No. 19-7408

ORIGINAL

IN THE

SUPREME COURT OF THE UNITED STATES

Daniel J. Bowman — PETITIONER
(Your Name)

vs.

United States — RESPONDENT(S)

ON PETITION FOR A WRIT OF CERTIORARI TO

UNITED STATES COURT OF APPEALS FOR THE SIXTH CIRCUIT
(NAME OF COURT THAT LAST RULED ON MERITS OF YOUR CASE)

PETITION FOR WRIT OF CERTIORARI

DANIEL JAY BOWMAN
(Your Name)

FSL Elkton P.O. Box 10
(Address)

Lisbon, OH 44432
(City, State, Zip Code)

N/A
(Phone Number)

QUESTION(S) PRESENTED

Whether the Government's use of "Parallel Construction" to prosecute citizens violates their 4th and 5th Amendment rights.

LIST OF PARTIES

[x] All parties appear in the caption of the case on the cover page.

[ ] All parties **do not** appear in the caption of the case on the cover page. A list of all parties to the proceeding in the court whose judgment is the subject of this petition is as follows:

TABLE OF CONTENTS

INDEX TO APPENDICES

TABLE OF AUTHORITIES CITED

IN THE

SUPREME COURT OF THE UNITED STATES

PETITION FOR WRIT OF CERTIORARI

Petitioner respectfully prays that a writ of certiorari issue to review the judgment below.

OPINIONS BELOW

[X] For cases from **federal courts**:

The opinion of the United States court of appeals appears at Appendix A to the petition and is

[ ] reported at _____; or,
[X] has been designated for publication but is not yet reported; or,
[ ] is unpublished.

The opinion of the United States district court appears at Appendix B to the petition and is

[ ] reported at _____; or,
[X] has been designated for publication but is not yet reported; or,
[ ] is unpublished.

[ ] For cases from **state courts**:

The opinion of the highest state court to review the merits appears at Appendix _____ to the petition and is

[ ] reported at _____; or,
[ ] has been designated for publication but is not yet reported; or,
[ ] is unpublished.

The opinion of the _____ court appears at Appendix _____ to the petition and is

[ ] reported at _____; or,
[ ] has been designated for publication but is not yet reported; or,
[ ] is unpublished.

JURISDICTION

[X] For cases from **federal courts**:

The date on which the United States Court of Appeals decided my case was 11/12/19.

[X] No petition for rehearing was timely filed in my case.

[ ] A timely petition for rehearing was denied by the United States Court of Appeals on the following date: _____, and a copy of the order denying rehearing appears at Appendix _____.

[ ] An extension of time to file the petition for a writ of certiorari was granted to and including _____ (date) on _____ (date) in Application No. ___A_____.

The jurisdiction of this Court is invoked under 28 U. S. C. § 1254(1).

[ ] For cases from **state courts**:

The date on which the highest state court decided my case was _____. A copy of that decision appears at Appendix _____.

[ ] A timely petition for rehearing was thereafter denied on the following date: _____, and a copy of the order denying rehearing appears at Appendix _____.

[ ] An extension of time to file the petition for a writ of certiorari was granted to and including _____ (date) on _____ (date) in Application No. ___A_____.

The jurisdiction of this Court is invoked under 28 U. S. C. § 1257(a).

CONSTITUTIONAL AND STATUTORY PROVISIONS INVOLVED

AMENDMENT 5

No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a Grand Jury, except in cases arising in the land or naval forces, or in the Militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offence to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation.

AMENDMENT 6

In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the Assistance of Counsel for his defence.

STATEMENT OF THE CASE

."Parallel construction" is the process of sanitizing "dirty" information obtained by the intelligence community known as "Five Eyes", (Five Eyes consists of the intelligance agencies in the U.S.A., Canada, United Kingdon, Austrailia and New Zealand.) and "cleaning it up" by fabricating a narrative the Courts will likely find plausible. This is an example of such a case.

The Government's story in this case is technically implausible. They claim to have linked disperate data streams (e-mails) to the petitioner via human investigation, performed by FBI Special Agent Daniel O'Donnell, FBI investigative Support Specialist Kristen Mueller and FBI Special Agent Cristin McCaskill.

