

**IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF PENNSYLVANIA**

ELLIOTT J. SCHUCHARDT,
individually and doing business as the
Schuchardt Law Firm, on behalf of
himself and all others similarly situated,

CIVIL DIVISION

Case No. 2:14-cv-00705-CB

Plaintiffs,

v.

DONALD TRUMP, President of the
United States, et. al.,

Defendants.

**AFFIDAVIT OF WILLIAM E. BINNEY IN
OPPOSITION TO DEFENDANTS' RENEWED MOTION
TO DISMISS SECOND AMENDED COMPLAINT**

I, William Binney, declare:

1. I am a former employee of the National Security Agency. Unless otherwise indicated, I have personal knowledge of each and every fact set forth below and can competently testify thereto. A true and correct copy of my resume is attached hereto as Exhibit 1.

2. I have reviewed the complaint in the above-captioned civil lawsuit. It is my understanding, based on the complaint, that the Plaintiff, Elliott Schuchardt, contends that the Defendants are "unlawfully intercepting, accessing, monitoring and/or storing [his] private communications." (Complaint, ¶ 50).

3. It is my understanding, based on the complaint, that Mr. Schuchardt is a consumer of various types of electronic communication, storage, and internet-search services. These include "the e-mail services provided by Google and Yahoo; the internet search service provided by Google; the cloud storage services provided by Google and Dropbox; the e-mail and instant message services provided by Facebook; and the cell phone and text communication service provided by Verizon Communications." (Complaint, ¶ 49).

4. The allegations in the Complaint are true and correct: Defendants are intercepting, accessing, monitoring and storing the Plaintiff's private communications. I have knowledge of this information, based on the following facts.

Background

5. Between 1965 and 1969, I spent four years working in the U.S. Army Security Agency (the "ASA"). Until 1976, the ASA was the signals intelligence operation for the U.S. Army. Its mission was to intercept, acquire and decipher communications between persons, in electronic or any other form.

6. After the army, I spent 32 years working at the National Security Agency (the "NSA"). The NSA is the signals intelligence agency within the Department of Defense.

7. At the NSA, I held a variety of positions. These included the following positions:

- 2001 - Technical Leader, Intelligence
- 1999-2001 - Representative to the National Technology Alliance Executive Board
- 1996-2001 - Member of the Senior Technical Review Panel
- 1995-2001 - Co-founder/leader of the Automation Research Center (ARC)
- 2000-2001 - Technical Director of the Analytic Services Office
- 1998-2000 - Chair of the Technical Advisory Panel to the Foreign Relations Council
- 1998-2000 - Analysis Skill Field Leader, Operations
- 1997-2000 - Technical Director, World Geopolitical and Military
- 1996-1997 - Technical Director, Russia
- 1975-1996 - Leading analyst for warning, Russia
- 1970-1975 - Analyst on Russia

8. When I left the NSA in 2001, I was the Technical Leader for intelligence at the agency. As Technical Leader, I was the senior technical person in analysis at the NSA.

9. Prior to that, I was the Technical Director of the Analytical Services Office. In such position, I was responsible for handling all technical issues relating to the acquisition, development and distribution of signals intelligence for the agency's 6,000 analysts. These analysts were responsible for analysis and reporting for the entire world.

10. My duties included working with foreign governments who receive signals intelligence collected by the NSA. These include the so-called "Five Eyes" -- i.e. the intelligence agencies for Australia, Canada, New Zealand, and the United Kingdom, in addition to the United States.

Issues Relating to Surveillance of the Internet

11. At the NSA, I was the primary designer and developer of a number of programs designed to acquire and analyze very large amounts of information and data files. The final program I was addressing dealt with the acquisition of information from the internet.

12. The problem with the internet was the large amount of data. By 1998, the SIGINT Automation Research Center (known as the "SARC") had developed for the agency the ability to capture massive volumes of data from fiber optic cables.

13. I had to figure out how to handle all that data to avoid burying our analysts. From my experience with the former Soviet Union, it seemed clear to me that selecting information out of the internet by using known relationships was the smart way to go. My approach was to use social networks, as defined by metadata relationships (and some additional rules) to smartly select data from the tens of terabytes flowing by.

