

DECLARATION OF
LESLIE M. SZWAJKOWSKI

COMMONWEALTH OF VIRGINIA *

*

COUNTY OF FAIRFAX *

UPON OATH, THE AFFIANT STATES AS FOLLOWS:

1.

My name is Leslie M. Szwajkowski. I am over the age of eighteen (18), of sound mind, and fully capable of providing this Declaration. The Declaration is based on my own personal knowledge, including the information I have collected and learned during the course of my career and the subject investigation.

2.

I am a citizen and resident of Clifton, Virginia. My educational experience includes a BS degree from Northwestern University; a JD degree from Washington University in St. Louis, MO; and educational experience at the Defense Language Institute.

3.

For the past thirty-four years, I have been involved in various aspects of government law enforcement, including serving as Unit Chief of the Federal Bureau of Investigation (FBI) Electronic Surveillance Technology Section. I held this position from 1999 until my retirement from the FBI in 2003. I also served as the FBI liaison for national and international law enforcement in implementing Communications Assistance for Law Enforcement Act (CALEA) wiretapping law. The purpose of this law, passed in 1994, is to enhance law enforcement agencies' ability to conduct electronic surveillance by requiring telecommunications carriers and equipment manufacturers to modify and design their equipment, facilities, and services to allow built-in surveillance capabilities enabling federal agencies to monitor all telephone, broadband internet, and VoIP traffic. I worked closely with Verizon communications, the largest carrier impacted, in implementation of CALEA. Additionally, I conducted special agent work with the FBI in criminal and national security matters; counterintelligence; legal advisor to FBI field office personnel; government contracts; the management of

classified interagency technical programs; provided consulting services to FBI finance divisions; and served as a consultant to the government in the area of government contracting.

4.

Around Thanksgiving, 2012, I was contacted by a colleague regarding Sharyl Attkisson. I was informed that Ms. Attkisson was an investigative news reporter with CBS News and that she had contacted him around Thanksgiving concerning strange phone line disruptions. The friend drove to Ms. Attkisson's residence and conversed with her about the various difficulties. Knowing of my government connections and areas of expertise, the colleague asked me if I had time to reach out to her. I spoke with Ms. Attkisson by telephone and agreed to meet her for the purpose of evaluating her computer. I first met Ms. Attkisson on or about January 8, 2013, where I took possession of her computer. I then delivered it to a confidential source trained in the evaluation of computer spyware intrusion and who has explicit access to information about government computer intrusion tools and capabilities.

5.

On or about January 9, 2013, I called Ms. Attkisson and advised her that the computer analysis was "positive" for spyware intrusion, but that the full analysis would take a bit more time. Given the nature of the intrusion, including the obvious and shocking evidence pointing to U.S. government involvement in the intrusion, I advised Ms. Attkisson about certain steps she needed to take to ensure privacy in further communications about the topic.

6.

Shortly thereafter, in January, 2013, I met Ms. Attkisson for the purpose of returning her computer and discussing the findings of the confidential analysis. I personally advised Ms. Attkisson at the time that I, and my associates involved, were quite shocked at what we found; and that we felt what was transpiring, and had transpired, was outrageous. I personally could not imagine that something like this could ever happen in the United States of America. I so-advised Ms. Attkisson.

7.

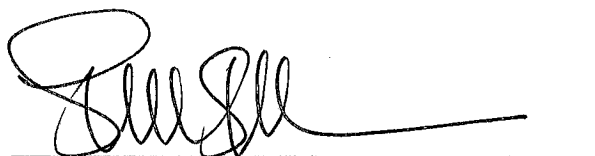
During the course of the conversation, I advised Ms. Attkisson that the internal investigation and analysis of her computer yielded clear evidence that the computer was infiltrated by a sophisticated person or entity that used commercial, non-

attributable spyware that was proprietary to only government agencies, including the CIA, FBI, or the National Security Agency (NSA). 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.

8.

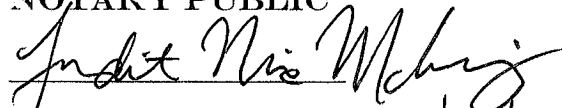
The analysis also revealed that the intruder accessed Ms. Attkisson's Skype account, stole the password, activated the audio, and made heavy use of both, presumably as a listening tool. According to the evidence, the intrusion stopped abruptly about the time that Ms. Attkisson noted that her computers stopped self-starting at night.

THE AFFIANT SAITH NOTHING FURTHER.



LESLIE M. SZWAJKOWSKI

NOTARY PUBLIC



My commission expires: 08/31/18

