by the government, including illegal surveillance of the media and its representatives. This is true because protection of speech and expression is central to the concept of the American political system, including a direct link between freedom of speech and vibrant democracy. Free speech is an indispensable tool of self-governance in a democratic society. Rather than having the government establish and dictate truth, freedom of speech enables the truth to emerge from diverse opinions.[8]

[8] Concurring in *Whitney v. California,* 274 U.S. 357 (1927), Justice Louis Brandeis wrote that "freedom to think as you will and to speak as you think are means indispensable to the discovery and spread of political truth."

The Constitution's framers provided the press with broad freedom, including the freedom necessary to the establishment of a strong, independent press sometimes referred to as our "fourth branch" of the government.

Contrary to Defendants' views, this bundle of rights, largely developed by U.S. Supreme Court decisions, defines the "freedom of the press" guaranteed by the First Amendment. For instance, *Near v. Minnesota*, 283 U.S. 697 (1931), recognized freedom of the press by rejecting prior restraints on publication and ruling that a Minnesota law targeting publishers violated the First Amendment. *Branzburg v. Hayes*, 408 U.S. 665 (1972), was yet another landmark decision invalidating the use of the First Amendment as a defense for reports summoned to testify before a grand jury. Yet another was *New York Times Co. v. United States*, 403 U.S. 713 (1971), a decision making it possible for two newspapers to publish the then-classified Pentagon Papers without risk of government censorship or punishment.

These rights are not only critical, they are central to our form of government and our way of life. Any illegal intrusion by the government is inappropriate and actionable.

6. QUALIFIED IMMUNITY

A. THE FIRST AMENDMENT CLAIM: COUNT 7

The qualified-immunity defense is designed to shield government agents from liability for civil damages if their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known. *Behrens v. Pelletier*, 516 U.S 299 (1996), citing *Harlow v. Fitzgerald*, 457 U.S. 800, 818 (1982). Defendants Holder and Donahoe argue they are entitled to qualified immunity as to Count 7 – the First Amendment claim – because no reasonable official would have understood that illegal, warrantless surveillance and cyber-attacks on a U.S. citizen in the media violated First Amendment rights. Dkt. No. 72-1at pp. 56-57. The argument is

not only without precedent, it is extremely disturbing to think that top officials of our government would ever take the position that "no reasonable government official" would have known or expected that illegal, warrantless surveillance of a news reporter using state of the art cyber-attack-software was illegal. It's frankly an astonishing and frightening position.

In *Branzburg v. Hayes*, 408 U.S. 665 (1972), the Supreme Court addressed the issue of whether requiring newsmen to appear and testify before state or federal grand juries abridges the freedom of speech and press guaranteed by the First Amendment. The Petitioners pressed First Amendment claims, arguing that it is often necessary for members of the press to agree either not to identify the source of information published or to publish only part of the facts revealed, or both; that, if the reporter is nevertheless forced to reveal these confidences to a grand jury, the source so identified and other confidential sources of other reporters will be measurably deterred from furnishing publishable information, all to the detriment of the free flow of information protected by the First Amendment. *Id*. at 680. Although *Branzburg* is not directly on point with the facts here, the key constitutional principles enunciated are highly relevant to the issue of whether a reasonable public official would have understood that illegal, warrantless surveillance and cyber-attacks on a U.S. citizen in the media, and her family, violated First Amendment rights.

What was present in *Branzburg* was not nearly as important as what the Supreme Court noted was not present. For instance, the Supreme Court noted that neither party in *Branzburg* was suggesting that news gathering like Ms. Attkisson's reporting does not qualify for First Amendment protection because without some protection for seeking out the news, freedom of the press might be eviscerated. *Id*. at 681-82. Likewise, the Court noted, unlike in the present case, that *Branzburg* facts did not involve government intrusions upon speech or assembly, no prior restraint or restriction on what the press may publish, and no express or implied command that the

press publish what it prefers to withhold. *Id*. at 681-82. Similarly, no attempt was made to require the press to publish its sources of information or indiscriminately to disclose them on request, including illegal surveillance and capture of the information from the press. *Id*. at 681-82. To the contrary, the sole issue before the court in *Branzburg* was the obligation of reporters to respond to grand jury subpoenas as other citizens do, and to answer questions relevant to an investigation into the commission of crime. *Id* at 683. The case did not involve restraint on what newspapers could publish or on the type or quality of information reporters might seek to acquire, nor did it threaten the vast bulk of confidential relationships between reporters and their sources as illegal surveillance does here. Most telling, however, was the Supreme Court's comment that "[i]t would be frivolous to assert -- and no one does in these cases -- that the First Amendment, in the interest of securing news or otherwise, confers a license on the reporter to violate criminal laws." *Id.* at 692. The opposite is true as well in that it would be frivolous to assert that the First Amendment confers a license on the Government to violate criminal laws in doing what is otherwise not permitted legally under the Constitution. To argue that no reasonable official would realize that illegal surveillance of a private citizen in the media to collect what could only be collected with a warrant is similarly frivolous.

