UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND
Baltimore Division

SHARYL THOMPSON ATTKISSON, JAMES HOWARD ATTKISSON, SARAH JUDITH STARR ATTKISSON, Plaintiffs, v. ROD ROSENSTEIN; SHAWN HENRY; SEAN WESLEY BRIDGES; ROBERT CLARKE RYAN WHITE and UNKNOWN NAMED AGENTS 1-50 OF THE DEPARTMENT OF JUSTICE, in their individual capacities, Defendants.	Civil Action No. _____

PLAINTIFFS' COMPLAINT

Plaintiffs, by and through undersigned counsel, submit the following Complaint, challenging, under the Fourth Amendment to the United States Constitution and the Electronic Communications Privacy Act (ECPA), 18 U.S.C. §§ 2511 & 2520, the Defendants' unauthorized and illegal surveillance of the Plaintiffs' laptop computers and telephones from 2011-2014. The constitutional claim is brought pursuant to *Bivens v. Six Unknown Named Agents of Federal*

Bureau of Narcotics, 403 U.S. 388 (1971), which permits federal government officials to be sued for unconstitutional searches and seizures in violation of the Fourth Amendment. Defendants are sued in their individual capacities.

JURISDICTION

1. The subject litigation arises under the Constitution and laws of the United States, and the Court has jurisdiction over the subject matter of this Complaint under 28 U.S.C. §§ 1331 & 1346(b).

2. The subject actions are timely filed in that they are subject to the same statute of limitations as claims brought under 42 U.S.C. § 1983, and include the statute of limitations of the state where the constitutional torts occurred. While the applicable limitations period is borrowed from State law, the accrual date of a § 1983 action is defined by federal law. *Walker v. Epps*, 550 F.3d 407, 414 (5th Cir. 2008) (citing *Wallace v. Kato*, 549 -3- Case 3:12-cv-02458-M-BN, 1997 U.S. 384, 388 (2007)). Under federal law, an action accrues when a plaintiff has a complete and present cause of action or, expressed slightly differently, when the plaintiff can file suit and obtain relief. See, *Bay Area Laundry & Dry Cleaning Pension Trust Fund v. Ferbar Corp. of Cal.*, 522 U.S. 192, 201 (1997).

3. The actions are also timely based on equitable tolling principles. Here, the limitation periods do not begin to accrue where it was impossible or unreasonable for Plaintiffs to have sufficient notice of the nature and cause of the injury, including the wrongdoers, because the misconduct was carried out secretly and the facts have been and were concealed with an intent to avoid disclosure. The conduct included conducting surveillance inappropriately,

illegally, and secretly; lying about it; concealing it; and refusing to disclose the truth, all of which amounts to fraud, stealth, and subterfuge. Here, the Plaintiffs first acquired the details regarding key individuals involved in the surveillance in August, 2019, from a person involved in the wrongdoing who has come forward to provide information. Prior to that time, the Government and its agents and representatives had denied that any such conduct had occurred, including denials in Court pleadings and argument. The discovery rule is a recognition that the Legislature never intended to close the courts to plaintiffs inculpably unaware of their nature of the injuries or wrongs committed.

4. Similarly, the surveillance conducted here was ongoing for a significant, but yet unknown period of time, and included a continuation of illegal activity carried out by Defendants in conducting the surveillance thus constituting a continuous tort. Similarly, the accrual date for limitations purposes was tolled as a result of fraudulent concealment, which included knowledge by the Government of the illegal conduct; intentional overt acts of deception designed to conceal the truth, including verbal and written misrepresentations denying the misconduct ever occurred; and an intentional and conscious effort to conceal the truth from the public and Plaintiffs.

5. All conditions precedent to filing this action have been met. On *December 26, 2014, Plaintiffs submitted an Administrative Tort Claim to the United States Departm*ent of Justice and the United States Postal Service as required by law. Plaintiffs' claim was deemed denied by virtue of Claimants/Plaintiffs receiving no response from the respective federal agencies within six months of filing, pursuant to 28 U.S.C. § 2675(a). Plaintiffs have therefore

exhausted all available administrative remedies, and satisfied all conditions precedent, to the filing of suit.

6. This Fourth Amendment claim was dismissed by the United States Court of Appeals for the Fourth Circuit in *Attkisson v. Holder et. al.*, 925 F.3d 606 (4th Cir. 2019), but the Court specifically ordered that this claim be dismissed *without prejudice* to refile, pursuant to Federal Rule of Civil Procedure 4(m), because certain unnamed defendants had never received service of process. *See* 925 F.3d at 628. This claim is therefore timely because the Plaintiffs were allowed additional time to file the claims because the conduct referenced of the named-defendants was not discovered until after the limitations period had ordinarily expired, and because the Government and the defendants fraudulently concealed the facts now known about who was involved in the illegal surveillance.

7. A *Bivens* action may be filed in a district court (1) where any defendant resides as long as all defendants are residents of the state in which the court is located; or (2) where a significant portion of the actions or omissions giving rise to the claim occurred. 28 U.S.C. § 1391(b)(1)-(2). If neither of these first two options is available, then the plaintiff may bring the claim in a district court that has personal jurisdiction over any defendant regarding the action. 28 U.S.C. § 1391(b)(3).

