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,

Plaintiffs,

v.

BARACK H. OBAMA, in his capacity as President of the United States; JAMES R. CLAPPER, in his official capacity as Director of National Intelligence; ADM. MICHAEL S. ROGERS, in his official capacity as Director of the National Security Agency and Chief of the Central Security Service; and JAMES B. COMEY, in his official capacity as Director of the Federal Bureau of Investigation,

Defendants.

CIVIL DIVISION

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

COMPLAINT – CLASS ACTION

CLAIM OF UNCONSTITUTIONALITY

JURY TRIAL DEMANDED

SECOND AMENDED COMPLAINT

The Plaintiff, Elliott J. Schuchardt, individually and doing business as the Schuchardt Law Firm, files this Amended Complaint against the above-captioned Defendants, on behalf of himself and all those similarly situated.

Parties

1. The Plaintiff, Elliott J. Schuchardt, is an attorney having an office located at United States Steel Building, Suite 660, 600 Grant Street, Pittsburgh, PA 15219.

2. Defendant Barack H. Obama is President of the United States. As such, he has ultimate authority over the actions of the United States federal government. President Obama maintains an address at The White House, 1600 Pennsylvania Avenue, Washington, DC 20500.

3. Defendant James R. Clapper is the Director of National Intelligence ("DNI"). As such, Clapper has ultimate authority over the activities of the intelligence community. Defendant Clapper maintains an address at James R. Clapper, Director of National Intelligence, Washington, DC 20511.

4. Defendant Admiral Michael R. Rogers is the Director of the National Security Agency ("NSA"). As such, Rogers has ultimate authority for supervising and implementing all operations and functions of the NSA, the agency responsible for conducting surveillance authorized by the challenged law. Admiral Rogers maintains an address at National Security Agency, 9800 Savage Road, Fort Meade, MD 20755.

5. Defendant James B. Comey is the Director of the FBI. As such, Comey is responsible for applications made to the Foreign Intelligence Surveillance Court under Section 215 of the Patriot Act. Defendant Comey maintains an address at FBI Headquarters, 935 Pennsylvania Avenue, N.W., Washington, DC 20535-0001.

Background

1. This lawsuit seeks an injunction against the Defendants' bulk collection of domestic e-mail and phone records, in violation of the 4th Amendment of the United States Constitution.

2. The facts of this case are fairly well established.

3. In approximately 1996, the general public started using e-mail on a widespread basis.

4. Shortly thereafter, the federal government's electronic surveillance agency -- the National Security Agency ("NSA") -- began intercepting and storing international e-mail.

5. Domestic e-mail, however, was off limits to the agency without a court order. This is because of the requirements of the Fourth Amendment of the United States constitution.

6. On October 4, 2001, former President George W. Bush authorized a surveillance program that involved the government's collection of *domestic* e-mail without a warrant.

7. Since that date, a steady stream of high-ranking government officials has come forward to warn the American people of the implications – and dangers -- of the government's conduct.

Binney allegations

8. One of the first critics was William E. Binney, a senior employee of the NSA. Over the course of his career – 31 years -- Binney came to be regarded as something as a legend at the NSA, having mentored the technical work of approximately 6,000 employees.

9. While at the NSA, Binney set up a computer program designed to "data-mine" foreign e-mail communications quickly and efficiently.

10. After September 11, 2001, Binney learned that the NSA was using a similar type of program to collect and analyze domestic e-mail, without a warrant.

11. Binney tried to warn persons in the United States government that this was occurring, and that it could be extremely dangerous.

12. In late 2001, he resigned from the NSA, because he refused to cooperate in the agency's actions.

Jewel v. NSA

13. In May 2006, Mark Klein, an AT&T technician with 22 years of experience, revealed that the NSA was copying e-mail communications on AT&T's network by means of a secret facility set up in San Francisco.

14. On September 18, 2008, Carolyn Jewel and five other persons filed a class action lawsuit against the NSA in the United States District Court for the Northern District of California. The case is currently pending in such court under case number 08-cv-04373-JSW (the "Jewel case").

15. The complaint contends that the NSA has set up a network of surveillance devices that allow the NSA to acquire "the content of a significant portion of the phone calls, e-mail, instant messages, text messages, web communications – both international and domestic – of virtually every American who uses the phone system or internet."[1]

16. The complaint further contends that the defendants in the case are analyzing this data by means of computers, in what is described as a "vast data-mining operation."[2]

17. The complaint seeks an order enjoining the Jewel defendants from continuing to access the Plaintiffs' e-mail and other communications without a court order.

18. Significantly, several former employees of the NSA have filed Affidavits in the case *in support of an injunction*.

19. On July 2, 2012, William Binney filed an Affidavit. Paragraph 5 of the Affidavit states the following:

---

[1] Jewel Complaint, ¶ 9, Jewel v. NSA, Docket No. 1.

[2] Jewel Complaint, ¶ 11, Jewel v. NSA, Docket No. 1.