As if the foregoing was not sufficient to place a reasonable official on notice, the *Branzburg* court continued noting that, by way of example, official harassment of the press undertaken not for purposes of law enforcement, but to disrupt a reporter's relationship with his news sources would have no justification. *Id*. at 708. Tellingly, the Supreme Court as far back as 1972 made it crystal clear to all concerned, including reasonable government officials, that harassment, such as illegal surveillance and cyber-attacks, of a member of the press undertaken not for purposes of law

enforcement, but to simply "muzzle" or disrupt a reporter's relationship with sources had no reasonable justification under the law.

The clear message in *Branzburg* was that the First Amendment right at issue herein is clearly established. But like all constitutional rights, it is not an absolute right and so the question becomes by what process and under what circumstances can the government defeat that right. The government is permitted to try via legal process – a subpoena or a warrant – and whether the government's interests in the information outweighs the individual's First Amendment rights can then be determined by the courts. What the government clearly cannot do is engage in unilateral self-help, by illegal means, in violation of the Constitution. Plaintiffs have plead very specific First Amendment rights that were violated rather than simply general, broad principles. As a consequence, the motion must be denied.

If the foregoing is not sufficient, in 1979, the Third Circuit, in addressing a similar issue, noted that the interrelationship between news-gathering, news dissemination, and the need for a journalist to protect his or her source is "too apparent to require belaboring". *Riley v. City of Chester*, 612 F.2d 708 (3d Cir. 1979).

Not only has the government ignored clear precedent establishing the very rights sought to be protected here, the government has ignored its own internal rules and regulations designed to prevent the very illegal conduct perpetrated. According to Section 10-18.3(1)(d) of the FBI policies for online investigations, which are located in the *Manual of Investigative Operations & Guidelines*, Part 2 ("MIOG 2") (2007), FBI agents are – and were – prohibited from hacking into computers, including those belonging to subjects of FBI investigations, without legal authorization. Section 10-18.3 likewise stated that "[s]oftware tools cannot be used to defeat the security system of [a] targeted electronic facility or access areas that are not already publicly

viewable by general users of the system or the public absent a search warrant or other legal authorization."[9] As an example, the provision identified Internet Protocol addresses as information that could not be obtained through software tools without legal authorization.

There is yet more. The federal wiretap law, passed in 1968, permits surreptitious recording of conversations when one party consents, "unless such communication is intercepted for the purpose of committing any criminal or tortious act in violation of the Constitution or laws of the United States or of any State." Amendments signed into law in 1986 and 1994 expanded the prohibitions to unauthorized interception of most forms of electronic communications, including satellite transmissions, cellular phone conversations, computer data transmissions and cordless phone conversations.

The foregoing without question demonstrates that General Holder and Mr. Donahoe, among others, both objectively and subjectively knew such warrantless surveillance and information collection was illegal because they had actual knowledge that a warrant was necessary to search a newsroom or a reporter's home where there was reason to believe evidence of a crime would be found. *Zurcher v. Stanford Daily*, 436 U.S. 547 (1978), reh'g denied, 439 U.S. 885 (1978).

Likewise, the Second Circuit faced a similar issue in *Doe, Inc. v. Mukasey*, 549 F.3d 861 (2nd Cir. 2008). In *Mukasey*, the appeal challenged the constitutionality of statutes regulating the issuance by the FBI of a form of administrative subpoena commonly referred to as a National Security Letter ("NSL") to electronic communication providers seeking phone and internet activity. In determining that the challenged statutes violated First Amendment rights, the Second

---

[9] *See, e.g.*, Office of the Inspector General, U.S. Department of Justice, "*A Review of the FBI's Impersonation of a Journalist in a Criminal Investigation*", Oversight & Review Division 16-07, September, 2016. Version from internet at https://oig.justice.gov/reports/2016/o1607.pdf.