PARTIES

8. Plaintiffs incorporate and re-allege each and every allegation above as if fully set forth herein.

9. At all times relevant to the subject lawsuit, Plaintiff Sharyl Attkisson is, and was, a citizen and resident of Leesburg, Virginia, and an investigative reporter for CBS News. Plaintiff

was responsible for investigating, writing, publishing, and airing investigative news stories on a wide-variety of topics, including the federal gun-trafficking investigation that came to be known as *"Fast and Furious,"* and the controversial attack of the American diplomatic mission in Benghazi, Libya. At all times relevant hereto, Ms. Attkisson was a member of "the press" as described by the First Amendment to the Constitution of the United States. In the course of her investigative journalism, she experienced confrontational encounters with officials within the DOJ and White House who demanded disclosure of the identity of confidential sources who may have been leaking information. Federal agencies and the White House repeatedly withheld documents, at times invoking "national security" as justification. During the same time period, the DOJ implemented efforts to vastly expand its cyber security capabilities, efforts, and resources in the name of national security, including actively targeting journalists and news organizations as part of leak investigations. Ms. Attkisson discovered that her computers and telephone had been hacked or compromised remotely, and that an unauthorized party or parties had illegally infiltrated her electronics and placed software on her laptop computer, and that her confidential, professional, and personal information had been illegally accessed, compromised, and infiltrated.

10. At all times relevant to the subject lawsuit, Plaintiff James Howard Attkisson is and was a citizen and resident of Leesburg, Virginia, and was married to Sharyl Attkisson. Because much of the surveillance alleged in this complaint occurred at Ms. Attkisson's residence, Mr. Attkisson was subjected to surveillance as well, and his confidential, professional, and personal information was illegally accessed.

11. At all times relevant to the subject lawsuit, Plaintiff Sarah Judith Starr Attkisson was a citizen and resident of Leesburg, Virginia, and the daughter of James and Sharyl Attkisson. Because much of the surveillance alleged in this complaint occurred at Sarah Attkisson's residence, she was subjected to surveillance as well, and her confidential, professional, and personal information were illegally accessed.

12. Defendant Rod Rosenstein ("Rosenstein") is a citizen and resident of 5704 Tanglewood Drive, Bethesda, Maryland 20817. At all times relevant to the subject lawsuit, Rosenstein was United States Attorney for the District of Maryland and ordered the unlawful surveillance and hacking of the computer systems of the Plaintiffs. Rosenstein, as Government-official, agent or employee, violated the Constitution as shown herein through his own individual actions.

13. Defendant Shawn Henry ("Henry") is a citizen and resident of 1204 North Danville, Arlington, VA 22201.

14. Defendant Sean Wesley Bridges ("Bridges") is a citizen and resident of Virginia with his current address at the FCI Petersburg Medium, 1060 River Road, Hopewell, VA 23860.

15. Defendant Ryan White ("White") is a citizen and resident of 5211 Daybrook Circle, Apartment 431, Rosedale, MD 21237.

16. Defendant Robert Clarke ("Clarke") is a citizen and resident of the United States. His current home address is unknown.

17. At all times relevant to the subject lawsuit, Defendant Shaun Wesley Bridges, Shawn Henry, Robert Clarke, and Ryan White were agents and/or employees of the United States

Government working with Rosenstein and physically located in Maryland, and conducted the unlawful surveillance and hacking of the computer systems of the Plaintiffs. These defendants, as Government-officials, agents or employees, violated the Constitution as shown herein through their own individual actions.

18. Defendant Shaun Wesley Bridges served as a Special Agent with the U.S. Secret Service for approximately six years, operating out of the Baltimore Field Office. Between 2012 and 2014, he was assigned to the Baltimore Silk Road Task Force, a multi-agency group investigating illegal activity on the Silk Road, a covert online marketplace for illicit goods, including drugs. In 2015 and 2017, Bridges was convicted of corruption related to his government work, and is now serving a prison sentence.[1]

19. Defendant Robert Clarke was, like Bridges, a member of the Silk Road Task Force.

20. Defendant Shawn Henry was head of the Washington D.C. field office of the Federal Bureau of Investigation (FBI). He previously served as head of cybercrime at the FBI in the capacity of executive assistant director of the Criminal, Cyber, Response, and Services Branch under FBI Director Robert S. Mueller, III.[2] In 2012, Henry left the FBI and now is president of *CrowdStrike Services*, a company that seeks to mitigate targeted online attacks on corporate and government networks globally.[3]

21. Ryan White worked as an undercover informant for the Department of Justice and as a

---

[1] https://www.justice.gov/opa/pr/former-secret-service-agent-sentenced-scheme-related-silk-road-investigation

[2] https://archives.fbi.gov/archives/news/pressrel/press-releases/shawn-henry-named-assistant-director-in-charge-of-the-fbi2019s-washington-field-division

[3] https://www.crowdstrike.com/

contractor operating out of the Baltimore office under a group supervised by Rosenstein. In this capacity, White conducted work for the FBI, United States Secret Service, Drug Enforcement Administration and the Bureau of Alcohol Tobacco and Firearms, where he and others were ordered to illegally hack into computer systems, servers, emails and phones.