> [In late 2001,] the NSA began to implement the . . . President's Surveillance Program ("PSP"). [M]embers of my . . . team were given the task of implementing various aspects of the PSP. They confided in me and told me that the PSP involved the collection of domestic electronic communications traffic without any of the privacy protections built into [the former program].
>
> I resigned from the NSA in late 2001. I could not stay after the NSA began purposefully violating the Constitution.[3]

20. Thomas Drake, a former employee of the NSA with 29 years of experience in the field, also filed an affidavit. Drake's affidavit states as follows:

> Various employees who were implementing . . . aspects of the PSP confided in me and told me that the PSP *involved the collection of domestic electronic communications traffic without any privacy protections or judicial oversight*.
>
> * * *
>
> [The NSA] has, or is in the process of obtaining, the capability to seize and store most electronic communications passing through its U.S. intercept centers. The wholesale collection of data allows the NSA to identify and analyze Entities or Communities of Interest later *in a static database.*
>
> * * *
>
> Given a central database, the question becomes how the NSA and other federal agencies (FBI, CIA, Homeland Security, etc.) use it. The data is searchable and available. *There is no effective technical oversight by Congress or the courts*. It is seductively enticing to ignore the law.[4]

21. Kirk Wiebe, a third former employee of the NSA, also filed a statement in the case. Paragraph 9 of Wiebe's affidavit states as follows:

> I agree with the analysis and conclusions set forth in Mr. Binney's declaration, particularly about the capabilities of the NARUS device.

---

[3] Binney Affidavit, ¶ 5, Jewel v. NSA, Docket No. 88 (emphasis added).

[4] Drake Affidavit, ¶¶ 7-9 Jewel v. NSA, Docket No. 87 (emphasis added).

> Like Mr. Binney, I have concluded that . . . the NSA has chosen to seize and save all electronic communications.[5]

22. On August 31, 2011, the United States Court of Appeals for the Ninth Circuit issued an opinion finding that the Jewel plaintiffs had standing to sue the NSA for an injunction. Jewel v. NSA, 673 F.3d 902 (9th Cir. 2011).

23. The case is currently pending before the U.S. District Court for the Northern District of California.

Snowden allegations

24. In June 2013, a new person came forward to warn of the danger of the Defendants' conduct. That citizen was Edward Snowden.

25. Snowden is a former system administrator for the Central Intelligence Agency ("CIA") and a counterintelligence trainer at the Defense Intelligence Agency ("DIA"). Snowden later worked for the consulting firm, Booz Allen Hamilton, inside an NSA center located in Hawaii.

26. In these positions, Snowden worked directly with the Chief Information Officer at the CIA to solve the agency's technology problems. He was therefore in a very senior position in the government.

27. While working for the Defendants, Snowden learned that the Defendants were intercepting, monitoring and storing the content of all or substantially all of the e-mail sent by American citizens by means of several large internet service providers. Snowden also learned that the Defendants were collecting information about all phone calls made in the United States.

[5] Wiebe Affidavit, ¶ 9, Jewel v. NSA, Docket No. 86 (emphasis added).

28. Virtually all of this collection activity was being done without a judicial warrant.

29. On March 13, 2013, Defendant James Clapper, the then-Director of National Intelligence, told a committee of the United States Senate that the NSA does "not wittingly" collect information on millions of Americans.

30. Clapper's statement was a knowing falsehood, designed to mislead the United States Congress.[6]

31. Snowden learned of Clapper's statement on the following day. He then decided to expose the Defendants' bulk collection of private communications.

32. Like William Binney, Snowden had previously tried to obtain reform from inside the United States government. However, he had been unable to do so. He therefore leaked documents revealing the Defendants' collection program to the *Guardian* and *Washington Post* newspapers.

33. On June 5, 2013, the *Guardian* published an article based on Snowden's documents. The article reported that the Defendants had obtained a secret court order from the Foreign Intelligence Surveillance Court (the "FISC") directing Verizon Business Network Services, Inc. ("Verizon") to provide to the Defendants all "call detail records" for calls made wholly within the United States.[7]

---

[6] Clapper's statement was also made under oath, a federal crime punishable by up to eight years in prison. 18 U.S.C. § 1001 (2014).

[7] See Ex. A to First Amended Complaint, Glenn Greenwald, "NSA Collecting Phone Records of Millions of Verizon Customers Daily," Guardian, June 5, 2013. A copy of the Verizon order is attached as Exhibit B to the First Amended Complaint. This complaint incorporates by reference all documents referred to herein that have been filed elsewhere in this case or in the Jewel case.

34. Shortly thereafter, the Defendants admitted that the FISC order was genuine, and declassified the program.[8] There is therefore no issue of fact concerning whether the Defendants are collecting call detail records.