In sum, their story is that in January of 2012 Cybertip 1299337 was reported to the National Center for Missing and Exploited Children (NCMEC). This tip led to them determining that a person using the e-mail address joeyme06@gmail.com from IP 24.165.196.194 had violated 18 U.S.C. §§2252 and 2252A.

Then in February, Time Warner cable provided them with the name and address of the possible offender, Teresa Butner in Ravenna Ohio. This was enough to obtain a search warrant for her address, but our team of investigators didn't do that, instead they did nothing, and waited five months.

In March, the Queensland Police Service (QPS) arrested an Austrailian citizen using a Microsoft Hotmail account to distribute Child Pornography (CP), and this is when the government's story becomes implausible. They claim that in July of 2012, Special Agent (SA) O'Donnell flew to Austrailia to review 111 e-mail accounts they suspected were accessed from within the United States, that communicated with the Austrailian citizen. This claim in not plausible because there is no reason for SA O'Donnell to fly to Austrailia to perform this work. He has a high speed internet connection in his office in Maryland and could review the QPS information, instead of spending 3 months in Austrailia supposedly analyizing this data. This narrative was added to explain the five month delay.

Regardless of where SA O'Donnell analyized the QPS data, his path to joey006@lavabit.com is not credible and should be rejected by this Court, as the path is too long, convoluted (see Appendix C paragraph 6-30) and obviously fabricated.

To understand why, this Court must accept the fact that the FBI routinely engages in unconstitutional activity. As reported by Brad Miller in **THE AMERICAN PROSPECT** Magazine (fall 2019), the FBI has a "Total Information Awareness" program to "collect and correlate information to identify relationships between individuals, locations and events that may be indicators of terrorist or other activities of interest." Brad Miller is

not a Journalist, he was a congressman (from 2003 to 2013) and chair of the House's Science Investigation and Oversight Subcommities, so the Court should give his reporting considerable weight. He shows that Congress eliminated funding for the FBI's program from the DOJ's appropriation in 2007; but, he doubts the program died. He states "the Bush administration claimed power to divert funds appropriated by Congress from approved programs to secret programs not approved or even forbidden by Congress." Mr. Miller concludes "DOJ almost certainly moved the program to a 'dark' part of the FBI's budget."

The Executive's branches use of secret systems to prosecute citizans should not be allowed to continue; thus, this petition for Certiorari.

REASONS FOR GRANTING THE PETITION

REASON ONE

The evidense strongly suggests the FBI's PRISM system was used for this prosecution. As the Court in SCHUCHARDT vs. THE PRESIDENT OF THE UNITED STATES (Civil Action # 14-705) explained on 9-30-2015: In order to properly contextualize the factual claims in this litigation, a brief overview of several pertinent statutes is warranted. In 1978, Congress enacted the Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801 et seq. ("FISA"), to "authorize and regulate certain governmental electronic surveillance of communications for foreign intelligence purposes." Clapper v. Amnesty int'l USA, U.S._, 133 S. Ct. 1138, 1143, 185 L. Ed. 2d 264 (2013). FISA provided a procedure for the federal government to legally obtain domestic electronic surveillance related to foreign targets, see 50 U.S.C. §§ 1804(a)(3) & 1805(a)(2), and created an Article III court-the Foreign Intelligence Surveillance Court ("FISC") - with jurisdiction "to hear applications for and grant orders approving" such surveillance. 50 U.S.C. § 1803(a)(1).