22. Plaintiffs are unaware of the true names and capacities, whether individual or otherwise, of the Unknown Federal Agents referenced in the caption and therefore sue the unnamed Defendants by fictitious names. Plaintiffs are informed and believe, and on that basis, allege, that these Defendants, and each of them, are in some manner responsible and liable for the acts and/or damages alleged inthe Complaint, and that these Defendants, including all Defendants, are and were employees or agents of the federal governmentwho acted under color of law, and that each subjected Plaintiffs to, or caused them to be subjected to, constitutional violations and damages from Defendants' tortious actions.

23. The Fourth Amendment protects the rights of American citizens and guarantees that citizens will be free of unreasonable searches and seizures. Defendants herein have expressly interfered with those rights.

24. The facts alleged herein, and those referenced from public sources, demonstrate a clear and present danger to our most fundamental protections as a result of an intelligence community employing surreptitious collection techniques, including highly sophisticated forms of electronic surveillance, to achieve overly broad intelligence targeting and collection objectives in violation of law.

25. During all times relevant to the subject Complaint, Ms. Attkisson was an investigative

reporter for CBS News. She served CBS for twenty (20) years. Her job required her to investigate and report on national news stories. In 2011, during the course of her reporting, Ms. Attkisson began investigating what later became known as the "Fast and Furious" gun-walking story involving federal agents from the Bureau of Alcohol, Tobacco, and Firearms (ATF) improperly permitting weapons to pass into the hands of the Mexican drug cartels.

26. Her first *Fast and Furious* report aired on CBS on February 22, 2011. The report quoted and relied upon numerous confidential sources, all of whom were critical of the *Fast and Furious* gun-walking strategy deployed by the respective federal agencies.

27. In February, 2011, the ATF, in an internal memorandum, instigated an orchestrated campaign against Ms. Attkisson's report, including efforts to discredit it, and outlined a strategy for the Agency to push "positive stories" in order to "preempt some negative reporting."[4]

28. In March 2011, Defendants Henry, Bridges, Clarke, and White—all of whom were government employees connected to a special multi-agency federal government task force based in Baltimore, Maryland—were ordered by defendant Rosenstein to conduct home computer surveillance on the Attkissons and other U.S. citizens. Defendants Henry, Bridges, Clarke, White and John Does ultimately were involved in the surveillance operation of the Attkissons.

---

[4] See http://www.cbsnews.com/8301-31727_162-20039251-10391695.html "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."

29. Despite the foregoing efforts, Ms. Attkisson continued to report *Fast and Furious* stories. When contacted for comment, DOJ officials persisted in their denial of the allegations and continued efforts to unveil Ms. Attkisson's confidential sources. ATF sources told Ms. Attkisson that the Agency was actively seeking to identify government insiders who were providing information or "leaking" to her and CBS.

30. In September, 2011, Ms. Attkisson reported on secret audio recordings that implicated the FBI in an alleged discrepancy in its accounting of evidence in the *Fast andFurious* related murder of Border Patrol Agent Brian Terry.

31. The referenced reporting by Ms. Attkisson was public reporting available both on television and online.

32. In an October 4, 2011, email exchange, Attorney General Eric Holder press aide Tracy Schmaler told White House deputy press secretary Eric Schultz of Schmaler's plan to contact one of Ms. Attkisson's editors and CBS's chief Washington correspondent in an attempt to silence Ms. Attkisson.

> "I'm also calling Sharryl's [sic] editor and reaching out to Scheiffer [sic]," Schmaler wrote. "She's out of control."
>
> In a subsequent email, the White House's Schultz stated he supported Schmaler's plan, writing: "Good. Her piece was really bad for AG [Holder]."[5]

33. Also in September 2011, Ms. Attkisson reported on the alleged involvement of an F.B.I. informant in the *Fast and Furious* matter.

---

[5] https://www.judicialwatch.org/documents/control/

34. In October 2011, Ms. Attkisson reported on the continuing controversy regarding the F.B.I.'s accounting of evidence in *Fast and Furious.*

35. In November 2011, Ms. Attkisson reported on evidence contradicting Attorney General Holder's sworn testimony wherein he claimed that he had only heard of *Fast and Furious* for the first time in the past couple of weeks.

36. In mid-to-late 2011, Ms. Attkisson, Mr. Attkisson, and Sarah Attkisson began to notice 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 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.

37. In December, 2011, Ms. Attkisson reported on the DOJ's formal retraction of a letter and a misrepresentation it had made to Congress in February, 2011, which had stated, incorrectly, there had been no "gun-walking."

38. In January 2012, Ms. Attkisson contacted Verizon about ongoing internet problems and intermittent connectivity because the residential internet service began constantly dropping off. She had not experienced similar problems previously. In response to the complaint, Verizon sent a new router, which was immediately installed. The new router failed to resolve the issues. In January 2012, Ms. Attkisson began a series of reports, spanning several

months, which were critical of the Executive Branch's green energy initiatives, including the *Solyndra* failure.