35. The following day, on June 6, 2013, the *Guardian* published a second article based on Snowden's documents.[9] The article reported that the Defendants had obtained direct access to the servers of several large internet companies, including Yahoo, Google, Facebook, Twitter, Dropbox, and Apple. This program is known as "Prism."

36. The documents show that the Defendants are intercepting, accessing and storing (hereafter, "collecting") massive quantities of e-mail and other data created by United States citizens.

37. The information collected includes the *full content* of e-mail, videos, photos, stored data, voice over IP, file transfers, as well as a variety of other information.[10]

38. Such information is obtained "directly from the servers of these U.S. service providers: Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple."[11]

39. According to the documents, the Defendants began collecting information from Microsoft on September 11, 2007; from Yahoo on March 12, 2008; from Google on January 14, 2009; from Facebook on June 3, 2009; from YouTube on September 24,

---

[8] On December 16, 2013, Judge Richard J. Leon of the United States District Court for the District of Columbia found the Defendants' program unconstitutional, and issued a preliminary injunction against the program. See Klayman v. Obama, Case No. 1:13-cv-00851-RJL (D.C. Cir. 2013).

[9] See Exhibit C to First Amended Complaint, Glenn Greenwald, "NSA Prism Taps into User Data of Apple, Google and Others," Guardian, July 6, 2013.

[10] See Exhibit D to First Amended Complaint.

[11] Id.

2010; from Skype on February 6, 2011; from AOL on March 31, 2001; and from Apple in October 2012 (only days after the death of its founder, Steve Jobs).[12]

40. The above dates (and referenced document) are extremely important. They show that the Defendants are collecting all of the content in the various stated-categories. If the Defendants were not collecting *all content*, then the above beginning dates for collection of "stored communications" would not be relevant or important to the Defendants.

41. Other documents, provided by Snowden, confirm this understanding. For example, one of the slides provided by Snowden is labeled "New Collection Posture." It says: "Sniff It All, Know It All, Collect It All, Process It All."[13] Another document boasts that the Defendants are "one step closer to collecting it all."[14]

42. For example, the Defendants are literally storing every single document stored on Microsoft's Skydrive -- a cloud service. One document states as follows:

> Beginning on 7 March 2013, PRISM now collects Microsoft Skydrive data as part of PRISM's standard Stored Communications collection package. . . . This means that analysts will no longer have to make a special request to SSO for this -- a process step that many analysts may not have known about. This success is the result of the FBI working for many months with Microsoft to get this tasking and collection solution established. "Skydrive is a cloud service that allows users to store and access their files on a variety of devices."[15]

[12] See Exhibit E to First Amended Complaint.

[13] See Exhibit F to First Amended Complaint.

[14] See Exhibit G to First Amended Complaint.

[15] See Exhibit H to First Amended Complaint.

43. According to journalist Bob Woodward, the NSA has developed the ability "to capture all the data, store it, [and] make it instantly available to intelligence analysts and operators."[16]

44. The Defendants' collection efforts have become so massive that the Defendants are having difficulty processing all of the data. According to one document obtained from Snowden: "Collection is outpacing [the Defendants'] ability to ingest, process and store to the 'norms' to which [they] have become accustomed."[17]

45. Any doubt about the meaning of these documents is resolved by the public statements made by Edward Snowden, himself. During a video interview published by the *Guardian*, on June 10, 2013, Snowden stated:

> I, sitting at my desk, could wiretap anyone, from you or your accountant, to a federal judge or even the president, if I had a personal e-mail.[18]

46. One month later, on July 12, 2013, Snowden released a statement during a press conference. The first paragraph of the statement read as follows:

> Hello. My name is Edward Snowden. A little over a month ago, I had a family, a home in paradise, and I lived in great comfort. I also had the capability, without a warrant, to search for, seize, and read your communications. Anyone's communications at any time. That is the power to change people's fates. It's also a serious violation of the law, the 4th and 5th Amendments to the Constitution of my country.[19]

---

[16] Bob Woodward, Obama's Wars, at 7.

[17] See Exhibit I to First Amended Complaint.

[18] See Exhibit J to First Amended Complaint, Glenn Greenwald, "X-Keyscore: NSA Tool Collects Nearly Everything A User Does on the Internet," Guardian, July 31, 2013.

[19] See Exhibit K to First Amended Complaint, "Edward Snowden Statement: It was the Right Thing to \Do and I Have No Regrets," Guardian, July 13, 2013.

47. Following Snowden's disclosures, the Defendants claimed that they were only storing "metadata," and not the actual words of the citizenry's electronic communications. Snowden responded to this allegation in March 2014, when he appeared at a TED conference in Vancouver, Canada. During that appearance, Snowden said the following:

> The best way to understand PRISM . . . is to first talk about what PRISM *isn't*. Much of the debate in the U.S. has been about metadata. They've said it's just metadata, it's just metadata . . . . *PRISM is about content*.[20]

48. More recently, extended interviews with Snowden have appeared in Laura Poitras' film, *CitizenFour*. In the film, Snowden directly states that the Defendants are collecting the *full content* of Americans' e-mail, without a warrant.

