

No. _____

In the
Supreme Court of the United States

ELLIOTT J. SCHUCHARDT, individually and
doing business as the Schuchardt Law Firm,
Petitioner,

v.

PRESIDENT OF THE UNITED STATES, ET AL.,
Respondents.

On Petition for Writ of Certiorari to the
United States Court of Appeals
for the Third Circuit

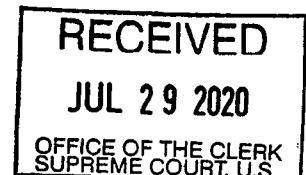
PETITION FOR WRIT OF CERTIORARI

ELLIOTT J. SCHUCHARDT
SCHUCHARDT LAW FIRM
6223 Highland Place Way
Suite 201
Knoxville, TN 37919
(865) 304-4374
elliott016@gmail.com

Appearing Pro Se

July 27, 2020

Becker Gallagher · Cincinnati, OH · Washington, D.C. · 800.890.5001



QUESTIONS PRESENTED

On June 5, 2013, former United States government contractor Edward Snowden released documents indicating that the federal government was intercepting and electronically storing (“collecting”) the *full content* of e-mail in the United States without a warrant.

The Petitioner, Elliott Schuchardt, is an attorney practicing law in Knoxville, Tennessee. On June 2, 2014, Schuchardt filed suit against the federal government, seeking an injunction to prevent collection of his e-mail, and that of the members of his proposed class.

The issues in this case are as follows:

1. Whether Schuchardt has presented sufficient factual evidence of Defendants’ bulk collection of e-mail to establish a *prima facie* case for violation of the 4th Amendment.
2. Whether the executive branch of the federal government should have unfettered access to the nation’s e-mail database, without having to seek access through the courts.

PARTIES TO THE PROCEEDING

The Petitioner is Elliott J. Schuchardt, individually and doing business as the Schuchardt Law Firm. The Petitioner was the Appellant in the Third Circuit case below.

The Respondents are various officers of the United States federal government, in their official capacities. The Respondents were the Appellees below. The Respondents are:

Donald J. Trump, in his capacity of President of the United States

John Ratcliffe, as Director of National Intelligence

Paul M. Nakasone, as Director of the National Security Agency

Christopher A. Wray, as Director of the Federal Bureau of Investigation

STATEMENT OF RELATED PROCEEDINGS

Schuchardt v. President of United States et al., U.S. Court of Appeals for the Third Circuit, Case No. 19-1366, opinion and judgment entered on Mar. 2, 2020.

Schuchardt v. Trump, et al., U.S. District Court for the Western District of Pennsylvania, Case No. 14-705, opinion and judgment entered Feb. 4, 2019.

Schuchardt v. President of United States, et al., U.S. Court of Appeals for the Third Circuit, Case No. 15-3491, opinion and judgment dated Feb. 5, 2016.

Schuchardt v. Obama, et al., U.S. District Court for the Western District of Pennsylvania, Case No. 14-705, opinion and judgment dated Sept. 30, 2015.

TABLE OF CONTENTS

QUESTIONS PRESENTED	i
PARTIES TO THE PROCEEDING.....	ii
STATEMENT OF RELATED PROCEEDINGS ...	iii
TABLE OF AUTHORITIES.....	vii
OPINIONS BELOW.....	2
JURISDICTIONAL STATEMENT	3
CONSTITUTIONAL PROVISION INVOLVED....	3
STATEMENT OF CASE	4
PROCEDURAL BACKGROUND	15
REASONS FOR GRANTING THE PETITION ...	18
I. The District Court erred by dismissing this case for lack of subject matter jurisdiction	18
A. Schuchardt has adequately pled a cause of action for violation of the 4th Amendment.....	19
B. The District Court erred by deciding the <i>merits</i> of this case on a motion challenging subject matter jurisdiction	25
C. Schuchardt presented to the lower court ample factual evidence of improper government collection of e-mail	27
II. It is proper for the Court to grant a writ of certiorari in this case	29

A. The executive branch is infringing on the investigatory function of this Court	30
B. Respondents' conduct is an impermissible "general warrant."	33
C. The Respondents' system provides no effective protection for the information of U.S. citizens	35
D. Four federal circuit courts have held that plaintiffs have standing in collection cases, such as this case	37
E. The Privacy and Civil Liberties Board did not ratify Respondents' collection activities. . . .	41
CONCLUSION	43
APPENDIX	
Appendix A Opinion and Judgment in the United States Court of Appeals for the Third Circuit (March 2, 2020)	App. 1
Appendix B Order and Judgment Order in the United States District Court for the Western District of Pennsylvania (February 4, 2019)	App. 19
Appendix C Opinion and Judgment in the United States Court of Appeals for the Third Circuit (October 5, 2016)	App. 25

Appendix D	Memorandum Order and Judgment Order in the United States District Court for the Western District of Pennsylvania (September 30, 2015)	App. 65
Appendix E	Constitutional Provision Involved.	App.81
Appendix F	Second Amended Complaint (November 24, 2014).	App. 82
Appendix G	Affidavit of Elliott J. Schuchardt (January 7, 2015)	App. 119
Appendix H	Affidavit of William E. Binney (July 4, 2017).	App. 124

TABLE OF AUTHORITIES

CASES

<i>ACLU v. Clapper</i> , 785 F.3d 787; 2015 U.S. C.A.App. LEXIS 7531 (2d Cir. 2014)	37, 38
<i>Ashcroft v. Iqbal</i> , 556 U.S. 662, 129 S. Ct. 1937 (2009)	19
<i>Boumediene v. Bush</i> , 553 U.S. 723, 128 S. Ct. 2229 (2008)	30
<i>Clinton v. City of New York</i> , 524 U.S. 417, 118 S. Ct. 2091 (1998)	33
<i>Davis v. United States</i> , 328 U.S. 582, 66 S. Ct. 1256, 90 L. Ed. 1453 (1946)	44
<i>Davis v. Wells Fargo</i> , 824 F.3d 333 (3d Cir. 2020)	1, 26
<i>Gould Elecs., Inc. v. United States</i> , 220 F.3d 169 (3d Cir. 2000)	18, 25
<i>Hartig Drug Co. Inc. v. Senju Pharm. Co. Ltd.</i> , 836 F.3d 261 (3d Cir. 2016)	25
<i>Jewel v. NSA</i> , 673 F.3d 902 (9th Cir. 2011).....	37
<i>Klayman v. Obama</i> , 957 F. Supp. 2d 1 (D.D.C. 2013).....	40
<i>Marbury v. Madison</i> , 5 U.S. 137 (1803).....	30