39. When the computer issues failed to resolve, Ms. Attkisson reached out to professionals for assistance, including Leslie M. Szwajkowski, a former member of law enforcement with experience in the Federal Bureau of Investigation (FBI) Electronic Surveillance Technology Section, FBI liaison for national and international law enforcement in implementing Communications Assistance for Law Enforcement Act (CALEA) wiretapping law, surveillance capabilities within federal agencies to monitor telephone, broadband internet, and VoIP traffic, including experience with Verizon, the largest carrier impacted as part of CALEA. In January, 2013, Ms. Attkisson turned her computer over to a professional (Leslie Szwajkowski) trained in the evaluation of computer spyware intrusion and who had access to information about government computer intrusion tools and capabilities. (*Exhibit* 01 – Declaration) On or about January 9, 2013, Mr. Szwajkowski reported to Ms. Attkisson that the computer forensic analysis was "positive" for spyware intrusion, but that the full analysis would take more time and resources.

40. By the end of January, 2013, Mr. Szwajkowski and his colleagues advised Ms. Attkisson that they were quite shocked at what was found; and that they felt the intrusion was government-related due to the tools used and the sophistication of the intrusion. In short, Ms. Attkisson was informed that the internal investigation and analysis of her computer yielded clear evidence that the computer was infiltrated by a sophisticated person or entity that used commercial, non-attributable spyware that was proprietary to only government agencies. The

particular intrusion entered the computer silently and was attached to an otherwise innocuous email that Ms. Attkisson likely received and opened sometime in February, 2012. The analysis likewise revealed that the intrusion was "redone" in July, 2012, through a BGAN satellite terminal. The intrusion was "refreshed" at a later time using Wi-Fi within a Ritz Carlton hotel. The uninvited programs were running constantly on the laptop, and included a keystroke program that monitored everything typed on the computer, visited online, and viewed on the screen. The intruder had full access to email, including Ms. Attkisson's CBS work account. The intruder was likewise able to access Ms. Attkisson's and her family's passwords to all of their financial accounts and other applications. I informed Ms. Attkisson that she should assume that her smart phones were also impacted. The analysis also revealed that the intruder accessed Ms. Attkisson's Skype account, stole the password, activated the audio, and made heavy use of both, presumably as a listening tool. According to the evidence, the intrusion stopped abruptly about the time that Ms. Attkisson noted that her computers stopped self-starting at night.

41. In February 2012, an unauthorized party or parties remotely installed sophisticated surveillance spyware on Ms. Attkisson's Toshiba laptop. The invasion was obviously unknown to Ms. Attkisson at the time, but revealed later by forensic computer analysis, including factual evidence demonstrating that Plaintiffs' computer systems were targets of unauthorized surveillance efforts, including prolonged ongoing surveillance of the family's iMac desktop computer. Artifacts remaining on the iMac showed the intrusions were occurring as early as June, 2011. The forensic analysis likewise revealed direct targeting of

Plaintiff's Blackberry mobile phone when connected to the iMac. Records reveal intruder(s) performed a file recovery process that transferred large numbers of records off the BlackBerry. Intruder(s) made changes to Plaintiffs' Virtual Private Network (VPN) computer settings to enable the built-in Ethernet connection, after years of not being used, reflecting further clear evidence of unauthorized surveillance activities. Ethernet systems allow the connection of a number of computer systems to form a local area network.

42. Forensics and recovered records reveal the intruders issued an "*smbclient*" command and used the iMac as a mounted network shared resource, providing further evidence of uninvited, remote surveillance designed to enable the contents on the iMac to be easily exposed as well as exfiltrated or secretly removed. The unauthorized intruder(s) maintained complete control of the Plaintiffs' systems. Intruder(s) accessed Plaintiffs' e-mails, personal files, Internet browsing, passwords, execution of programs, financial records and photographs. Information recovered directly from Plaintiffs' computer proved that remote communication with Plaintiffs' system was executed via multiple IP addresses owned, controlled, and operated by the United States Postal Service. The IP addresses were not associated with any web server or website used by the USPS, and forensic analysts' attempts to communicate with the IP addresses were rejected. Forensic evidence proves the IP addresses were remote, unauthorized intrusions and not random finds on the computer, nor the result of Plaintiffs visiting a website. Analysis demonstrated that unknown parties remotely initiated communications channels between the referenced post office IP addresses and Plaintiffs' computer systems. Thus, evidence shows that intruder(s) using the IP addresses, which are part of the federal

government, were secretly and without authority from Plaintiffs communicating directly with Plaintiffs' computer on an ongoing basis during the times in question. The investigation revealed that the presence of the USPS addresses on Plaintiffs' computer was not a mistake; not a random event; and it was not technically possible for these IP addresses to simply appear on the computer systems without activity by someone using them as part of a formal cyber-attack. Two IPv4 addresses were found to be owned by the USPS and used by the APT attacker(s) to support the illegal cyber-attacks carried out. The two USPS IPv4 addresses are 56.91.143.9 and 56.189.149.2. (*Exhibit* 02 – Declaration of Scantling)

43. Significantly, the Baltimore-based multi-agency task force where some of the surveillance of the Plaintiffs originated included representatives of the USPS, and the task force had used IP addresses assigned to the USPS on more than one occasion.

44. Plaintiffs' recent attempts to retrieve relevant records from the USPS failed when the USPS notified Plaintiffs it had failed to preserve the records. *See* Deposition of Cliff M. Biram, Jr., Oct. 17, 2017, at 60-64.