49. Snowden has therefore confirmed the allegations of Binney, Drake and Wiebe in the Jewel case.

Levinson allegations

50. Following Snowden's disclosures, the Defendants contacted Snowden's e-mail service, Lavabit, and made an extraordinary demand.

51. The Defendants demanded that Lavabit install a device on its server which would have provided the Defendants with access to the full content of all e-mail messages for *all of Lavabit's 410,000 customers*.[21]

[20] Transcript of Snowden appearance, www.ted.com.

[21] See Exhibit L to First Amended Complaint, Statement of Ladar Levinson, Owner of Lavabit.

52. The Defendants also demanded that the company's owner, Ladar Levinson, provide to the government the private encryption keys for all of Lavabit's e-mail accounts.[22]

53. On August 8, 2013, Levinson voluntarily shut down Lavabit, because he could no longer provide a secure e-mail service to his customers.[23]

54. The following day, on August 9, 2013, another encrypted e-mail service -- Silent Circle -- voluntarily shut down operations. After doing so, Silent Circle destroyed its e-mail server so that its database of e-mail communications would not fall into the Defendants' hands.

55. Since August 9, 2013, there has been no secure e-mail service within the United States. The content of all e-mail sent or passing through the United States is monitored and/or stored by the Defendants without a warrant.

Defendants' Purported Authority

56. On January 17, 2014, the White House issued a "Presidential Policy Directive" admitting that the Defendants are collecting "signals intelligence" "in bulk."

57. The Directive made repeated reference to an obscure presidential order, Executive Order 12333, as partial grounds for the bulk collection of private data.

58. Executive Order 12333 authorizes bulk collection of data about United States citizens for a variety of very broad reasons. The order was originally issued in December 1981. The order was amended in 2004 and 2008, substantially expanding the

---

[22] See Exhibit L to First Amended Complaint. When Levinson challenged the Defendants' demands, the Defendants' argued that they were not bound by the Fourth Amendment because Lavabit's e-mail database would be inspected by "means of a machine." Id. This confirms that the Defendants are data-mining the nation's e-mail database.

[23] Id.

alleged powers granted by the order. The order has been subject to little or no judicial review.

59. On July 18, 2014, the *Washington Post* published an article written by John Napier Tye, a former employee of the United States State Department.

60. In such position, Tye attended two classified National Security Agency briefings on Executive Order 12333, in Fall 2013 and February 2014, so that he could help prepare the State Department's response to the leaks disclosed by Snowden.[24]

61. In the article, Tye stated that the Defendants were claiming the legal authority to collect the nation's entire e-mail database under Executive Order, No. 12333.[25] According to Tye:

> Once it [your data] transits outside of the US, or is stored on a server outside of the United States . . . it can be collected under 12333. There's nothing in the executive order that would prevent all of your communications from being collected. . . . When the NSA collects data in a foreign country, it is possible and even likely that they will collect American's data and communications… In theory almost every electronic communication that every American sends to another American within the United States can be collected by the NSA under this authority, outside of our borders, because of how the Internet is designed. . . .
>
> It's a very intrusive power. Even Congress and the courts don't know anything about 12333. None of the mechanisms that we have in place is performing an oversight role.[26]

[24] Cyrus Farivar, "Meet John Tye: the kinder, gentler, and by-the-book whistleblower," Ars Technica, Aug. 20, 2014.

[25] John Napier Tye, "Meet Executive Order 12333: The Reagan Rule That Allows the NSA to Spy on Americans," Washington Post, July 18, 2014.

[26] John Haltiwanger, "The U.S. Government Made It Legal to Look at All of Your Messages and This Whistleblower Has Proof," Elite Daily, Aug. 19, 2014. Tye, a Rhodes Scholar with a law decree from Yale University, maintains that the Defendants' bulk collection of domestic e-mail is a violation of the Fourth Amendment of the United States

62. According to a document that was recently declassified, Executive Order 12333 is the "primary source of NSA's foreign intelligence-gathering authority."[27]

63. Thus, it appears that the Defendants are doing the bulk of their collection under the purported authority of Executive Order 12333 – a federal rule that was never reviewed or enacted by Congress.

64. The Defendants, however, are not able to obtain everything under Executive Order 12333. To obtain certain information, such as encrypted e-mails, the Defendants need additional information -- from the persons providing such encryption.[28]

65. To obtain this latter information, the Defendants appear to be using Section 215 of the Patriot Act. 50 U.S.C. § 1861 (2014).

66. Section 215 authorizes the Defendants to request a subpoena, called a "National Security Letter," from the Foreign Intelligence Surveillance Court (the "FISC"). The entire proceeding is secret and done on an *ex parte* basis, without the knowledge of the proposed recipient of the letter. Id.