<i>Mortensen v. First Fed. Sav. & Loan Ass'n</i> , 549 F.2d 884 (3d Cir. 1977)	25
<i>United States v. Mitchell</i> , 377 F. Supp. 1326 (D.D.C. 1974)	31
<i>United States v. Nixon</i> , 418 U.S. 683 (1974)	30, 31, 32
<i>Warden, Maryland Penitentiary v. Hayden</i> , 387 U.S. 294, 87 S. Ct. 1642, 18 L. Ed. 2d 782 (1967)	34, 35
<i>Wikimedia Foundation v. National Security</i> <i>Agency</i> , 857 F.3d 193 (4th Cir. 2017)	18, 39
<i>Youngstown Sheet & Tube Co. v. Sawyer</i> , 103 F. Supp. 569 (D.D.C. 1952)	30

CONSTITUTION AND STATUTES

U.S. Const. art. III, Sect. 1	31
U.S. Const. amend. IV	<i>passim</i>
28 U.S.C. § 1254	3
28 U.S.C. § 1331	1, 18
Foreign Intelligence Surveillance Act, 50 U.S.C, chap. 36	5

RULES

Fed. R. Civ. P. 12(b)(1)	1, 18, 25, 26
Sup. Ct. R. 13.1	3

OTHER AUTHORITIES

3 Elliot's Debates	35
"Erin Burnett - Outfront," CNN, May 13, 2013, at https://www.youtube.com/watch?v=fFnCe0gTh1Y	28
Report of the Privacy & Civil Liberties Board (2014).....	42
James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," N.Y. Times, Dec. 16, 2005.....	28
Statement of Diane Roark, former staff member, United States Senate, at 1 hour, 13 minutes in https://www.c-span.org/video/?450976-1/national-security-agency-september-11-2001	5, 27
Transcript of Snowden appearance, at www.ted.com	14

PETITION FOR WRIT OF CERTIORARI

The Petitioner, Elliott J. Schuchardt, files this petition for a writ of certiorari to review a judgment of the United States Court of Appeals for the Third Circuit.

On March 2, 2020, the Third Circuit entered an order finding that the Petitioner did not establish subject matter jurisdiction in this case, pursuant 28 U.S.C. § 1331.

The Petitioner respectfully requests that the Court grant a writ of certiorari for the reasons set forth below.

First, it was improper for the District Court to decide this case on a Rule 12(b)(1) motion to dismiss for lack of subject matter jurisdiction, when the merits of such motion were the *same* as the merits of the case itself. The Third Circuit has repeatedly stated that cases should *not* be dismissed in such circumstances. *See Davis v. Wells Fargo*, 824 F.3d 333, 348-349 (3d Cir. 2020).

Second, there are important public policy reasons why this case should move forward. Schuchardt contends that Respondents are collecting the full content of the nation's e-mail database, in violation of the 4th Amendment of the United States Constitution.

Respondents have established a computer database of private communications, which they can presently access at will. Such database consists of the full content of all e-mail sent within or passing through United States communication facilities.

As evidence of this statement, Schuchardt filed with the District Court an affidavit of William E. Binney -- a former technical director at the National Security Agency. (App. 124). In his affidavit, Binney testified that he helped create Respondents' system, has reviewed the documents released by Edward Snowden, and believes Respondents are continuing to collect the full collection of the nation's e-mail. *Id.*

The bulk collection system established by Respondents is unworkable, and will foreseeably be abused by those who control the database. In fact, abuse of the system is already occurring, with alleged unauthorized access to the database taking place during the 2016 federal election.

It is safer to place such database in the hands of the internet service providers themselves, *with access being controlled by the courts*. Public policy and the 4th Amendment require such conclusion.

OPINIONS BELOW

The opinion of the Court of Appeals, dated March 2, 2020, is reported at 802 Fed. Appx. 69, 111 Fed. R. Evid. Serv. (CBC) 908, 2020 WL 995735. It is reproduced at App. 1-18.

The opinion of the District Court, dated February 4, 2019, is unreported, but is available at 2019 U.S. Dist. LEXIS 17174, 2019 WL 426482. It is reproduced at App. 19-24.

The opinion of the Court of Appeals, dated February 5, 2016, is reported at 839 F.3d 336. It is reproduced at App. 25-64.

The opinion of the District Court, dated September 30, 2015, is unreported, but is available at 2015 U.S. Dist. LEXIS 132962. It is reproduced at App. 65-80.

JURISDICTIONAL STATEMENT

This appeal is from a judgment of the U.S. Court of Appeals for the Third Circuit entered on March 2, 2020.

This Court has jurisdiction over this petition pursuant to 28 U.S.C. § 1254 (2020).

This petition has been filed within the time limits set forth in Supreme Court Rule 13.1 and Supreme Court Order 589.

CONSTITUTIONAL PROVISION INVOLVED

The Fourth Amendment of the United States Constitution states as follows:

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.

U.S. Const. amend IV.

STATEMENT OF CASE

This case challenges Respondents' collection of e-mail sent within the United States without a warrant. The facts of the case are well-established.

In 1998, the National Security Agency (the "NSA") developed the ability to tap the nation's fiber optic lines, in order to collect¹ certain information associated with the nation's growing e-mail traffic. (C.A.App. 229, ¶ 12). The initial program was led by William Binney, a technical director at the NSA. (C.A.App. 230, ¶¶ 16-17). Binney is the Petitioner's expert witness in this case.

In the late 1990s, there was an internal debate at the NSA as to whether the government should collect the full content of e-mail, or just information relating to the persons sending and receiving the communication. That debate was secretly resolved -- at least temporarily -- following the events of September 11, 2001. (C.A.App. 230).

On October 4, 2001, President George W. Bush authorized the NSA to collect the *full content* of e-mail sent within or passing certain United States communication facilities. The program, called Stellar Wind, was *not* disclosed to the general public.² (C.A.App. 94, 230).

¹ In this brief, the term "collect" means to intercept, access and store an electronic communication or information in a digital form.