In the wake of the terrorist attacts of September 11, 2001, Congress passed the USA PATRIOT Act, Pub. L. No. 107-56, § 215, which, inter alia empowered the FBI to seek authorization from the FISC to "require[e] the production of any tangible

things (including books, records, papers, documents, and other items) for an investigation . . . to protect against international terrorism." 50 U.S.C. 1861(a)(1). Since 2006, the government has relied on this provision "to operate a program that has come to be called 'bulk data collection,' namely, the collection, in bulk, of call records produced by telephone companies containing 'telephony metadata' - the telephone numbers dialed (incoming and outgoing), times, and durations of calls." See Obama v. klayman, 800 F.3d 559, 2015 U.S. App. LEXIS 15189, 2015 WL 5058403 (D.C. Cir. Aug. 28 2015) ("KlaymanII").

in 2008, Congress amended FISA by way of the FISA Amendments Act ("FAA"), Pub. L. No. 110-261 (2008). The pertinent FAA provision, section 702 of FISA, 50 U.S.C. § 1881a, "supplement[ed] pre-existing FISA authority by creating a new framework under which the Government may seek the FISC's authorization of certain foreign intelligence surveillance targeting. . . non-U.S. persons located abroad." Amnesty Int'l, 133 S. Ct. at 1144. The government relies upon the authority granted by Section 702 to collect internet data and communications through a program called "PRISM." 2d Am. Compl. (Doc. 19) ¶¶ 33, 35.

American citizens first learned of the government's bulk data collection programs through a series of articles published

in The Guardian, a British newspaper, in June of 2013. Id. Each article relied on leaked documents provided by a former NSA government contractor, Edward Snowden. Id. ¶¶ 24-27, 33-39. The first of these articles, published on June 5, 2013, revealed a leaked order from the FISC directing Verizon Business Network Services, Inc. ("Verizon Business") to produce "call detail records or 'telephony metadata" to the NSA for all telephone calls made through its systems within the United States (including entirely-domestic calls). Id. ¶ 33. Shortly thereafter, the government acknowledged that the FISC order was genuine and that it was part of a broader program of bulk collection of telephone metadata. Id. ¶ 34; ACLU v. Clapper, 785 F. 3d 787, 796 (2nd Cir. 2015).

The following day, June 6, 2013, The Guardian published a second article detailing the manner in which the PRISM collection program was used to intercept, access and store e-mail and other internet data created by United States citizens using large internet companies, such as Yahoo, Google, Facebook, Dropbox and Apple. Id. ¶¶ 35-38. According to the leaked documents, the government began collecting information from, inter alia, Yahoo on March 12, 2008; from Google on January 14, 2009 from Facebook on June 3, 2009; and from Apple in October 2012. Id. ¶ 39. discussing the scope of the governments data collection abilities,

Snowden, in a series of public statements and interviews, averred that he could search, seize, and read anyone's electric communications at any time from his desk during his time working with the NSA. Id. ¶¶ 45-46.

Since those revelations, several former NSA employees and whistleblowers have stepped forward to supply further details concerning the scope and breadth of the government's data collection programs. 1 William Binney, former senior employee of the NSA, stated that the NSA used a computer program to collect and search domestic internet traffic, a process known as "data mining." Id. ¶¶ 9,19. Mark Klein, a former AT&T technician, 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 Id. ¶ 13. Thomas Drake, another NSA employee, asserted that the NSA has been, or may be, obtaining the ability to seize and store "most electric comunications." Id. 20. A third former NSA employee, Kirk Wiebe, corroborated the allegations made by Drake and Binny. Id. ¶ 21.

The petitioner believes that, unlike Schuchardt, these facts give him standing to challenge his conviction soley based on "PRISM." (Count 1) thus providing an execllant reason to grant the writ.

REASON TWO

18 U.S.C. 2255A prosecutions exploded after 2004. The Prison's Lexus/Nexus database returns the following information: In Second Circuit District Courts prosecutions went from 79 (2000-2006) to 270 (2007-now). In the Third, they went from 13 (1994-2004) to 168 (2005-now). In the Fourth, they went from 0 (2000-2003) to 304 (2004-now). In the Sixth, they went from 1 (pior to 2004) to 406 (2004-now). And as a final example, they went from 20 (before 2007) to 371 (2007-now) in the Ninth.