45. In February 2012, Ms. Attkisson contacted Verizon yet again to complain about continuing anomalies.

46. In March 2012, a Verizon representative visited Ms. Attkisson's home and replaced the router a second time. The representative also replaced the entire outside FiOS service box. Despite Verizon's efforts, however, the anomalies persisted.

47. In April-May 2012, the DOJ and FBI publicly announced a new effort to vastly expand cyber related efforts to address alleged "national security-related cyber issues." During the same

time frame, the DOJ secretly--and without notice--seized personal and phone records belonging to journalists from the Associated Press news agency in violation longstanding DOJ practice. The records seizure was not publicly known at the time, but was later revealed.[6]

48. In July 2012 the DOJ designated U.S. Attorneys' offices to act as "force multipliers" in its stepped-up cyber efforts in the name of national security.[7]

49. That same month, July 2012, intruders remotely "refreshed" the ongoing surveillance of Ms. Attkisson's Toshiba computer. Again, the access was unknown to Ms.Attkisson at the time, but was revealed later through computer forensic analysis.

50. In September 2012, Wikileaks published internal emails from a global intelligence company doing business with government agencies. The materials made reference to"Obama leak investigations" and the alleged "witch hunts of investigative journalists learning information from inside the beltway sources." The email states, "(T)here is a specific tasker from the [White House] to go after anyone printing materials negative to the Obama agenda (oh my.) Even the FBI is shocked."

51. On October 5, 2012, CBS aired Ms. Attkisson's first Benghazi story for CBS, which was critical of the Executive Branch's handling of the security requests at the U.S. compound in Benghazi, Libya, where Ambassador Christopher Stevens and three (3) other U.S. personnel were killed on September 11,2012.

---

6 http://blogs.justice.gov/main/archives/date/2012/11

7 http://www.wikileaks.org/gifiles/docs/1210665_obama-leak-investigations-internal-use-only-pls-do-not.html (last accessed on October 28, 2014).

52. On October 8 2012, CBS aired another Attkisson report on Benghazi that included an interview with whistleblower Col. Andrew Wood. During the weeks following the airing of Col. Wood's interview, Ms. Attkisson made personal contact with numerous confidential sources within the federal government (or who had links to intelligence agencies within the U.S. government). The confidential government sources reported to Ms. Attkisson 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.

53. During the same time period, October of 2012, the DOJ continued its stepped-up cyber efforts with its National Security Division providing specialized training at DOJ headquarters for the National Security Cyber Specialists (NSCS) network and the Criminal Division's Computer Crime and Intellectual Property Section (CCIPS).

54. In the latter part of October 2012, Ms. Attkisson, Mr. Attkisson, and Sarah Attkisson began noticing an escalation of electronic problems at their personal residence, including interference in home and mobile phone lines, computer interference, and television interference. They were still unaware of any intrusion, however.

55. During the same general time frame, several sources with close ties to the intelligence community approached Ms. Attkisson privately and informed her that the government would likely be monitoring her electronically in an effort to identify her confidential sources, and also to monitor her continued *Fast and Furious* and *Benghazi* stories.

56. From November 7-9, 2012, Attorney General Holder hosted a national training conference at DOJ headquarters for the expanded efforts of DOJ's National Security Cyber Specialists

(NSCS).

57. 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.

58. In November 2012, Ms. Attkisson's phone line became nearly unusable because of anomalies and interruptions. Her mobile phones also experienced regular interruptions and interference, making telephone communications unreliable, and, at times, virtually impossible.

59. In December 2012, Ms. Attkisson discussed her phone and computer issues with friends, contacts, and sources, via her home phone, mobile phones, and email. She decided to begin logging the times and dates that the computers turned on at night without her input. Soon after these phone and email discussions, the computer nighttime activity stopped.

60. Computer forensic analysis later revealed that the intruders executed remote actions in December, 2012, to remove evidence of the intrusion from Ms. Attkisson's computers and home electronic equipment.

61. During this time frame, Defendants remotely removed evidence from Ms. Attkisson's computers.

62. In December 2012, a contact with U.S. government intelligence experience conducted an inspection of Ms. Attkisson's exterior home. During the course of the inspection, the consultant discovered an anomaly with Ms. Attkisson's FiOS (Verizon) box: an extra fiber optics line was dangling from the exterior of the box. Based on the odd finding, Ms. Attkisson contacted Verizon on December 31, 2012, which denied it had installed or had knowledge of the extraneous fiber optics line affixed to the equipment at the Attkisson's

home and suggested Attkisson contact law enforcement authorities. Shortly thereafter, a person identifying herself as a Verizon supervisor telephoned Ms. Attkisson to advise her that Verizon would be dispatching a technician to the house the following day. It would be New Year's Day, so Ms. Attkisson informed the purported supervisor that it was unnecessary to dispatch a technician just then, and she offered to send them a photograph of the stray fiber optics line to save Verizon the trip. The purported supervisor declined the photograph and insisted that a technician would be present on New Year's Day.

63. On January 1, 2013, a person represented to be a Verizon technician visited the Attkisson's home and removed the additional fiber optics cable from the system. Ms. Attkisson asked the technician toleave the cable. The technician placed it next to the equipment and left the home. When Ms. Attkisson's husband later arrived home and went to retrieve the extraneous cable for expert examination, the cable had already been removed and was no longer on the premises.