67. The Foreign Intelligence Surveillance Court ("FISC") is authorized to issue such a letter upon a finding that there are "reasonable grounds" to believe that the requested records are "relevant to an authorized investigation." 50 U.S.C. § 1861(b)(2)(A) (2014).

Constitution. John Napier Tye, "Meet Executive Order 12333: The Reagan Rule That Allows the NSA to Spy on Americans," Washington Post, July 18, 2014.

[27] "Overview of Signals Intelligence Authorities," available on ACLU website.

[28] While the Defendants can intercept encrypted e-mail, they cannot read them without the encryption codes. This is because even the fastest supercomputers cannot obtain encryption codes that exceed a certain number of digits. This is what created the market for Lavabit and Silent Circle.

68. Once a National Security Letter has been issued, the recipient of such letter is prohibited from disclosing the existence of the letter to any person other than his or her attorney, and persons authorized by the FBI. 50 U.S.C. § 1861(d)(1) (2014).[29]

69. In addition to the above two sections, the Defendants are purporting to act pursuant to Section 702 of the Foreign Intelligence Surveillance Act ("FISA"), codified at 50 U.S.C. § 1881a.

70. On June 8, 2013, Defendant James Clapper, the then-Director of National Intelligence, released a statement which admitted and declassified portions of the Prism program.

71. Clapper's statement implied that the Defendants' collection of information was being done solely under Section 702 of FISA.[30]

72. Clapper's statement was disingenuous, in that it implied that the Defendants' collection of information for the Prism database was far smaller than its actual scope, and that the Defendants were acting under a single, limited authority.

73. As stated above, the Defendants' collection program under Prism is far broader than the limited collection referred in Clapper's statement.

74. On June 19, 2014, the U.S. House of Representatives overwhelmingly approved a bill that would prevent the Defendants from conducting searches of the

[29] This provision of the law appears to be a patent violation of the First Amendment. Ladar Levinson, the owner of Lavabit, challenged this provision. After many months of litigation, a federal judge authorized him to tell his story publicly. It is only because of his litigation that we know that the Defendants were seizing *all* of the e-mail in the Lavabit server, *together* with the decryption pass codes.

[30] Section 702 allows the Attorney General and the Director of National Intelligence to obtain information relating to foreign intelligence investigations, subject to review by the FISC. The authority is far more limited than the above two authorities, Section 215 of the Patriot Act and Executive Order 12333.

nation's e-mail database without a warrant. The bill was adopted by a large majority of house members, 293 to 123.

75. The U.S. Senate has not acted on the bill as of this date.

Class Action Allegations

76. Pursuant to Rules 23(a) and 23(b) of the Federal Rules of Civil Procedure, the Plaintiff brings this action on behalf of himself and a nationwide class (the "Nationwide Class") of similarly situated persons defined as: American citizens who are subscribers, users, and/or consumers of the internet services of Google, Yahoo, and Facebook, the cloud storage services of Dropbox, and the telecommunication services of Verizon.

77. Excluded from the Nationwide Class are the Defendants, their legal representatives, heirs, successors, and assigns of Defendants, and all judges who may ever adjudicate this case.

78. This action is brought as a class action and may be so maintained pursuant to the provisions of Rule 23 of the Federal Rules of Civil Procedure. The Plaintiff reserves the right to modify the Nationwide Class.

79. Numerosity of the Nationwide Class: The National Class is so numerous that the individual joinder of all members, in this or any action is impracticable. The exact number or identification of Class members is presently unknown to the Plaintiff, but it is believed that the Class numbers over a hundred million citizens. The identity of Class members and their addresses maybe ascertained from the business records for Google, Yahoo, Facebook, Dropbox and Verizon. Class members may be informed of the pendency of this action by a combination of direct mail and/or public notice.

80. Commonality: There is a well-defined community of interest in the questions of law and fact involved affecting the members of the Class. These common legal and factual questions include:

a. Whether Defendants' surveillance and gathering of American citizens' telephonic, internet, and social media data violated the Plaintiff's and Class Members' constitutional rights, as guaranteed under the First and Fourth Amendments;

b. Whether the Plaintiff's and Class members are entitled to declaratory, injunctive and/or equitable relief; and

c. Whether the Plaintiff and Class Members are entitled to declaratory, injunctive and/or equitable relief.

81. Typicality: The Plaintiff's claims are typical of the claims of the members of the Class because the Plaintiff and the Class members are or were each a subscriber, consumer, or user of the internet services of Google, Yahoo, and Facebook, the cloud storage services of Dropbox, and the telecommunication services of Verizon. The Plaintiff and all members of the Class have similarly suffered harm arising from Defendants' violations of law, as alleged herein.

82. Adequacy: The Plaintiff is an adequate representative of the Class because his interests do not conflict with the interests of the members of the Class they seek to represent. The Plaintiff is not seeking any sort of attorneys fees in this case.[31] The Plaintiff intends to prosecute this action vigorously. The Plaintiff will fairly and adequately protect the interest of the members of the Class.

