BASIS OF CLAIM

This communication serves as notice of the basis of the claim brought against the Department of Justice by Sharyl Attkisson, James Attkisson, and Sarah Attkisson pursuant to the FEDERAL TORT CLAIMS ACT, 28 U.S.C. § 2675. Employees or agents of the Department of Justice conducted unauthorized and illegal surveillance of Ms. Attkisson's laptop computers and telephones from 2011-2013. By conducting said surveillance, the employees or agents of the Department of Justice violated the ELECTRONIC COMMUNICATIONS PRIVACY ACT, 18 U.S.C. §§ 2511 and 2520, the STORED COMMUNICATIONS ACT, 18. U.S.C. §§ 2701 and 2707, the COMPUTER FRAUD AND ABUSE ACT, 18 U.S.C. § 1030, the FOREIGN INTELLIGENCE SURVEILLANCE ACT, 50 U.S.C. § 1810, and the VIRGINIA COMPUTER CRIMES ACT, Virginia Code Ann. § 18.2-152.12.

Ms. Attkisson was an investigative reporter for CBS News for twenty (20) years. Her job required her to investigate and report on national news stories. In 2011, during the course of her reporting, she 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 Mexican drug cartels.

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 involved federal agencies.

In February, 2011, the ATF, in an internal memorandum, instigated an orchestrated campaign against Ms. Attkisson's report, including efforts to discredit her reporting, and outlined a strategy for the Agency to push "positive stories" in order to "preempt some negative reporting."[1]

---

[1] 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."

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 and target government insiders providing information or "leaking" to her and CBS.

In September, 2011, Ms. Attkisson reported on the existence of secret audio recordings implicating the F.B.I. in an alleged discrepancy in accounting of evidence in the *Fast and Furious* related murder of Border Patrol Agent Brian Terry. Also in September, 2011, Ms. Attkisson reported on evidence indicating that the DOJ communicated with White House Officials about *Fast and Furious* and on the alleged involvement of an F.B.I. informant in the *Fast and Furious* matter.

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

In mid-to-late 2011, Ms. Attkisson, James Attkisson, and Sarah Attkisson began to discuss 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.

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

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. Ms. Attkisson began a series of

reports, spanning several months, that were critical of some of the Executive Branch's green energy initiatives, including the Solyndra failure.

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. Ms. Attkisson contacted Verizon yet again to complain about continuing anomalies.

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.

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 of longstanding DOJ practice. The records seizure was not publicly known at the time, but was later revealed.

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.[2] That same month, intruders remotely "refreshed" the ongoing surveillance of Ms. Attkisson's Toshiba computer. Again, the access was unknown to Ms. Attkisson, but was revealed later through computer forensic analysis.

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."[3]

On October 5, 2012, CBS aired Ms. Attkisson's first Benghazi story for CBS, which was quite critical of the Executive Branch's handling of security requests at the

[2] http://blogs.justice.gov/main/archives/date/2012/11

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

U.S. compound in Benghazi, Libya, where Ambassador Christopher Stevens and three (3) other U.S. personnel were killed on September 11, 2012.

On October 8, 2012, CBS aired another Attkisson report on Benghazi that included an interview with whistleblower Col. Andrew Wood.[4] 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 individuals 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.

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).

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

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.

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).[5] On November 13, 2012, the F.B.I. initiated a body of cyber

---

[4] http://www.cbsnews.com/8301-18563_162-57528335/security-dwindled-before-deadly-libyan-consulate-attack/

[5] "With the network built, the [Justice] department will be able to accelerate some of the national security cyber work that has been ongoing since [National Security Division's] cyber review." "To equip this large cyber cadre in how to best address these new threats, the department has developed and carried out extensive training. Last week's inaugural NSCS conference covered topics ranging from digital evidence, to the Foreign Intelligence Surveillance Act, to current threat trends, to common challenges in combating national security cyber threats specifically. Underscoring the importance of this mission, Attorney General Eric Holder, FBI Director Robert Mueller, Assistant Attorney General Monaco, and others from the department and the FBI addressed the network throughout the three-day conference. .. the network will help strengthen partnerships between the department and agencies across the U.S. government,

security case investigations that would later relate to the illegal intrusions directed at Ms. Attkisson.

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.

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.