² The program was only disclosed to the chairperson and ranking opposing party member of the U.S. House and U.S. Senate intelligence committees. No other members of Congress were briefed on the program.

With this decision, the NSA's philosophy became very different. Its goal and *modus operandi* were now to "own the internet" and "collect it all."³

In December 2005, the New York Times published an article about the Stellar Wind program, exposing it for the first time. (D.C.Docket No. 68, at 1.) A few months later, in May 2006, an AT&T technician revealed that the NSA was copying all e-mail passing through an AT&T communication facility in San Francisco. *Id.*

Following these disclosures, the federal government sought to establish the legality of the Stellar Wind program through the Foreign Intelligence Surveillance Court (the "FISC"). (D.C.Docket No. 68, at 2.) The FISC is a court established pursuant to the Foreign Intelligence Surveillance Act, 50 U.S.C. chap. 36 ("FISA"). *Id.*

On December 13, 2006, the U.S. Department of Justice filed an application with the FISC for approval of the Stellar Wind program. The application asked the FISC to give the government blanket authority to collect all e-mail passing through specific communication facilities. Once collected, the e-mail could be searched with approval of the Attorney General, but not a court. (D.C.Docket No. 68, at 2.)

³ See Statement of Diane Roark, former staff member, United States Senate, at 1 hour, 13 minutes in <https://www.c-span.org/video/?450976-1/national-security-agency-september-11-2001>.

On January 10, 2007, the Honorable Malcolm J. Howard, a judge with the FISC, preliminarily approved the government's petition. *Id.*

Shortly thereafter, then-Attorney General Alberto Gonzales told the media that the warrantless collection program had been brought "under the authority of the FISC." He described the administration's legal theory as "innovative" and "complex." (D.C.Docket No. 68, at 2.)

However, Gonzales spoke too soon. On March 21, 2007, the government filed an application to renew the bulk collection authority approved by Judge Howard. This time, the FISC *denied* the application. *Id.* In an opinion written on April 3, 2007, Judge Roger Vinson held that the government's bulk collection of e-mail was *not* authorized by the Foreign Intelligence Surveillance Act. *Id.* at 2.

In denying the government's request, Judge Vinson explained his reasoning as follows:

Congress intended the pre-surveillance "judicial warrant procedure," and particularly the judge's probable cause findings, to provide an external check on executive branch decisions to conduct surveillance.

Contrary to this intent of Congress, the probable cause inquiry proposed by the government *could not possibly* restrain executive branch decisions to direct surveillance at any particular individual, telephone number or e-mail address.

* * *

The government would have all the probable cause findings . . . made *by executive branch officials*, subject to after-the-fact reporting to the Court. That result cannot be squared with the statutory purpose of providing a pre-surveillance “external check” on surveillance decisions.⁴

Judge Vinson therefore ordered the government to cease collecting e-mail as of May 31, 2007.⁵

Before finishing his opinion, however, Judge Vinson addressed the government’s argument that the President can collect the nation’s e-mail under his powers as Commander in Chief of the armed forces. Vinson addressed this argument as follows:

I recognize that the government maintains that the President may have “constitutional or statutory authority to conduct the electronic surveillance detailed herein *without Court authorization*.” [Citations omitted]. **Nothing in this order and opinion is intended to address the existence or scope of such authority, or this Court’s jurisdiction over such matters.**⁶

In other words, the FISC indicated that it would “look the other way” if the President sought to collect the nation’s e-mail under the President’s alleged powers as Commander in Chief. In making this

⁴ D.C.Docket No. 23, at 4; D.C.Docket No. 23-4, at 15-16.

⁵ D.C.Docket No. 23, at 4; D.C.Docket No. 23-4, at 21.

⁶ D.C.Docket No. 23, at 5; D.C.Docket No. 23-4, at 20 (emphasis added).

statement, Vinson gave the Defendants a green light to collect the nation's e-mail database, without further involvement of – or oversight from – the FISC. That is exactly what Defendants did. (D.C.Docket No. 68, at 3).

During the summer of 2007, Defendants began to ramp up the most massive invasion of privacy ever seen in the history of the world. Their goal was then -- and it is *now* -- to intercept and store all online documents and communications. This includes all documents sent by e-mail, as well as documents stored in cloud service providers, such as Dropbox or Microsoft's Sky Drive. (C.A.App. 100, 149-51).

Defendants' systematic collection got underway on the sixth anniversary of the 911 attacks: On September 11, 2007, Defendants began bulk collection of e-mail sent by means of Microsoft's e-mail service. On March 12, 2008, the Defendants began bulk collection of Yahoo e-mail and web search queries. Other providers followed: Google on January 14, 2009; Facebook on June 3, 2009; YouTube on September 24, 2010; Skype on February 6, 2011; AOL on March 31, 2012; Apple in October 2012; and Dropbox in June 2013. (C.A.App. 108-09; 145-46).

Binney disclosures

During the past fifteen years, a number of persons from the intelligence community have come forward to warn the American people of the dangers of Defendants' conduct.

One of the first critics was William E. Binney, a senior employee of the NSA and the technical director

of the team that created the system. Over the course of his 31-year career, Binney has mentored the technical work of approximately 6,000 employees at the NSA. (C.A.App. 229, ¶ 9).

On July 2, 2012, Binney made the following statement in an Affidavit, filed in this case:

[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.

(C.A.App. 188, ¶¶ 5-6) (emphasis added).

Other former-NSA employees back up Binney's allegations. Thomas Drake, a former employee of the agency with 29 years of experience, 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.

* * *

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.

(C.A.App. 199-200, ¶¶ 7-8, 10) (emphasis added).

Thus, according to the NSA's own former employees, the agency is collecting the full content of the nation's e-mail without a warrant.

Snowden disclosures

In June 2013, another member of the intelligence community came forward. That person was Edward Snowden. (C.A.App. 143).

Snowden is a former system administrator for the Central Intelligence Agency ("CIA"). He later worked for the consulting firm, Booz Allen Hamilton, inside an NSA center located in Hawaii. (C.A.App. 143). In these positions, Snowden worked directly with the Chief Information Officer at the CIA to solve the agency's technology problems. Thus, like "Deepthroat" in the Watergate scandal, Snowden was a senior

government employee with knowledge of what was going on. *Id.*

While working for Respondents, Snowden learned that Respondents were collecting the full content of substantially all of e-mail sent by American citizens by means of several large internet service providers. (C.A.App. 143).