83. This suit may also be maintained as a class action pursuant to Rule 23(b)(2) of the Federal Rule of Civil Procedure 23(b)(2) because Plaintiffs and the Class seek declaratory and injunctive relief, and all of the above factors of numerosity, common

[31] If the Plaintiff retains counsel in this matter, then he will be seeking attorneys fees to compensate such counsel.

questions of fact and law, typicality and adequacy are present. Defendants have acted on grounds generally applicable to the Plaintiff and the Class as a whole, thereby making declaratory and/or injunctive relief proper.

84. Predominance and Superiority: This suit may also be maintained as a class action under Rule 23(b)(3) of the Federal Rule of Civil Procedure because questions of law and fact common to the Class predominate over the questions affecting only individual members of the Class and a class action is superior to other available means for the fair and efficient adjudication of this dispute. The damages suffered by each individual Class member, depending on the circumstances, may be relatively small or modest, especially given the burden and expense of individual prosecution of the complex and extensive litigation necessitated by Defendants' conduct. Furthermore, it would be virtually impossible for the Class members, on an individual basis, to obtain effective redress for the wrongs done to them. Moreover, even if Class members themselves could afford such individual litigation, the court system could not. Individual litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expenses to all parties and the court system presented by the complex legal issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of a single adjudication, economy of scale, and comprehensive supervision by a single court.

COUNT I

Declaratory and Injunctive Relief

Violation of the Fourth Amendment

Bulk Collection of E-mail

85. The Plaintiff incorporates by reference the allegations set forth in the preceding paragraphs as though fully set forth herein.

86. The Plaintiff, Elliott J. Schuchardt, is an American citizen and constitutional lawyer.

87. 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.

88. The Defendants are unlawfully intercepting, accessing, monitoring and/or storing the private communications of the Plaintiff, made or stored through such services.

89. This complaint will refer to the Defendants' above-described activities as the “collection” of private communications.

90. The Defendants’ collection of data includes both the content of the Plaintiff’s e-mail, as well as the “metadata” associated with such e-mail.

91. For purposes of this complaint, the content of an e-mail includes the actual text of the e-mail and any attachments to the e-mail, including photographs and documents.

92. Since March 12, 2006, the Defendants have been collecting both the content and the metadata of the Plaintiffs' private e-mail communications sent through the Yahoo e-mail system.

93. Since January 14, 2009, the Defendants have been collecting both the content and the metadata of the Plaintiffs' private e-mail communications sent through the Google "gmail" e-mail system.

94. Since January 14, 2009, the Defendants have been collecting the content and the metadata of the Plaintiffs' private internet search history through the Google search website.

95. Since June 3, 2009, the Defendants have been collecting the content of the Plaintiff's e-mail and instant messages through Facebook.

96. Upon information and belief, since approximately June 2013, the Defendants have been collecting the content and metadata of documents stored by the Plaintiff using the Dropbox cloud storage service.

97. The documents, images and communications collected by the Defendants contain information of a private and confidential nature. Such communications include bank account numbers; credit card numbers; passwords for financial data; health records; and trade secrets of a confidential and valuable nature.

98. The documents and communications collected by the Defendants also include communications with clients of Schuchardt's law firm, which are privileged and confidential under applicable law.

99. Upon information and belief, the Defendants are storing such information in a computer database, or through a government program, which the Defendants call "Prism."

100. Upon information and belief, the Defendants are collecting such information in order to "data mine" the nation's e-mail database. Data mining in the process of collecting, searching and analyzing large amounts of data for the purpose of finding patterns or relationships in such data.

101. The Defendants' conduct is unlawful under the United States Constitution, the civil and criminal laws of the federal government, and the civil and criminal laws of the Commonwealth of Pennsylvania.

102. It is impossible to understate the danger of the Defendants' conduct. The framers of the United States constitution were familiar with abusive governmental conduct. They therefore specifically stated that the United States government would not have the power to search and seize the private papers of United States citizens without obtaining a *warrant* from a neutral and detached magistrate, issued upon a finding of probable cause.

103. Now, for the first time in history, a small group of persons within the United States government is attempting to seize all of the private, electronic communications of the American citizenry, with little or no independent review.

104. The system set up by the Defendants – where the government has possession of all private communications and stored electronic documents – is unstable. The system is ripe for abuse and could lead to the destruction of the republic.

105. According to 28 U.S.C. § 2201, this Court has the power to adjudicate a dispute between the Plaintiff and the Defendants involving any issue involving federal law.

106. The Plaintiff is aggrieved by the above-described conduct of the Defendants.

107. The Defendants are subject to the law established by the United States Constitution.

108. According to the 4th Amendment of the United States Constitution:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

109. The Plaintiff has an expectation of privacy in the above-described private information and electronic communications being collected by the Defendants.

110. The Defendants have unlawfully collected such information in violation of the 4th Amendment, without obtaining a warrant and without probable cause.