14. In other words, we focused on persons who had *known relationships* to people or websites deemed to be either radical or dangerous to United States national interests. This created a much smaller subset of data to acquire and analyze, but still did not completely solve the problem.

15. Human analysts still had to manually identify the groups and entities associated with activities that the NSA sought to monitor. That process was so laborious that it significantly hampered the NSA's ability to do large-scale data analysis.

16. One of my roles at the NSA was to find a means of automating the work of human analysts. As Technical Director, I supervised, helped design, and participated in the development of a program called "Thin Thread." Thin Thread was designed to identify networks of connections between individuals from their electronic communications over the internet in an automated fashion, in real time.

17. Devices running Thin Thread monitored international communications traffic passing over the internet. Where one side of an international communication was domestic, the NSA had to comply with the requirements of the Fourth Amendment and the Foreign Intelligence Surveillance Act ("FISA"). With Thin Thread, for United States nationals, no content would be captured, and metadata would be encrypted (to ensure the privacy of U.S. citizens) until a warrant could be obtained from the Foreign Intelligence Surveillance Court.

18. The attacks on September 11, 2001 completely changed how the NSA conducted surveillance. FISA ceased to be an operative concern, and the individual liberties preserved in the U.S. Constitution were no longer a consideration. In October 2001, the NSA began to implement a group of intelligence activities now known as the "President's Surveillance Program."

19. The President's Surveillance Program *involved the collection of the full content of domestic e-mail traffic* without any of the privacy protections built into Thin Thread. This was done under the authorization of Executive Order 12333. This meant that the nation's e-mail could be read by NSA staff members without the approval of any court or judge.

20. The President's Surveillance Program became public in 2005, when the New York Times published an article about the program. The government initially accused me and my colleague, Kirk Wiebe, of leaking the program to the New York Times. However, neither Kirk nor I was responsible for the leak, and we were formally cleared of the allegation in 2010.¹

The NSA still collects full content of e-mail without a warrant.

21. The NSA is still collecting the full content of U.S. domestic e-mail, without a warrant. We know this because of the highly-detailed information contained in the documents leaked by former NSA-contractor, Edward Snowden. I have personally reviewed many of these documents.

22. I can authenticate these documents because they relate to programs that I created and supervised during my years at the NSA.

23. Defendants have also admitted the authenticity of these documents.

24. In 2013, James Clapper, the former Director of National Intelligence, issued an order directing all present and former employees of the intelligence community to not publicly discuss the documents released by Mr. Snowden.

25. On or about January 29, 2014, Clapper -- speaking again in his capacity as Director of National Intelligence -- testified before a public session of the U.S. Senate Intelligence Committee. During the hearing, he called on Snowden to "return" the documents Snowden took from Defendants.

¹ The information was actually leaked by Thomas Tamm. Tamm was formerly an attorney in the U.S. Department of Justice Office of Intelligence Policy and Review. In that position, he learned that the government was using information from illegally-collected e-mail to apply for warrants to the Foreign Intelligence Surveillance Court. The FBI gave Kirk Wiebe and me Letters of Immunity in February 2010 in return for testimony about the activities of Thomas Drake.

26. On September 15, 2016, the U.S. House of Representative issued a formerly classified report admitting that Snowden had released approximately 1.5 million classified documents.

27. It is my understanding that the government has admitted these facts many other times as well.

28. There is therefore no doubt that the documents released by Snowden are authentic.

29. Mr. Snowden provided copies of his documents to two journalists, Laura Poitras and Glenn Greenwald. Poitras and Greenwald then released the documents to the Guardian, the Washington Post, and the Intercept, as well as various other publications. I obtained the documents that I reviewed, for purposes of this affidavit, from such publications. I also obtained some documents from German sources, who obtained the documents from Poitras while she was in Germany.

30. The documents that I obtained include the exhibits attached to this Affidavit, as well as Exhibits B, D, E, F, G, H and I attached to Mr. Schuchardt's First Amended Complaint, filed in this case. However, the documents that I reviewed are not limited to such documents.

31. The documents provided by Mr. Snowden are the type of data that experts in the intelligence community would typically and reasonably rely upon to form an opinion as to the conduct of the intelligence community.

The allegations in the Plaintiff's complaint are true and correct.