In early 2013, Snowden approached several reporters to disclose his discovery. The information he provided led to a series of articles published in the *Guardian* and *Washington Post* newspapers. (C.A.App. 144, ¶¶ 32-33).

On June 6, 2013, the *Guardian* published an article, which reported that Respondents had obtained direct access to the servers of several large internet companies, including Yahoo, Google, Facebook, Twitter, Dropbox, and Apple. (C.A.App. 145, ¶ 35).

The article is based on documents provided by Edward Snowden. Such documents show that Respondents are collecting *all e-mail* sent by means of certain internet companies based in the United States. This includes e-mail sent by means of Microsoft, Yahoo, Google, Facebook, PalTalk, AOL, Skype, YouTube and Apple. (C.A.App. 108-09). The documents also show that Respondents are collecting all documents stored by means of certain cloud service providers, such as Dropbox and Microsoft's Skydrive. (C.A.App. 145-46).

For example, one document is labeled "New Collection Posture." It says: "Sniff It All, Know It All, Collect It All, Process It All." (C.A.App. 110, 146).

Another document boasts that the Respondents are “one step closer to **collecting it all**.” (C.A.App. 111, 146).

Respondents are literally storing every single document stored on Microsoft’s Skydrive -- a cloud service. For example, 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.”

(C.A.App. 112, 146-47).

Respondents’ collection efforts have become so massive that Respondents are having difficulty processing all of the data. According to one document obtained from Snowden: “Collection is outpacing [Respondents’] ability to ingest, process and store to the ‘norms’ to which [they] have become accustomed.” (C.A.App. 113, 147).

Any doubt about the meaning of these documents is resolved by the statements made by 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.

(C.A.App. 115, 147) (emphasis added).

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.

(C.A.App. 126-27, 147).

The above statements are astonishing, and indicate a massive breach on the part of the Respondents of the public trust, as well as a violation of United States law.

Following Snowden's disclosures, Respondents claimed that they were only storing "metadata," and not the actual content of electronic documents and communications.⁷

⁷ Metadata refers to certain information relating to a specific e-mail. It includes the date and time of the communication; the sender; and the recipient of the e-mail. However, it would not include the content of the e-mail.

Snowden responded to the government's "spin" in March 2014, when he appeared at a TED conference in Vancouver, Canada by means of video conference. 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.*⁸

(C.A.App. 148).

More recently, extended interviews with Snowden have appeared in Laura Poitras' film, *CitizenFour*. In that film, Snowden states directly that the Respondents are collecting the *full content* of Americans' e-mail, without a warrant or any sort of court supervision. *Id.*

Snowden has therefore confirmed the allegations of earlier whistleblowers, Binney and Drake.

Lavabit Disclosures

Prior to June 2013, Edward Snowden used an encrypted e-mail service called "Lavabit." (C.A.App. 148-49).

Following Snowden's disclosures, Respondents approached Lavabit and demanded that Lavabit install a device on its server which would have provided Respondents *with access to the full content of all e-mail messages for all of Lavabit's 410,000 customers*, an extraordinary – and patently illegal – request.

⁸ See Transcript of Snowden appearance, at www.ted.com.

(C.A.App. 130, 148-49). Respondents 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. *Id.*

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

The following day, on August 9, 2013, another 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 Respondents' hands. (C.A.App. 131, 149).

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

PROCEDURAL BACKGROUND

The Plaintiff, Elliott Schuchardt, is an attorney practicing law in Knoxville, Tennessee. Schuchardt has practiced law for twenty-eight years. (C.A.App. 156).

Schuchardt is a consumer of many of the internet services at issue in this case. He uses e-mail provided by Google, Facebook and Yahoo; he conducts web searches through the Google search engine; and he stores his personal and law firm documents by means of the Dropbox cloud storage service. (C.A.App. 156, 255).

As a lawyer, Schuchardt is required to keep his communications with clients confidential. He is not able to do so if the Respondents are actively intercepting and storing his e-mail and online documents. (C.A.App. 255).

On June 2, 2014, Schuchardt filed a complaint against the Respondents, seeking an injunction. Schuchardt subsequently amended the complaint on September 2 and November 24, 2014. (C.A.App. 70, 138).

On December 11, 2014, the Respondents filed a motion to dismiss Schuchardt's second amended complaint, pursuant to Rule 12(b)(6) of the Federal Rules of Civil Procedure. (C.A.App. 8).

On January 7, 2015, Schuchardt filed a motion for a preliminary injunction. (C.A.App. 8). The District Court denied the motion shortly thereafter. *Id.*

On September 30, 2015, the District Court entered an order dismissing the case, after finding that Schuchardt did not have standing to raise the issues set forth in the complaint. (App. 65).

On October 14, 2015, Schuchardt appealed to the U.S. Court of Appeals for the Third Circuit. (C.A.App. 8).

On October 5, 2016, the Third Circuit reversed the District Court's order dismissing the case. (App. 25). In its opinion, the court found that Schuchardt had established "facial" standing to pursue the case. The court remanded the case to the District Court, to

consider whether Schuchardt had sufficient factual evidence to move forward with his allegations. *Id.*

On March 15, 2017, Respondents filed a second motion to dismiss the complaint. (C.A.App. 11). Schuchardt filed a response in opposition to the motion July 10, 2017. (C.A.App. 11-12). Schuchardt's response consisted of a brief and several affidavits. One of the affidavits was submitted by William E. Binney, a former technical director at the National Security Agency. (App.124).

On February 4, 2019, the District Court entered a memorandum opinion and order dismissing the case. (App. 19).

On February 12, 2019, Schuchardt appealed the District Court's order to the U.S. Court of Appeals for the Third Circuit. (C.A.App. 13, 68).

On September 23, 2019, the Third Circuit held oral argument in connection with the case. On March 2, 2020, the Circuit Court issued an opinion and order affirming the District Court's order dismissing the case. (App. 1)

REASONS FOR GRANTING THE PETITION

The District Court dismissed this case for lack of subject matter jurisdiction, pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure.

In doing so, the court improperly decided the case on the merits, before the case could be litigated.

I. The District Court erred by dismissing this case for lack of subject matter jurisdiction.

A claim may be dismissed under Rule 12(b)(1) only if it “clearly appears to be immaterial” or is “wholly insubstantial and frivolous.” *Gould Elecs., Inc. v. United States*, 220 F.3d 169, 178 (3d Cir. 2000). This is an extremely *low standard*, which indicates that this case should move forward.