Circuit first noted that the First Amendment principles relevant to the analysis were "well-established", such as existing law prohibiting prior restraint (*Alexander v. United States*, 509 U.S. 550 (1993)); and prohibiting impermissible censorship (*Freedman v. Maryland*, 380 U.S. 51 (1965)). In addressing the "secrecy" aspect of the statutes that permitted secret warrant-type requests, the Second Circuit noted that the concern was that the Petitioner's First Amendment rights were being restrained from publicly expressing a category of information that was relevant to intended criticism of a governmental entity. *Id* at 878. More importantly, however, "there was no question that speech critical of the exercise of the State's power lies at the very center of the First Amendment", *Id*., citing *Gentile v. State Bar of Nevada*, 501 U.S. 1030, 1034 (1991), and that "there is practically universal agreement that a major purpose of that Amendment (First Amendment) was to protect the free discussion of governmental affairs." *Landmark Communications, Inc. v. Virginia*, 435 U.S. 829, 838 (1978).

In summary, although the government is permitted to make any argument it desires, the compelling history of First Amendment jurisprudence, when combined with common sense, proves beyond question that a reasonable government official would have clearly known that illegal surveillance of a member of the media designed to chill free press and cut-off sources of embarrassing reporting was illegal as a matter of law.

B. THE FOURTH AMENDMENT CLAIM: COUNT 8

As to the Fourth Amendment claim, Defendants Holder and Donahoe argue for qualified immunity claiming that (a) the complaint merely alleges what amounts to vicarious liability or *respondeat superior* thus making the claim invalid, and (b) Plaintiffs fail to allege any facts suggesting that Holder and Donahoe were personally involved in the alleged illegal surveillance and cyber-attack. Dkt. No. 72-01 at p. 58.

As set forth above, the *respondeat superior* argument mischaracterizes the Complaint, ignores applicable law under *Bivens*, and ignores facts. Likewise, the second argument – that the Complaint fails to allege facts sufficient to suggest that Defendants Holder and Donahoe were personally involved – is simply a mischaracterization of the Complaint and the very clearly plead allegations.

CONCLUSION

Sharyl Attkisson and her family suffered real and concrete harm when the federal government illegally violated their Constitutional rights by conducting illegal surveillance and cyber-attacks on the electronic life both at work and at home. Like the Doe defendants, Defendants Holder and Donahoe know they are "too big to jail," that their criminal conduct will not result in prosecution, and that at most, they will face giving sworn testimony in front of a jury and be forced to either tell the truth or continue the charade that has now existed for almost six (6) years. The Constitution was created for a reason: to empower Americans like the Attkisson family to be free from illegal, warrantless invasions into their personal life and careers by the very government charged with responsibility for enforcing those rights." The Complaint adequately pleads a sound legal basis for permitting Plaintiffs their day in court.

For all of the foregoing reasons, the Court should deny Defendant's amended motion to dismiss.

Respectfully Submitted,

SHARYL THOMPSON ATTKISSON
JAMES HOWARD ATTKISSON
SARAH JUDITH STARR ATTKISSON

By Counsel

/s/ David W. Thomas
David W. Thomas, Esq. (DC Bar No. 976513)
J. Gregory Webb, Esq. (admitted *pro hac vice*)
E. Kyle McNew, Esq. (admitted *pro hac vice*)
MichieHamlett PLLC
500 Court Square, Suite 300
Post Office Box 298
Charlottesville, VA 22902-0298
(434) 951-7200; (434) 951-7218 (Facsimile)
dthomas@michiehamlett.com
gwebb@michiehamlett.com
kmcnew@michiehamlett.com

C. Tab Turner, Esq. (admitted *pro hac vice*)
TURNER & ASSOCIATES, P.A.
4705 Somers Avenue, Suite 100
North Little Rock, AR 72116
(501) 791-2277
tab@tturner.com

CERTIFICATE OF SERVICE

I hereby certify that on October 7, 2016, I electronically filed the foregoing with the Clerk of the Court using the CM/ECF system, which will send notification of such filing to the following:

John C. Truong
Ronald C. Machen, Jr.
Daniel F. Van Horn
United States Attorney's Office
555 Fourth St., N.W.
Washington, DC 20530
E-mail: John.Truong@usdoj.gov

/s/ David W. Thomas
David W. Thomas, Esq. (DC Bar No. 976513)
J. Gregory Webb, Esq. (admitted *pro hac vice*)
E. Kyle McNew, Esq. (admitted *pro hac vice*)
MichieHamlett PLLC
500 Court Square, Suite 300
Post Office Box 298
Charlottesville, VA 22902-0298
(434) 951-7200; (434) 951-7218 (Facsimile)
dthomas@michiehamlett.com