32. On the basis of the documents that I have reviewed, I can advise the Court that the allegations in the Plaintiff's complaint are true and correct: Defendants are intercepting, accessing and storing Schuchardt's private communications, without a warrant. This is known as "collection" of data in the intelligence community.

33. The communications collected include the full content and associated metadata² of e-mail, text messages, and web queries performed by United States citizens.

34. These records are collected inside the United States, as well as at overseas locations. The data is then stored in data centers located at Fort Meade, Maryland; Bluffdale, Utah; and at other sites in the United States.

35. The Snowden documents make it clear how this collection is occurring. For example, consider Exhibit 2 to this Affidavit, labeled "Fairview at a Glance." Fairview is the NSA program responsible for the upstream³ collection of data from the AT&T telecommunications system. Exhibit 2 shows the locations where the NSA has tapped into the AT&T system to collect data from the system. As the slide indicates, the vast majority of the data collected is *domestic communications*. Conversations with foreigners are represented by the green dots, which mark international fiber optic cables coming in from offshore. The slide shows that the NSA is collecting both "content" and "metadata" as part of the Fairview program.

36. Next, consider Exhibit 3, labeled "US-983 Stormbrew." Exhibit 3 is a photograph of the tap points for the NSA's Stormbrew program. Stormbrew is the program responsible for the upstream collection of data from the Verizon telecommunications network. As indicated by the photo, collection from Verizon is also occurring within the United States.

² Metadata consists of information about other data. For e-mail, it would include information such as the name of the sender and recipient; the date and time it was sent; and the internet service provider used to send the message.

³ In computer networking, "upstream" refers to the direction in which data is transferred from the client (i.e. the person creating the data) to the centrally-located computer server. This process is commonly referred to as "uploading" data. The opposite is referred to as "downloading" data. In other words, the term "upstream" refers to the process of harvesting, or collecting, data.

37. Exhibit 4, labeled "Blarney Access," shows the tap points for the NSA's Blarney program. Blarney is the program responsible for the upstream collection of data from 30+ providers of internet service, domestic long distance service, and data centers.

38. Once the data is collected, the NSA breaks it down into various subcategories, which are made searchable through various query-programs. These categories are shown in Exhibit 5.

39. The broadest query program is called "XKeyscore." According to Exhibit 5, XKeyscore is a method for searching the "front end full take feeds" from the fiberoptic cables. "Full take" means that the NSA is taking everything off these lines, which means full content of e-mail and web queries. This would include Plaintiff Schuchardt's e-mail and web queries.

40. XKeyscore can be searched, or "tasked", by means of an e-mail address. Thus, when Mr. Snowden said that he could read the e-mail of a federal judge if he had that judge's e-mail address, he was not exaggerating.

41. The NSA breaks the data down further by conducting automated searches based on words it refers to as the "Dictionary." The dictionary consists of metadata, words or phrases which are of interest to the NSA at any given time. It may include the names of various parties-in-interest. It can also be as broad as various inflammatory concepts, such as "assassinate" or "bomb." As indicated on Exhibit 4, the results from the dictionary search (designated by the term "Pinwale") are still massive.

42. The Snowden documents also reveal something very interesting. Exhibit 5 is a document labeled "Treasuremap." Treasuremap is a program designed to identify the real-time location of "any device, anywhere, all the time." In other words, the NSA is creating a program that shows the real-time location of all cell phones, tablets and computers in the world, at any

time. To have a state-actor engaging in this sort of behavior, without any court supervision, is troubling.

Defendants lack legal authority for bulk collection.

43. In their public statements, the Defendants claim that collection of information is limited, and is being done pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA"). FBI Director James Comey recently described Section 702 of FISA as the "crown jewel" of the intelligence community.

44. Defendants, however, are not being candid with the Court. Collection is actually being done pursuant to Executive Order 12333(2)(3)(c), which -- to my knowledge -- has never been subject to judicial review. This order allows the intelligence community to collect "*incidentally* obtained information that *may indicate* involvement in activities that *may violate* federal, state, local or foreign laws." Any lawyer can appreciate the scope of this broad language.

45. Thus, there is no question that Defendants are intercepting, accessing and storing Plaintiff's private communications. The relevant question is whether bulk collection should continue in its existing form, or whether the system needs to be changed or supervised by the courts.