64. Throughout the month of January, 2012, Ms. Attkisson repeatedly contacted the purported Verizon technician to seek the location of the missing cable. The person representing himself as a technician never returned any of the calls at the number he had provided.

65. In January and February of 2013, Plaintiffs continued to experience phone and internet usage issues, including drop-offs, noises, and other interference. Verizon was notified and technicians and supervisors made additional contacts and visits.

66. On January 8, 2013, Ms. Attkisson made arrangements to deliver her Toshiba laptop to an individual with special expertise in computer forensics. On January 9, 2013, the forensics

expert reported to Ms. Attkisson that the Toshiba laptop showed clear evidence of outside and unauthorized "intrusion," and that the sources of the intrusions were state-supported, due to the sophisticated nature of the technology used.

67. On January 10, 2013, the computer was returned to Ms. Attkisson, along with a report. According to the report, the forensics computer expert found that sophisticated software had been used to accomplish the intrusions, and the software fingerprint indicated the software was proprietary to the federal government. The intrusions included, among other surveillance, keystroke monitoring, exfiltration of data, audio surveillance of Plaintiffs' conversations and activities at home by activating Skype, mining personal passwords, monitoring work and personal email, and probable compromise of Plaintiffs' work and personal smartphones. According to the report, this stage of surveillance conducted using the identified software spanned most of 2012 at least. The report also stated the intruders had accessed CBS network systems, such as the ENPS program, and that the perpetrator(s) had also placed three (3) classified documents deep in the computer's operating system. Ms. Attkisson thereafter notified her direct supervisor at CBS News of the laptop intrusion and findings.

68. On February 2, 2013, an independent forensic computer analyst retained by CBS News spent approximately six (6) hours at Ms. Attkisson's home, during which time he reported finding evidence on both Ms. Attkisson's Toshiba laptop and Apple desktop computers of a coordinated, highly-skilled series of actions and attacks directed at the operation of the computers and the storage and access of data thereon. CBS engaged the company to do further

analysis of the Toshiba laptop in an attempt to recover wiped data.

69. In March 2013, Ms. Attkisson's Apple desktop computer began malfunctioning and, after several days of it freezing and emitting a burning odor, it shut down. Ms. Attkisson was unable to turn the Apple computer back on after this event.

70. On April 3, 2013, Ms. Attkisson filed a complaint with the DOJ Inspector General.

71. On May 6, 2013, an official with the United States Department of Justice Inspector General's office called Ms. Attkisson and stated that he had checked with the FBI, and the FBI denied any knowledge of any operations concerning Ms. Attkisson's computers or phone lines. The official also stated that there was no PATRIOT Act related order authorizing surveillance of Ms. Attkisson.

72. On May 21, 2013, Ms. Attkisson publicly stated in a radio interview her belief that her computers had been compromised, but did not assign or allege responsibility. A news outlet sought a statement from the DOJ regarding Ms. Attkisson's assertions. The DOJ issued a written response stating, "To our knowledge, the Justice Department has never compromised Ms. Attkisson's computers, or otherwise sought any information from or concerning any telephone, computer or other media device she may own or use."

73. On June 10, 2013, the independent cyber security firm hired by CBS confirmed that there was a highly sophisticated intrusion into Ms. Attkisson's Toshiba work computer, as well as remote intrusions in December, 2012, to try to delete all evidence of the intrusion(s).

74. On June 11, 2013, CBS News issued a public statement, based on the forensics report, confirming that Ms. Attkisson's computer was accessed by an unauthorized, external,

unknown party on multiple occasions in late 2012, and that the party used sophisticated methods to attempt to remove all possible indications of unauthorized activity.

75. The DOJ Inspector General requested a copy of the CBS forensic expert's report and requested the opportunity to examine the CBS Toshiba computer. CBS denied the requests. Ms. Attkisson then retained an independent computer forensics expert to conduct further analysis of the Toshiba computer, as well as her personal iMac.

76. In September, 2013, while Ms. Attkisson continued working on the *Benghazi* story at her home in the evening, she observed for the first time that a third computer, her personal MacBook Air, was accessed remotely and briefly controlled while she was using it to work on a story related to the Benghazi case.

77. In June of 2013, though Plaintiffs were unaware at the time, the FBI had begun conducting inquiries of Ms. Attkisson's computer intrusions, listing her as the "victim," 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.[8]

78. The FBI investigation involving Ms. Attkisson's computer intrusions was circulated to the DOJ's national cyber security group and was 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.

---

[8] Ms. Attkisson was unaware of the F.B.I. case at the time it was opened and for months thereafter.

79. Although CBS did not release the compromised CBS computer to the DOJ Inspector General, in January, 2014, Ms. Attkisson asked the Inspector General to examine her personal Apple desktop computer.

80. On January 16, 2014, and January 27, 2014, the head of the DOJ Inspector General Computer Forensics unit and a colleague visited Ms. Attkisson's home as part of the investigation, which included analysis of the family's Apple desktop but not the primary computer involved: the CBS Toshiba laptop.