Schuchardt has subject matter jurisdiction in this case because the complaint pleads a violation of the 4th Amendment of the Constitution. The 4th Amendment prohibits government interference with the private papers of the citizenry, without a warrant issued upon a finding of probable cause. U.S. Const., 4th Amend.

Subject matter jurisdiction exists in this case pursuant to 28 U.S.C. § 1331, which states that the district courts of the United States “shall have original jurisdiction of all civil actions arising under the Constitution, laws, or treaties of the United States.” 28 U.S.C. § 1331 (2020).

It is proper for the Court to reverse the lower courts’ decision for the reasons set forth below.

A. Schuchardt has adequately pled a cause of action for violation of the 4th Amendment.

“To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, ‘to state a claim to relief that is plausible on its face.’” *Wikimedia Foundation v. National Security Agency*, 857 F.3d 193, 208 (4th Cir. 2017).

In *Ashcroft v. Iqbal*, 556 U.S. 662, 678, 129 S. Ct. 1937, 1949 (2009), this Court elaborated on this standard:

A pleading that offers “labels and conclusions” or “a formulaic recitation of the elements of a cause of action will not do.” 550 U.S., at 555, 127 S. Ct. 1955, 167 L. Ed. 2d 929. Nor does a complaint suffice if it tenders “naked assertion[s]” devoid of “further factual enhancement.” [citations omitted].

To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to “state a claim to relief that is plausible on its face.” *Id.*, at 570, 127 S. Ct. 1955, 167 L. Ed. 2d 929. A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. *Id.*, at 556, 127 S. Ct. 1955, 167 L. Ed. 2d 929.

Iqbal, 556 U.S. at 678, 129 S. Ct. at 1949 (emphasis added).

The Petitioner, Elliott Schuchardt, has satisfied this standard. Schuchardt's complaint includes a plethora of factual allegations concerning improper government collection of e-mail. Specifically, Count I of the Second Amended Complaint states as follows:

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 Respondents 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 Respondents' above-described activities as the "collection" of private communications.

90. The Respondents' 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 Respondents 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 Respondents 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 Respondents 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 Respondents have been collecting the content of the Plaintiffs' e-mail and instant messages through Facebook.

96. Upon information and belief, since approximately June 2013, the Respondents 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 Respondents 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 Respondents also include communications with clients of Schuchardt's law firm, which are privileged and confidential under applicable law.

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

100. Upon information and belief, the Respondents 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 Respondents' 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 Respondents' 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 Respondents – 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 Respondents involving any issue involving federal law.

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

107. The Respondents 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 Respondents.

110. The Respondents 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 Respondents 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 Respondents, is unlawful as a violation of the 4th Amendment of the United States Constitution.

113. If the Respondents 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.

(App. at 105-109).

Thus, the complaint itself pleads ample detail of improper government collection.

B. The District Court erred by deciding the merits of this case on a motion challenging subject matter jurisdiction.

The District Court considered Respondents' motion to be a "factual challenge" pursuant to Rule 12(b)(1) of the Federal Rules of Civil Procedure. In doing so, the District Court improperly considered the merits of the case on a preliminary motion to dismiss.

On a Rule 12(b)(1) factual challenge, the plaintiff has the burden of proof and the burden of persuasion. *Mortensen v. First Fed. Sav. & Loan Ass'n*, 549 F.2d 884, 891 (3d Cir. 1977); *Gould Elecs. Inc. v. United States*, 220 F.3d 169, 176 (3d Cir. 2000). Thus "a 12(b)(1) factual challenge strips the plaintiff of the protections and factual deference provided under 12(b)(6) review" for a typical motion to dismiss on the merits. *Hartig Drug Co. Inc. v. Senju Pharm. Co. Ltd.*, 836 F.3d 261, 268 (3d Cir. 2016).

For this reason, it is *improper* for a court to dismiss a case pursuant to Rule 12(b)(1) when the jurisdictional facts are intertwined with the merits of the case. As explained by the Third Circuit:

We have repeatedly cautioned against allowing a Rule 12(b)(1) motion to dismiss for lack of subject matter jurisdiction to be turned into an attack on the merits. *E.g.*, *Gould Elecs. Inc. v. United States*, 220 F.3d 169, 178 (3d Cir. 2000); *Growth Horizons, Inc. v. Delaware Cty., Pa.*, 983 F.2d 1277, 1280-81 (3d Cir. 1993); *Kehr Packages, Inc. v. Fidelcor, Inc.*, 926 F.2d 1406, 1408-09 (3d Cir. 1991) Caution is necessary

because the standards governing the two rules differ markedly, as Rule 12(b)(6) provides greater procedural safeguards for plaintiffs than does Rule 12(b)(1). . . . Unlike Rule 12(b)(6), under which a defendant cannot contest the plaintiff's factual allegations, Rule 12(b)(1) allows a defendant to attack the allegations in the complaint and submit contrary evidence in its effort to show that the court lacks jurisdiction. *Mortensen*, 549 F.2d at 891. Thus, improper consideration of a merits question under Rule 12(b)(1) significantly raises both the factual and legal burden on the plaintiff. Given the differences between the two rules, "[a] plaintiff may be prejudiced if what is, in essence, a Rule 12(b)(6) challenge to the complaint is treated as a Rule 12(b)(1) motion." *Kehr Packages*, 926 F.2d at 1409.

Davis v. Wells Fargo, 824 F.3d 333, 348-349 (3d Cir. 2020).

According to the above case, it is improper for a court to decide the merits of a case on a motion to dismiss pursuant to Rule 12(b)(1), when the motion raises the *same* issues as the factual challenge to jurisdiction. Yet that is exactly what the Third Circuit did in this case. It is therefore proper for this Court to reverse the order of the Third Circuit.