Bulk collection is unnecessary and constitutes a moral hazard to government employees.

46. The NSA's current theory of surveillance can be described as "the needle and the haystack" approach. Under this approach, the NSA deems it necessary to acquire and monitor all information in the universe of information on the internet. This includes full content of e-mail, text messages, web search queries, and documents stored online by cloud providers, such as

Dropbox. In order to find the proverbial "needle in the haystack," it is necessary to first collect the haystack.

47. There are multiple problems with this process.

48. First, as the Plaintiff, Elliott Schuchardt, has pointed out in his pleadings, bulk collection violates the 4th Amendment of the U.S. Constitution because Defendants are "intercepting, accessing and storing" the private communications of the entire society, without court supervision. This leads to moral hazards, because NSA analysts can spy on their lovers, or Wall Street executives to gain information valuable for insider trading. Politicians can also use the NSA database to spy on the political opposition.

49. These concerns are not theoretical; they are *already happening*. According to media reports, President Obama's former National Security Advisor, Susan Rice, requested e-mail and phone records on President Trump and various members of his political campaign *during and after the 2016 election*.

50. According to these reports, the National Security Council ("NSC") has computer logs showing when Rice requested and viewed such records. The requests were made from July 2016 through January 2017, and included President Trump and various members of his campaign staff. According to an internal NSC report, the accessed information contained "valuable political information on the Trump transition." Rice's requests into Trump-related conversations increased following the presidential election last November. None of the requests were reviewed by any independent court.⁴

⁴ President Trump is incensed by Rice's conduct, and the present system of bulk collection of private information. On April 5, 2017, Trump publicly described Rice's actions as a "crime," saying "I think the Susan Rice thing is a massive story. I think it's a massive, massive story. All over the world. It's a bigger story than you know." On April 12, 2017, Trump again characterized the Rice story as "such a big story; I'm sure it will continue forward, but what they did is horrible." See Maggie Haberman, Matthew Rosenberg and Glen Thrush, "Trump, Citing

51. Given human nature, it is foreseeable that this sort of illegal conduct will occur again, if the present system of bulk collection remains in place, and unsupervised by the courts.

52. We also know that certain NSA staffers have used their access to e-mail and phone calls to conduct surveillance on current and former significant others. The NSA has referred to this sort of action as "LOVEINT," a phrase taken from other internal-NSA terms of art, such as "SIGINT" for signals intelligence.

53. It would be far safer to require Google, Yahoo and other internet service providers to store communications *on their facilities* for a certain amount of time, and then allow government access to such communications by means of court warrants, as contemplated (and required) by the nation's founders in the Fourth Amendment.

Bulk collection interferes with the surveillance process.

54. However, there are other equally serious problems with bulk collection. The problem, from my point of view as a former Technical Director at the NSA, is that bulk collection acquires too much data. Bulk collection makes it impossible for the NSA to actually do its job.

55. For example, consider the Pinwale program, discussed above, in which the NSA searches the collected data based on certain pre-defined keywords, known as the "dictionary." The results from the dictionary search are known as the "daily pull."

56. Eighty percent of the NSA's resources go towards review of the daily pull. The problem is that the daily pull is enormous. It is simply not possible for one analyst to review all questionable communications made by millions of people generating e-mail, text messages, web

No Evidence, Suggests Susan Rice Committed Crime," N.Y. Times, Apr. 5, 2017; Aaron Rugar, Think Progress, Apr. 12, 2017, <https://thinkprogress.org/trump-susan-rice-lies-wiretapping-surveillance-817a89beb77a>.

search queries, and visits to websites. Every person making a joke about a gun, bomb or a terrorist incident theoretically gets reviewed by a live person. This is not possible. When I was at the NSA, each analyst was theoretically required to review 40,000 to 50,000 questionable records each day. The analyst gets overwhelmed, and the actual known targets -- from the metadata analysis -- get ignored.

57. This is clear from some of the internal NSA memos released by Edward Snowden and published by the Intercept. In these memos, NSA analysts say:

"NSA is gathering too much data. . . . It's making it impossible to focus."

"Analysis Paralysis."

"Data Is Not Intelligence."

"Overcome by Overload."