81. During the investigation, the DOJ Inspector General investigators remarked to Ms. Attkisson that they saw a great deal of suspicious activity on the Apple computer. However, as months went by, the investigators told Ms. Attkisson that the scope of their investigation had been narrowed by an unnamed party. The investigators also indicated the DOJ Inspector General Counsel's office had entered the picture and would decide whether Ms. Attkisson could see the report or any information about her computer.

82. The DOJ Inspector General ultimately refused to release the final written report to Ms. Attkisson. The DOJ Inspector General also failed to properly respond to Ms. Attkisson's subsequent Freedom of Information Act requests on the topic. The DOJ Inspector General finally released only a summary upon Congressional request on the eve of Ms. Attkisson's testimony to a Senate panel in early 2015.

83. Although the DOJ Inspector General summary noted a great deal of advanced mode computer activity not attributable to Ms. Attkisson or anybody in her household, the report nonetheless concluded, paradoxically, that it found no evidence of intrusion into her personal Apple

computer. Government officials then provided the summary to the press and falsely implied that government examiners had ruled out intrusions into Plaintiff's computers. The DOJ Inspector General did not examine the compromised CBS laptop computer or any other devices and did not include them in its report.

84. Among other findings, Ms. Attkisson's computer forensics expert has identified multiple unauthorized communications channels opened into her Toshiba laptop directly connected to Internet Provider (IP) addresses belonging to a federal government agency, specifically the United States Postal Service, indicating unauthorized surveillance whose source is the federal government.

85. The analysis shows the connection to a federal government agency was in use prior to January 8, 2013. The USPS has been publicly reported, including in IG internal audits, to have a working relationship with the FBI, Department of Homeland Security, and DOJ for domestic surveillance projects. In addition, the Rosenstein-led multi-agency task force in Baltimore that conducted surveillance of the Attkissons' computer systems used USPS IP addresses on other occasions to conduct operations.

86. Ms. Attkisson's analysts also found that although the government source who first analyzed her CBS Toshiba laptop in January, 2013, wiped evidence, he or she likely copied and retained the evidence on an external hard drive.

87. Ms. Attkisson's analysts also found that direct evidence pointing to attribution for Ms. Attkisson's computer intrusions may also reside on the CBS network computer systems.

88. Ms. Attkisson recently sought to retrieve additional forensic information from the Baltimore-

based cybersecurity firm that CBS originally hired to conduct forensics on Ms. Attkisson's CBS computers. CBS had provided written assurances that it would preserve all such material. However, CyberPoint informed Ms. Attkisson that it has destroyed the material.

89. The above-cited events, which offer only brief highlights of the cyber-attacks suffered in Plaintiffs' home, caused Plaintiffs to incur unreasonable and unnecessary expenses in an effort to diagnose and correct the problems resulting from the attacks and intrusions; resulted in an invasion of their personal and family privacy; caused them to fear for their individual and family's well-being and safety; interfered with their ability to use their telephones, computer, and television; caused them fear for her sources' well-being and safety; interfered with Plaintiffs' ability to maintain necessary contacts with sources to perform her professional investigative reporting duties as a member of the press; affected Plaintiffs' sources' willingness to communicate with her; distracted from her duties as an investigative reporter; and resulted in irreparable tension in her relationship with her employer.

90. The actions of Defendants as described above, including the government intrusions, negligently, recklessly, and intentionally caused Plaintiffs' rights to privacy to be violated, and trespassed upon Plaintiffs' real and personal property as alleged herein, without probable cause or any other legal justification, and as a result, Plaintiffs suffered damages.

91. The surveillance of Plaintiffs' computers and telephones violated the Plaintiffs' right to privacy and trespassed upon their real and personal property. The violation of Plaintiffs' right to privacy, and Constitutional rights, and the trespass upon Plaintiffs' real and person property proximately caused injuries, as set forth herein.

92. At all times relevant to the subject Complaint, the Defendants acted with reckless and callous indifference to the rights of Plaintiffs with the intent to subject them to, or cause them to be subjected to, constitutional violations under the Fourth Amendment of the United States Constitution.

93. It is worth noting that during the time period of the events alleged in this Complaint, former NSA representatives who previously left in protest of the mass privacy violations alleged to be occurring within the agency, came forward and spoke publicly confirming that Government personnel were targeting journalists using surveillance techniques unique to the Government, confirming that the DOJ and the agencies operating under it were targeting journalists as part of the paranoia surrounding alleged leakers using unique and state-sponsored technology.

94. Although the Director of National Intelligence, James Clapper, testified before the Senate Intelligence Committee in March, 2013, denying the existence of illegal surveillance and data collection of millions of Americans, whistleblower Edward Snowden's revelations in June, 2013, proved Clapper's testimony was false. Facing accusations of perjury from members of Congress, Mr. Clapper sent a letter to the committee chairwoman, Sen. Dianne Feinstein, in July, 2013, apologizing for his "clearly erroneous" remarks made under oath about the secret surveillance and data collection projects being undertaken.

95. Yet more former Government employees continued to come forward providing further support for the existence of such "black ops" programs targeting citizens like Plaintiffs. For instance, Russell Tice, who spent nearly 20 years working in various government agencies,

including the Office of Naval Intelligence, Defense Intelligence Agency, and NSA, publicly stepped forward with alleged firsthand knowledge of the targeting of journalists for surveillance. Speaking on television in 2009, Mr. Tice confirmed that while serving as an analyst at the NSA, he personally witnessed an agency program that gathered information on U.S. news organizations and journalists.