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

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 strange 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. Shortly thereafter, a person identifying herself as a Verizon supervisor telephoned Ms. Attkisson to advise her she was dispatching a technician to the house the next day. It would be New Year's Day, so Ms. Attkisson informed the purported supervisor that it was not necessary to dispatch a technician just then, and she offered to send them a photograph of the stray fiber optics line to

---

including the Department of Homeland Security, the Department of Defense, and various elements of the Intelligence Community. The network also will work particularly closely with the FBI's National Cyber Investigative Joint Task Force (NCIJTF) to help preserve all intelligence collection, prevention, disruption and response options for cyber national security threats. ..Going forward, the NSCS network is focused on ensuring a whole-of-government and all-tools approach to combating cyber threats to national security. The network will be working to bring investigations and prosecutions as viable options for deterrence and disruption as part of the government-wide response to these threats. The network will also be advising and consulting other parts of the government in the use of additional tools to counter these threats."
http://blogs.justice.gov/main/?s=NSCS%2C+specialized+training&search.x=25&search.y=16

save Verizon the trip. The purported supervisor declined the photograph and insisted that a technician would be present on New Year's Day.

On January 1, 2013, a Verizon technician visited the Attkisson's home and removed the additional fiber optics cable from the system. Ms. Attkisson asked the technician to leave the cable. The technician placed it next to the equipment and left the home. When Ms. Attkisson's husband arrived home and went to retrieve the extraneous cable, it was no longer located where the technician left it.

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 provided.

In January and February of 2013, Ms. Attkisson 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.

On January 8, 2013, Ms. Attkisson made arrangements to deliver her Toshiba laptop to a contact with connections to a forensics computer expert with experience in the intelligence community. 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 intrusion were state-supported due to the nature of the technology used.

On January 10, 2013, the computer was returned to Ms. Attkisson through an intermediary, along with a report. According to the report, the forensics computer expert found that so-called sophisticated software had been used to accomplish the intrusion, and the software fingerprint indicated the software was proprietary to the federal government. The intrusion included, among other surveillance, keystroke monitoring, exfiltration of data, audio surveillance of Ms. Attkisson's conversations and activities at home while conducting Skype interviews, mining personal passwords, monitoring work and personal email, and probable compromise of Ms. Attkisson's work and personal smart phones. According to the report, the surveillance by the identified software spanned most of 2012 at a minimum. The report also stated the intruders had accessed CBS network systems, such as the ENPS program, and that someone had also placed three (3) classified documents deep within the computer's

operating system. Ms. Attkisson thereafter notified her direct supervisor at CBS News of the laptop intrusion.

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.

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

On April 3, 2013, Ms. Attkisson filed a complaint with the DOJ Inspector General. On May 6, 2013, an official with the United States Inspector General's office called Ms. Attkisson and stated that he had checked with the FBI, and the FBI denied any knowledge of 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.

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."

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

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.

The DOJ Inspector General requested a copy of the CBS forensic expert's report along with the opportunity to examine the Toshiba computer. CBS denied the requests. Ms. Attkisson then retained an independent computer forensics expert to conduct further analysis of the Toshiba computer.

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 MacBookAir, was accessed remotely, controlled, and that data was deleted.

In June, 2013, the F.B.I. opened a case on Ms. Attkisson's computer intrusions under the auspices of a national security issue, but it failed to contact or interview her. (Ms. Attkisson was unaware of the F.B.I. case at the time it was opened and for months thereafter.)

The F.B.I. case involving Ms. Attkisson's computer intrusions was circulated to the DOJ's national cyber security group and included with a set of cases opened in November, 2012, during the DOJ's expansion of its cyber team and the announcement of its intention to use "new tools" in its arsenal.

In January, 2014, Ms. Attkisson agreed to release her personal Apple desktop computer to the DOJ Inspector General for analysis.

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 Apple desktop. As of this filing, they have not yet provided Ms. Attkisson formal findings or a report.

Among other findings, Ms. Attkisson's computer forensics expert has identified an unauthorized communications channel opened into her Toshiba laptop directly connected to an Internet Provider (IP) address belonging to a federal government agency, specifically the United States Postal Service, indicative of unauthorized surveillance.

The analysis shows the connection to a federal government agency was in use prior to January 8, 2013. The USPS is known to have a strong relationship with the FBI, Department of Homeland Security, and DOJ when conducting computer forensic actions.

Ms. Attkisson's analyst also found that while the government source who first analyzed the Toshiba laptop in January, 2013, wiped evidence, there are indications

that he or she likely copied and retained the evidence on an external hard drive.

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

The above-cited events, which offer only brief highlights of the cyber attacks suffered in Ms. Attkisson, James Attkisson, and Sarah Attkisson's home, caused the 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 and constitutional rights; 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 Ms. Attkisson fear for her sources' well-being and safety; interfered with her ability to maintain necessary contacts with sources to perform her professional investigative reporting duties as a member of the press; affected her 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.

The foregoing narrative constitutes the basis of Ms. Attkisson, James Attkisson, and Sarah Attkisson's claims against the Department of Justice and the employees/agents involved in the subject surveillance.