**C. Schuchardt presented to the lower court
ample *factual* evidence of improper
government collection of e-mail.**

In the litigation below, Schuchardt presented ample factual evidence in support of his allegations. Such factual evidence consisted of an affidavit by William E. Binney, a former technical director at the National Security Agency. Binney reviewed some of the documents leaked by former government contractor Edward Snowden. In his affidavit, Binney stated his opinion that such documents were accurate and that they indicated Respondents are improperly collecting the nation's e-mail database. (App. 124)

Schuchardt provided a wide variety of other evidence as well. Such evidence included the following:

<u>Date</u>	<u>Disclosure</u>
December 2001	Colleagues at NSA disclose to William Binney that the agency is collecting full content of domestic e-mail, without privacy protections. (App. 124, ¶ 5; C.A.App. 230).
December 2001	According to U.S. Senate Staffer, Diane Roark, the objective of the NSA at this time was to "own the internet" and "collect it all." ⁹

⁹ See Statement of Diane Roark, former staff member, United States Senate, at 1 hour, 13 minutes in <https://www.c-span.org/video/?450976-1/national-security-agency-september-11-2001>.

December 2005	New York Times discloses existence of program collecting full content of domestic e-mail, without court supervision. ¹⁰ (C.A.App. 231).
February 2008	Scientist at Sandia National Laboratory discloses to Schuchardt that "every single e-mail that you send goes into a government database." (Schuchardt testimony).
May 1, 2013	Former FBI Special Agent, Tim Clemente, states on CNN that "all digital communications are captured," and can be reviewed retroactively. ¹¹
June 2013	Former CIA systems administrator, Edward Snowden, claims ability to access a database containing the full content of United States domestic e-mail. (C.A.App. 143-47).
August 2013	Ladar Levison complains that Defendants want the access codes for <i>all e-mail</i> within his encrypted e-mail service, Lavabit. (C.A.App. 130).

¹⁰ James Risen and Eric Lichtblau, "Bush Lets U.S. Spy on Callers Without Courts," N.Y. Times, Dec. 16, 2005, at A1.

¹¹ See "Erin Burnett - Outfront," CNN, May 13, 2013, at <https://www.youtube.com/watch?v=fFnCe0gTh1Y>.

June 2014	Schuchardt commences this lawsuit.
July 2017	William Binney confirms that the government is continuing to collect full content of U.S. domestic e-mail. (C.A.App. 231-32). His conclusion is based on a review of the Snowden documents, as well as his consulting for foreign governments. (C.A.App. 240, at ¶ 68).

As explained above, Schuchardt has significant evidence that Respondents are engaging in bulk collection of United States domestic e-mail. Schuchardt's evidence is documented in the affidavits filed in this case. (App. 119, 124).

II. It is proper for the Court to grant a writ of certiorari in this case.

There are numerous reasons why the Court should grant a writ of certiorari in this case.

First, the executive branch is interfering with the investigatory function of this Court, and illegally probing into the private communications of American citizens.

Second, the executive branch is abusing the power that it has obtained by assembling a database of the nation's private communications.

Third, the lower courts have indicated that it is proper for the courts to exercise jurisdiction in collection cases.

Finally, the executive branch's own investigatory body -- the Privacy and Civil Liberties Oversight Board -- has expressed concerns about the scope and breadth of the government's growing database.

Each of these arguments is discussed in greater detail below.

A. The executive branch is infringing on the investigatory function of this Court.

In 1803, in *Marbury v. Madison*, 5 U.S. 137 (1803), this Court stated that it has the power to issue orders binding upon the executive branch of the United States.

Since that time, the Court has jealously guarded the power of the federal courts, vis-a-vis the executive branch. See, e.g., *Youngstown Sheet & Tube Co. v. Sawyer*, 103 F. Supp. 569 (D.D.C. 1952) (president does not have the power to seize nation's steel mills under his alleged power as commander in chief of the armed forces); *United States v. Nixon*, 418 U.S. 683 (1974) (president does not have the power to determine the scope of a subpoena issued by a federal court); see also *Boumediene v. Bush*, 553 U.S. 723, 742, 128 S. Ct. 2229, 2246 (2008) ("The Framers' inherent distrust of governmental power was the driving force behind the constitutional plan that allocated powers among three independent branches.").

In this case, the executive branch is attempting to usurp the Court's investigatory function. This function was assigned to the federal courts by Article III of the U.S. Constitution. Specifically, that section provides as follows:

The judicial Power of the United States, shall be vested in one supreme Court, and in such inferior Courts as the Congress may from time to time ordain and establish.

U.S. Const., Art. III, Sect. 1.

By unilaterally seizing the nation's e-mail and searching it without a court order, the Respondents have rendered moot the need for this Court to review and issue subpoenas.

The judicial power of the United States cannot be shared with other branches of the federal government. In 1974, this Court addressed this issue in *United States v. Nixon*, 418 U.S. 683, 704-705, 94 S. Ct. 3090, 3106, 41 L. Ed. 2d 1039, 1062 (1974).

In that case, the U.S. District Court for the District of Columbia issued a subpoena to President Nixon, directing him to produce audio recordings of conversations that occurred in the Oval Office. Nixon moved to quash the subpoena, arguing that production would have violated "executive privilege." The District Court denied Nixon's motion, finding that the federal courts -- and not the President -- are the final arbiter of the law. *United States v. Mitchell*, 377 F. Supp. 1326 (D.D.C. 1974) (Sirica, J).

On appeal, this Court unanimously affirmed Judge Sirica. The Court explained its reasoning as follows:

Our system of government “requires that federal courts on occasion interpret the Constitution in a manner at variance with the construction given the document by another branch.”

* * *

The “judicial Power of the United States” . . . can no more be shared with the Executive Branch than the Chief Executive, for example, can share with the Judiciary the veto power. . . . Any other conclusion would be contrary to the basic concept of separation of powers and the checks and balances that flow from the scheme of a tripartite government. The Federalist, No. 47, p. 313 (S. Mittell ed. 1938). We therefore reaffirm that it is the province and duty of this Court “to say what the law is” with respect to the claim of privilege presented in this case. *Marbury v. Madison*, supra, at 177.

Nixon, 418 U.S. at 704-705, 94 S. Ct. at 3106 (1974).

The seizure of online documents in this case is far more pernicious than the facts of the *Nixon* case. In *Nixon*, the executive branch was wiretapping the political opposition. In this case, the executive branch is essentially wiretapping the entire nation, including the Court itself. (C.A.App. 86).

For the foregoing reasons, the executive branch is attempting to seize the Court’s power. The Plaintiff respectfully submits that the Court enforce its powers,

while it has the ability to do so. *Clinton v. City of New York*, 524 U.S. 417, 450, 118 S. Ct. 2091 (1998) (Kennedy, J., concurring) (“Liberty is always at stake when one or more of the branches seek to transgress the separation of powers”).