58. Bulk collection is making it difficult for the NSA to find the real threats. The net effect from the current approach is that people die first. The NSA has missed repeated terrorist incidents over the last few years, despite its mass monitoring efforts. The NSA *cannot identify* future terrorism because 99.9999% of what it collects and analyzes is *foreseeably irrelevant*. This is swamping the intelligence community, while creating the moral hazards and risks to the republic identified by Plaintiff Schuchardt.

59. After a terrorist incident occurs, only then do analysts and law enforcement go into their vast data, and focus on the perpetrators of the crime. *This is exactly the reverse of what they should be doing.* If the NSA wants to predict intentions and capabilities prior to the crime, then it must focus on *known* subversive relationships, giving decision-makers time to react and influence events.

60. There is a second reason why data mining bulk collected data is a waste of time and resources: the professional terrorists know that we are looking at their e-mail and telephonic communications. As a result, they use code words that are *not* in the dictionary, and will not come up in the daily pull.

61. For example, the terrorists who planned the September 11 attacks used code words to describe the targets of their planes. The word "town center" was used to describe the World Trade Center; "law" was used to describe the U.S. Capital Building, and "fine arts" was used to identify the White House.

62. Thus, collecting mass amounts of data and searching it to find the proverbial needle in a haystack doesn't work. It is fishing in the empty ocean, where the fish are scientifically and foreseeably not present.

There is a better method.

63. *The truth is that there has always been a safe, alternate path to take.* That's a focused, professional, disciplined selection of data off the fiber lines. This is doable using metadata recovered by what the intelligence community calls "graphing" (i.e. building social networks). (See DOD IG Report 05-INTEL-03).

64. Based on my thirty-two years of experience in the intelligence community, I can assure the Court that it is possible to identify, in advance, the vast majority of threats on the basis of either a deductive approach or an inductive approach to intelligence gathering. A deductive approach is done in the following manner:

- Build social networks based on relationships in metadata such as phone numbers, email addresses, credit cards, money transfers, travel arrangements, and the like.
- Isolate new members of these communities.

- Extend the zone of suspicion to two degrees/hops from known criminal or terrorist entities, but
- Exclude businesses and departments of governments to avoid including massive numbers of innocent individuals in the zone of suspicion

65. An inductive approach would be to monitor websites that advocate violence against the west, pedophile or other criminal activity.

66. Both of these approaches are known in the intelligence community as "smart selection." By doing "smart selection," the NSA would give privacy to everyone in the world, and provide a rich data environment for analysts to use, *and succeed* at the objective of intelligence – i.e. predicting intentions and capabilities of adversaries.

67. Government need not -- and should not -- be in the business of collecting the universe of data on the internet. If additional information beyond "smart selection" is necessary, then such information can be quickly and efficiently obtained from the third party communications providers, pursuant to a warrant.

The European Community is moving in the direction of smart selection.

68. I serve as a consultant to many foreign governments on the issues described in this affidavit. As such, I have testified before the German Parliament, the British House of Lords, and the EU Libe Committee on Civil Liberties on these issues. I also consult regularly with members of the European Union on intelligence issues.

69. On the basis of these conversations, it is my understanding that the European Union intends to adopt legislation requiring its intelligence community to get out of the business of bulk collection, and implement smart selection.

Other protections are necessary.

70. Finally, smart selection is not enough. Governments, courts and the public need to have an absolute means of verifying what intelligence agencies are doing. This should be done within government by having a cleared technical team responsible to the whole of government and the courts with the authority and clearances to go into any intelligence agency and look directly into databases and tools in use. This would insure that government as a whole could get to the bottom line truth of what the intelligence agencies were really doing.


71. I would also suggest that agencies be required to implement software that audits their analytic processes to insure compliance with law and to automatically detect and report any violations to the courts and others.

72. Finally, it is impossible to understate the importance of the Court's decision in this case. The intelligence communities in most of the world are using the American system of bulk collection, with all of its inefficiencies and moral hazards. If the United States were to get out of this business, and implement a system of smart selection, it would establish a healthy precedent that would have ramifications all over the planet.

73. I would be happy to discuss any and all of these issues with the Court.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Executed on July 04, 2017 at Severn, Maryland.


William E. Binney