111. As of this date, the Defendants have refused to provide any public explanation of the legal authority that purports to authorize their intrusion into the affairs of the Plaintiff.

112. The Plaintiff respectfully submits that any such purported authority, when ultimately disclosed by the Defendants, is unlawful as a violation of the 4th Amendment of the United States Constitution.

113. If the Defendants are purporting to act pursuant to secret orders established by the Foreign Intelligence Surveillance Court, the Plaintiff respectfully submits that any such authority is also unlawful as a violation of the due process clause of the 14th Amendment.

WHEREFORE, the Plaintiff respectfully requests that this Honorable Court enter an order (a) enjoining the Defendants from engaging in any further collection of the above-described information about the Plaintiff and the Nationwide Class, and (b)

establishing procedures to ensure that the Defendants refrain from unlawful conduct in the future.

COUNT II

Declaratory and Injunctive Relief

Violation of the Fourth Amendment

Bulk Collection of Verizon Metadata

114. The Plaintiff incorporates by reference the allegations set forth in the preceding paragraphs as though fully set forth herein.

115. Since approximately 2008, the Defendants have been collecting the metadata associated with the Plaintiff's cell phone communications through Verizon Communications.

116. Such metadata includes information about the persons that Schuchardt calls, the duration of such calls, and the frequency of such calls.

117. By obtaining such information, the Defendants have arrogated to themselves the ability to monitor Schuchardt's communications, and Schuchardt's business and political relationships. By doing so, the Defendants have obtained the power to contact and harass virtually all persons with whom Schuchardt does business.

118. This power is extremely dangerous in the hands of the Defendants. The Defendants are in control of a government organization that with vast police and military powers.

119. The Plaintiff has an expectation of privacy in the above-described information.

120. According to the Fourth Amendment of the United States Constitution, the power to seize and monitor the communications of citizens is reserved to a court of law, and not to the Defendants.

121. On December 16, 2013, the United States District Court for the District of Columbia found the Defendants' seizure of phone call metadata was unlawful under the Fourth Amendment of the United States Constitution. See Klayman v. Obama, Case No. 1:13-cv-00851-RJL (D.C. Cir. 2013).

122. According to 28 U.S.C. § 2201, this Court has the power to adjudicate a dispute between the Plaintiff and the Defendants involving any issue involving federal law.

WHEREFORE, the Plaintiff respectfully requests that this Honorable Court enter an order (a) enjoining the Defendants from engaging in any further collection of the metadata for the phone calls made through Verizon by the Plaintiff and the Nationwide Class, and (b) establishing procedures to ensure that the Defendants refrain from unlawful conduct in the future.

COUNT III

Injunctive Relief

Intrusion / Invasion of Privacy

123. The Plaintiff incorporates by reference all of the above paragraphs as though set forth herein in their entirety.

124. The Plaintiff has a reasonable expectation of privacy in the above-described communications being collected by the Defendants.

125. The Defendants have knowingly and intentionally invaded the privacy of the Plaintiff -- and have intruded upon the private affairs of the Plaintiff -- in violation of Pennsylvania law.

126. The Defendants' conduct is illegal under the laws of the federal government and the Commonwealth of Pennsylvania.

127. The Defendants are aware that their conduct is unlawful.

128. It is unclear whether monetary damages will be sufficient to compensate the Plaintiff.

129. The Defendants have already compromised, or caused the termination of, all secure e-mail communication services based in the United States.

130. Upon information and belief, the Defendants have also compromised the security of the cloud storage services, Dropbox and Microsoft's Skydrive.

131. Given the dearth of secure, alternative e-mail and cloud storage services available in the United States, the Plaintiff respectfully seeks injunctive relief against the Defendants.

WHEREFORE, the Plaintiff respectfully requests that this Honorable Court enter an order (a) enjoining the Defendants from engaging in any further collection of the above-described confidential information of the Plaintiff and the Nationwide Class, and (b) establishing procedures to ensure that the Defendants refrain from unlawful conduct in the future.

COUNT IV

Declaratory and Injunctive Relief

Violation of the First Amendment

Bulk Collection of E-mail and Verizon Metadata

132. The Plaintiff incorporates by reference all of the above paragraphs as though set forth herein in their entirety.

133. According to 28 U.S.C. § 2201, this Court has the power to adjudicate a dispute between the Plaintiffs and the Defendants involving any issue involving federal law.

134. The Defendants are collecting the actual content of the Plaintiff's e-mail and the metadata associated with the Plaintiff's phone calls made through Verizon.

135. In doing so, the Defendants have violated the First Amendment of the United States constitution. Such amendment states as follows:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

1st Amend.

136. The Plaintiff is no longer able to freely express himself by means of e-mail or documents stored by means of internet cloud services because the Defendants are collecting and data-mining such documents.