B. Respondents’ conduct is an impermissible “general warrant.”

In their pleadings filed with the FISC, Respondents have repeatedly emphasized their “internal controls” in accessing and searching the collected data.

However, these internal controls are not adequate, and will never work. The temptation to search the government’s massive and growing database of private communications will inevitably lead to abuses of Respondents’ unstable system. Political leaders will search the database for information about their opponents. NSA staffers will access the records of major law firms and investment banks for inside information concerning investments. Spurned lovers will use the database to cyber stalk the objects of their affection. The trade secrets of the Fortune 500 are at risk. The possibilities are limitless.

The key to the kingdom must be held by a third party, namely the courts. It should not be necessary to reinvent the wheel on this issue. History tells us the foreseeable result.

The United States constitution grew out of the governmental abuses common during the period from 1761 to 1791. This time period was characterized by aggressive search and seizure practices that were the result of the “general warrant.” A general warrant:

empowered a person “*to search in all places*, where books were printing, in order to see if the printer had a license; and if upon such search he found any books which he suspected to be libelous against the church or state, he was to seize them, and carry them before the proper magistrate.” [citation omitted]. Thus the general warrant became a powerful instrument in proceedings for seditious libel against printers and authors.

Warden, Maryland Penitentiary v. Hayden, 387 U.S. 294, 313-314, 87 S. Ct. 1642, 1653-1654, 18 L. Ed. 2d 782, 796 (1967). **A general warrant was, therefore, very similar to the power that the executive branch is attempting to seize from the Court in this case.**

In 1787, our present Constitution was drafted without a Bill of Rights. The absence of a Bill of Rights became a significant source of concern during the ratification process. There was much talk about general warrants, and the nation’s fear of them. *Id.* Patrick Henry spoke out concerning the dangers of the situation, using words that are, ironically, still relevant today:

The officers of Congress may come upon you now, fortified with all the terrors of paramount federal authority. . . . They may, unless the general government is restrained by a bill of rights, or some similar restriction, go into your cellars and rooms, and search, ransack, and measure, every thing you eat, drink, and wear.

They ought to be restrained within proper bounds.

Warden, Maryland Penitentiary, 387 U.S. at 316, 87 S. Ct. at 1655 (citing 3 Elliot's Debates 448-49).

During the ratification process, several states requested that the new Constitution be amended to provide protection against unjustified searches and seizures. In response, the first Congress proposed the Fourth Amendment, which became part of the Constitution in 1791.

The above history of the Fourth Amendment is important and relevant today. The dangers posed by Respondents' conduct are real. This is why some of the smartest people in the United States government – including William Binney – have risked their liberty to bring this matter to the attention of this Court. This is why there was such an uproar when the Snowden's disclosures became known in June 2013.

If the executive branch can seize all electronic communications without oversight, the power will be abused. As explained below, this is exactly what has occurred.

C. The Respondents' system provides no effective protection for the information of U.S. citizens.

There are several problems with the existing system.

First, as noted by Edward Snowden, the existing system makes possible a warrantless search of private

documents of United States citizens. There is no credible mechanism that requires third party -- *disinterested approval* -- before a search occurs. This has led to improper searches by governmental analysts of the e-mail of various love interests. (C.A.App. 236, ¶ 48, 52). During the 2016 federal election, there were also allegations that President Obama's National Security Adviser, Susan Rice, improperly conducted searches of President Trump's campaign. (C.A.App. 236, ¶ 49).

The existing system is monitored by persons *in the executive branch* -- i.e. other intelligence-community staffers who are generally friends with the people conducting the searches. As a result, there is both a moral hazard that improper searches will occur, and the violations *will not be reported*.

Second, the existing system can be "gamed" by persons at the top of the pyramid. As noted above, there is theoretically a record of every single query made into Respondents' systems -- designed as IC Reach and xKeyScore. However, it is possible for persons at the top of the system to delete the records of certain searches. This enables a higher level of misconduct, such as searches of pending Wall Street transactions, to enable insider trading, or as we found during the last election, inquiries in the opposing parties' political campaigns. (C.A.App. 237, ¶ 51).

D. Four federal circuit courts have held that plaintiffs have standing in collection cases, such as this case.

First, at least four federal circuit courts have held that plaintiffs have standing in collection cases, such as this. Each of these cases is discussed below.

1) Ninth Circuit.

In *Jewel v. NSA*, 673 F.3d 902 (9th Cir. 2011), a group of citizens sued the NSA, objecting to the agency's collection of e-mail through a communication facility in the San Francisco area.

The District Court in *Jewel* initially found that the plaintiffs did not have standing. However, on appeal, the Ninth Circuit found that the plaintiffs *had standing* to challenge the government's collection of e-mail. In reaching this conclusion, the court *rejected* the government's contention that there is heightened standing requirement in national security cases:

Article III imposes no heightened standing requirement for the often difficult cases that involve constitutional claims against the executive involving surveillance. See *Amnesty Int'l*, 638 F.3d at 149 ("We do not see any reason why the law of standing should be stricter or different in the surveillance context.").

Jewel, 673 F.3d at 913.

2) Second Circuit.

In 2014, the U.S. Court of Appeals for the Second Circuit reached a similar conclusion in *ACLU v.*

Clapper, 785 F.3d 787, *801; 2015 U.S. C.A.App. LEXIS 7531, **27 (2d Cir. 2014).

In that case, the American Civil Liberties Union filed suit to enjoin the government's collection of telephone metadata. The trial court, sitting in the Southern District of New York, found that the ACLU *had standing* to challenge the government's collection activities. *ACLU v. Clapper*, 959 F. Supp. 2d 724, 738 (S.D.N.Y. 2013).

On appeal, the U.S. Court of Appeals for the Second Circuit affirmed, and found that the ACLU had standing to challenge the government's collection of metadata. The Court explained its reasoning as follows:

Appellants in this case have . . . established standing to sue, as the district court correctly held. Appellants here need not speculate that the government has collected, may in the future collect, their call records. . . . It is not disputed that the government collected telephone metadata associated with the appellants' telephone calls. The Fourth Amendment protects against unreasonable searches and seizures. Appellants contend that the collection of their metadata exceeds the scope of what is authorized by § 215 and constitutes a Fourth Amendment search. . . . Whether or not such claims prevail on the merits, appellants surely have standing to allege injury from the collection, and maintenance in a government database, of records relating to them.