The only exception to this trend occured in the Tenth Circuit, where prosecutions went from 0 in 1998 to 128 (1999-now). The petitioner believes this fact provides strong circumstancial evidence the FBI developed its "parallel construction" project in the states covered by the Tenth Circuit. For example, review U.S. v. Kennedy, Kansas District Court case #99-10105-01 where the Court recounted these facts: on July 2, 1999, Steven Idelman was working as a customer support specialist for Road Runner, a high speed internet service provider. At approximately 9:00 p.m., Idelman received an anonymous phone call from a still-unidentified male ("the caller"). The caller told Idelman that he was at a friend's house, scanning other computers through the internet and had viewed images of child pornography on a computer the caller believed to be

serviced by Road Runner. The caller told Idelman the IP address of the computer from which the images were viewed, 24.94.200.54, and the directory and file names in which the images were located. The caller did not say he was a law enforcement officer or that he was directed to view the computer's files by any law enforcement officer. The caller did not ask Idelman to call the police.

Shortly after the anonymous call, Idelman went to a computer and accessed the IP address given to him by the caller. His purpose was to determine if what the caller told him was correct. He located the computer with the IP address 24.94.200.54 and the directory tree and files mentioned by the caller. Idelman viewed two images located within those files. One of the images depicted two boys, whom Idelman estimated to be approximately eight or nine years old, posed in sexual nature. Idelman then sent an e-mail to his supervisor, Anna Madden, describing the anonymous phone call and the results of his search of the computer with IP address 24.94.200.54.

(2000 U.S. Dist. Lexis 5) that same day, after consulting with Road Runner's corporate attorney Scott Petrie, the manager of Road Runner, made the decision to contact law enforcement authorities. Kerry Jones contacted the Exploited Children's unit of the Wichita Police Department, but his phone call

was not returned. Road Runner then contacted Special Agent Leslie Earl of the FBI. Special Agent Earl was informed by Road Runner that the FBI would need to obtain a court order for it to be able to supply the FBI with any subscriber information.

Unlike the Kansas Court, this court should ask the obvious question; "who provided the anonymous tip?" and grant the writ to find out.

REASON THREE

The Doj is using "Five Eyes" intelligence to prosecute U.S. citizens for various crimes. The government claims, for example, that the following five cases were initiated by "tips" from "foreign law enforcement" and/or "server misconfiguration", both claims are not credible per the axiom of "Occam's Razor", where when faced with two explainations for phenomenon, accept the simpler explaination; in these cases, "Five Eyes" intelligence:

1.) U.S. v. McGrath - Nebraska District Court (2014).
2.) U.S. v. Defoggi - 8th Cir. Case No. 15-1209.
3.) U.S. v. Ulbricht - 2nd Cir. Case No. 15-1815.
4.) U.S. v. Chase 4th Cir. District Court Case No. 5:15-CR15.
5.) U.S. v. Farrell Western District of Washington Case No. 2:15-CR-29

Mr. Farrell got closest to exposing the "Five Eyes" facts during his motion to compel. And he may have exposed it,

as his case's only document in Lexus/Nexus is the order denying his motion. In it, the Court reveals that the FBI claimed to have learned of his IP address (that was used to access the administrations section of the silk road 2.0 website) by getting it (by subpoena) from a computer research lab at Carnegie Mellon University (CMU). This is clearly "parallel construction". CMU's lab was funded by the DOD; thus the NSA would know about it and passed this information on to the DOJ. The lab's researchers were scheduled to give a presentation about their technique to a conference that year, but the DOD blocked them from doing so and the story died and Mr. Farrell's case disappeared.

Since concealing the use of "Five Eyes" surveilance is a violation of citizens 4th and 5th Amendment Rights, this fact provides an execllent reason for granting this writ.

CONCLUSION

Unlike in Schuchardt vs. The President of the United States, the government cannot claim the petitioner lacks standing to challenge the illegal and unconstitutional method(s) used to prosecute him. In this case, it is almost certain that Prism surveillance was used against him and that he was harmed by it.

The central allegation is simple, the NSA is intercepting, monitoring and storing the content of all electronic comunications of American citizens and letting the FBI access their database to prosecute citizens and hiding this fact with false naratives. That is serious misconduct and this court should address it.

The petition for a writ of certiotari should be granted.

Respectfully submitted,

Daniel Bowman

Date 12-18-2019

APPENDIX A