137. In preparing this complaint, the Plaintiff was not able to use e-mail to consult with certain persons, even though the proposed communications would be entirely lawful. This is because the Defendants could provide such communications *directly* to the lawyers representing the government in this lawsuit.

138. The Defendants have also interfered with the Plaintiff's ability to freely associate with other persons, because the Defendants have unilaterally obtained, without a warrant, phone and internet data showing with whom the Plaintiff associates.

139. If the Defendants' conduct is allowed to continue, it is possible that future American governments will use such information to blackmail or target political enemies.

WHEREFORE, the Plaintiff respectfully requests that this Honorable Court enter an order (a) enjoining the Defendants from engaging in any further collection of the above-described information about the Plaintiff and the Nationwide Class, and (b) establishing procedures to ensure that the Defendants refrain from unlawful conduct in the future.

COUNT V

Declaratory and Injunctive Relief

Violation of the Foreign Intelligence Surveillance Act

140. The Plaintiff incorporates by reference all of the above paragraphs as though set forth herein in their entirety.

141. According to 28 U.S.C. § 2201, this Court has the power to adjudicate a dispute between the Plaintiffs and the Defendants involving any issue involving federal law.

142. The Plaintiff is aggrieved by the above-described conduct of the Defendants.

143. If the Defendants are purporting to act pursuant to the Foreign Intelligence Surveillance Act, then it appears that the Defendants are in violation of such act.

144. According to 50 U.S.C. § 1861(b)(2)(B), the Defendants are required to utilize “minimization procedures” with respect to information that is inadvertently obtained concerning an “unconsenting United States person” during an investigation relating to international terrorism or clandestine intelligence activities.

145. On July 29, 2009, Attorney General Eric Holder adopted minimization procedures that allowed the Defendants to retain the Plaintiff's confidential and valuable information for a period of up to five years, and possibly longer.

146. Such minimization procedures were kept secret from the Plaintiff until recently.

147. The minimization procedures adopted by the Attorney General are unlawful, and do not comply with the federal law.

148. The Foreign Intelligence Surveillance Act does not contemplate, or authorize, the retention of the Plaintiff's confidential information for a period of five years.

WHEREFORE, the Plaintiff and the Nationwide Class respectfully request that this Honorable Court enter an order determining that the maximum duration of the minimization procedures under the Foreign Intelligence Surveillance Act, as it applies to the confidential information of the Plaintiff and the Nationwide Class, is substantially less than five years.

COUNT VI

Civil Liability

18 U.S.C. § 1810

149. The Plaintiff incorporates by reference all of the above paragraphs as though set forth herein in their entirety.

150. According to 18 U.S.C. § 1810, the Defendants are civilly liable to the Plaintiff for having unlawfully collected the Plaintiff's private communications and private data. Such statute provides as follows:

> § 1810. Civil liability
>
> An aggrieved person, other than a foreign power or an agent of a foreign power, as defined in section 101(a) or (b)(1)(A) [50 USCS § 1801(a) or (b)(1)(A)], respectively, who has been subjected to an electronic surveillance or about whom information obtained by electronic surveillance of such person has been disclosed or used in violation of section 109 [50 USCS § 1809] shall have a cause of

> action against any person who committed such violation and shall be entitled to recover--
>
> (a) actual damages, but not less than liquidated damages of $ 1,000 or $ 100 per day for each day of violation, whichever is greater;
>
> (b) punitive damages; and
>
> (c) reasonable attorney's fees and other investigation and litigation costs reasonably incurred.

18 U.S.C. § 1810 (2014).

151. The Defendants have violated such act by collecting and data mining the Plaintiff's private communications and documents.

152. The Defendants' conduct has been occurring on a daily basis since at least March 12, 2006 – a total of more than 3,000 days. At $100 per day, the total statutory damages exceeds $300,000, not including punitive damages and attorneys fees.

WHEREFORE, the Plaintiff respectfully requests that this Honorable Court enter an order awarding to the Plaintiff and the members of the Nationwide Class (a) actual or statutory damages in this case, (b) punitive damages, and (c) if the Plaintiffs are represented by an attorney other than the Plaintiff, Elliott Schuchardt, reasonable attorneys fees in bringing this action.

Respectfully submitted,

By: /s/ Elliott J. Schuchardt
Elliott Schuchardt
PA I.D. #78911

SCHUCHARDT LAW FIRM
U.S. Steel Tower, Suite 660
600 Grant Street
Pittsburgh, PA 15219
Phone: (412) 414-5138
E-mail: elliott016@gmail.com

CERTIFICATE OF SERVICE

I, Elliott Schuchardt, hereby certify that I served a true and correct copy of the foregoing Second Amended Complaint on the following person on this 24th day of November 2014 by means of the Court's CM / ECF electronic filing system:

Marcia Berman, Esq.
United States Dept. of Justice
marcia.berman@usdoj.gov
Counsel for the Defendants

/s/ Elliott Schuchardt
Elliott Schuchardt