ACLU v. Clapper, 785 F.3d 787, *801 (2d Cir. 2014) (emphasis added).

3) Fourth Circuit.

In 2017, the U.S. Court of Appeals for the Fourth Circuit held that the Wikimedia Foundation had standing to sue the National Security Agency, in a case alleging bulk collection of e-mail and text messages. *Wikimedia Foundation v. National Security Agency*, 857 F.3d 193 (4th Cir. 2017). The Fourth Circuit summarized its conclusion as follows:

[Wikimedia's] allegations are sufficient to make plausible the conclusion that the NSA is intercepting, copying, and reviewing at least some of Wikimedia's communications. To put it simply, Wikimedia has plausibly alleged that . . . the NSA seizes all of the communications along at least one of those roads. Thus, at least at this stage of the litigation, Wikimedia has standing to sue for a violation of the Fourth Amendment.

Id. at 211. In a dissent, Justice Davis indicated that he would have *granted standing to all of the Plaintiffs* in the case, and not just to Wikimedia. *Id.* at 217.

4) D.C. Circuit.

Finally, in 2013, the U.S. Court of Appeals for the District of Columbia found that a plaintiff had standing in another case, identical to this case. In *Klayman v. Obama*, 957 F. Supp. 2d 1, 27 (D.D.C. 2013), several private citizens sued the federal government, seeking an injunction on the government's collection of telephone metadata. The District Court Judge, the Honorable Richard Leon, found that the plaintiffs had standing:

Put simply, the Government wants it both ways. Virtually all of the Government's briefs and arguments to this Court explain how the Government has acted in good faith to create a comprehensive metadata database that serves as a potentially valuable tool in combating terrorism — in which case, the NSA must have collected metadata from Verizon Wireless, the single largest wireless carrier in the United States, as well as AT&T and Sprint, the second and third-largest carriers.

Klayman, 957 F. Supp. 2d at 27, 2013 U.S. Dist. LEXIS 176925, at 67-68. Judge Leon therefore rejected the government's reasoning, and found that the plaintiffs had standing.

On appeal, a plurality of justices on the D.C. Circuit agreed that the plaintiffs had standing, at least for purposes of limited discovery to determine whether the plaintiffs' records were being collected by the government. *Obama v. Klayman*, 800 F.3d 559 (D.C. Cir. 2015) ("On remand it is for the district court to

determine whether limited discovery to explore jurisdictional facts is appropriate.”).

The federal circuit courts are therefore attuned to the dangers posed by Respondents’ conduct, and are engaged on these issues. It is therefore proper for the Court to grant a writ of certiorari in this case, and review the Respondents’ activities.

E. The Privacy and Civil Liberties Board did not ratify Respondents’ collection activities.

In its opinion, the Third Circuit argued that Respondents’ collection activity had already been reviewed and vetted by the Privacy and Civil Liberties Oversight Board (the “PCL Board”).

It is proper for the Court to reject this conclusion.

During 2013 and 2014, the PCL Board interviewed a number of people, in connection with the subjects described herein. These included Schuchardt’s expert witness, William Binney.

On July 2, 2014, the PCL Board issued a report concerning the scope and legality of Respondents’ bulk collection of e-mail.

In that report, the Board expressed significant concern about the scope of Respondents’ collection activities.

First, the Board admitted that it did not have accurate information concerning the scope of Respondents’ bulk collection. Specifically, the Board stated as follows:

The government is presently unable to assess the scope of the incidental collection of U.S. person information under the program. For this reason, the Board recommends several measures that together may provide insight about the extent to which communications involving U.S. persons or people located in the United States are being acquired and utilized.

Report of the Privacy & Civil Liberties Board, at 10 (2014) (emphasis added). In other words, Respondents refused to admit -- even to its own board of inquiry -- how much e-mail it was collecting under the program.

Second, the Board did not find Respondents' activities to be constitutional. Specifically, the Board stated as follows:

The Board has found that certain aspects of the program's implementation raise privacy concerns. These include the scope of the incidental collection of U.S. persons' communications and the use of queries to search the information collected under the program for the communications of specific U.S. persons. The Board offers a series of policy recommendations to strengthen privacy safeguards and to address these concerns.

PCL Board Report, at 2 (emphasis added).

In light of these conclusions, it is proper for the Court to grant a writ of certiorari in this case, to review Respondent's collection activities.

CONCLUSION

This case poses a question of vital importance to every single American.

For the first time in human history, a small group of persons within the executive branch of the federal government has the power to read the private electronic communications of every person in our society. This is being done by means of a database of collected e-mail communications.

It is time to move this database back to where it belongs -- the internet service providers. This will ensure that access to the database is limited to persons who have obtained a warrant, as required by the 4th Amendment of the United States Constitution.

This can be done safely, and for the protection of all concerned. The documents in the database would still exist and would remain available for review by the appropriate authorities. The database could still be searched and accessed real time -- but only upon a finding of *probable cause* made by a court. This will ensure that the system will not be abused.

Seventy-five years ago, Justice Felix Frankfurter of this Court warned the American people of the importance of enforcing the 4th Amendment. He said:

This Court has thus far jealously enforced the principle of a free society secured by the prohibition of unreasonable searches and seizures. . . . It is not only under Nazi rule that police excesses are inimical to freedom. It is easy to make light of insistence on scrupulous regard

for the safeguards of civil liberties when invoked on behalf of the unworthy. It is too easy. History bears testimony that by such disregard are the rights of liberty extinguished, *heedlessly at first*, then stealthily, and brazenly in the end.

Davis v. United States, 328 U.S. 582, 597, 66 S. Ct. 1256, 1263, 90 L. Ed. 1453, 1462 (1946) (emphasis added).

Let us heed his words, while there is still time to do so.

* * *

WHEREFORE, for the reasons set forth above, the Petitioner, Elliott J. Schuchardt, respectfully requests that this Honorable Court enter an order granting a writ of certiorari in this case.

Respectfully submitted,

Elliott J. Schuchardt
SCHUCHARDT LAW FIRM
6223 Highland Place Way
Suite 201
Knoxville, TN 37919
(865) 304-4374
elliott016@gmail.com

Appearing Pro Se