96. In addition to the foregoing, and with regard to technological capabilities of the DOJ, NSA, White House, CIA and other government agencies to conduct remote access surveillance of computer systems, in August, 2013, the German magazine *Der Spiegel* reported that it reviewed NSA documents, which had been provided by Mr. Snowden, that provided clear evidence that the agency hacked into a "specially protected" internal communication system at the Qatar-based broadcaster Al-Jazeera, in almost an identical manner as with Plaintiffs intrusion. According to *Der Spiegel*, the NSA documents listed the operation as "a notable success."

97. One of the most striking recent revelations about the DOJ's pursuit of the media was the disclosure that the DOJ had, during relevant time frames, obtained e-mails from the Google account of James Rosen of Fox News, in which he corresponded with a State Department analyst suspected of leaking classified information about North Korea. Investigators routinely search the e-mails of suspected leakers, but Congress has specifically forbidden the searching of journalists' work product materials unless the reporter was alleged to have committed a crime and without due process of law.

98. In December of 2019, the Department of Justice Inspector General found that three teams of

handpicked FBI officials had committed egregious errors and misconduct concerning surveillance of U.S. citizens. This included an FBI attorney doctoring documentation; and FBI officials failing to submit the required "Woods file" documentation to support factual claims justifying a secret wiretap; improperly withholding exculpatory information; and relying on material that they knew to be unreliable.[9]

99. Defendant Rosenstein was a Department of Justice official directly involved in the questioned surveillance activity.

COUNT 1
VIOLATION OF THE FOURT
AMENDMENT TO THE CONSTITUTION

100. Plaintiffs incorporate and re-allege each and every allegation above as if fully set forth herein.

101. This action arises under *Bivens.*

102. At all times relevant to the subject Complaint, Defendants acted under color of law when conducting surveillance of the Attkissons.

103. The surveillance of the Attkissons' computers and telephone violated the Fourth Amendment to the United States Constitution. The Plaintiffs' right to be secure in their person, residence, papers, and effects against unreasonable searches and seizures was violated. The Plaintiffs had a reasonable expectation of privacy with respect to their computers and telephones, and the Defendants had no warrant authorizing the surveillance, nor did any exigent circumstances exist at the time of such surveillance.

104. The violation of the Plaintiffs' Fourth Amendment rights proximately caused their injuries, as

[9] https://www.justice.gov/storage/120919-examination.pdf

set forth herein.

105. The Defendants' acted with reckless and callous indifference to the federally protected rights of the Plaintiffs.

106. By virtue of the foregoing, the Defendants are liable to Plaintiffs for their violation of the Plaintiffs' rights under the Fourth Amendment.

COUNT 2

VIOLATION OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 18. U.S.C. §§ 2511 & 2520

98. All prior allegations are restated herein by reference.

99. The Defendants, individually and in concert, intercepted or endeavored to intercept the Plaintiffs' wire, oral, or electronic communications.

100. The Defendants, individually and in concert, used, endeavored to use an electronic, mechanical, or other device to intercept Plaintiffs' oral communications. Such device or devices were affixed to or transmitted a signal through a wire used in wire communications, and was for the purpose of obtaining information relating to business which affects interstate commerce. A substantial part of such conduct occurred in the Eastern District of Virginia.

101. The Defendants, individually and in concert, disclosed or endeavored to disclose the contents of Plaintiffs' wire, oral or electronic communications, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communications.

102. Upon information and belief, the above alleged conduct occurred without authorization from a court of competent jurisdiction.

103. As a direct and proximate result of the aforesaid conduct, Plaintiffs have suffered damages as set forth herein.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs request judgment in their favor against Defendants, jointly and severally, for compensatory and punitive damages in an amount to be proven at trial; for an injunction prohibiting the Defendants, and all other agents of the federal government, from conducting surveillance of any sort against Ms. Attkisson without first obtaining a warrant in compliance with the law; for a Declaration that Defendants' actions, practices, customs, and policies regarding the unauthorized surveillance of the Plaintiffs were unjustified, illegal, and violated the constitutional and legal rights; for attorney's fees and costs; and for such other and further relief as the Court may deem just and appropriate.

TRIAL BY JURY IS DEMANDED.

Respectfully Submitted,

SHARYL THOMPSON ATTKISSON
JAMES HOWARD ATTKISSON
SARAH JUDITH STARR ATTKISSON
By counsel

David Muncy
PLAXEN & ADLER, P.A.
10211 Wincopin Circle, Suite 620
Columbia, MD 21044
Phone: 410-413-7528
Fax: 410-730-1615
dmuncy@plaxenadler.com

C. Tab Turner, Esq. (*Pro Hac Vice*)
TURNER & ASSOCIATES, P.A.
4705 Somers Avenue, Suite 100
North Little Rock, Arkansas 72116
501-791-2277 – Office
501-791-1251 – Facsimile
Tab@tturner.com

Paul Schiff Berman (*Pro Hac Vice*)
Attorney at Law
9 Hesketh St.
Chevy Chase, MD. 20815
202-569-6837 - Phone
pberman@law.gwu.edu

Counsel for Plaintiffs