No. 18-

IN THE

Supreme Court of the United States

KEITH PRESTON GARTENLAUB,
AKA Keith Preson Gartenlaub,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

ON PETITION FOR A WRIT OF CERTIORARI TO THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT

PETITION FOR A WRIT OF CERTIORARI

TOR EKELAND
Counsel of Record
MARK JAFFE
LYDIA FIELDS
TOR EKELAND LAW PLLC
195 Montague Street, 14th Floor
Brooklyn, NY 11201
(718) 737-7264
tor@torekeland.com

Counsel for Petitioner

287073

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

QUESTIONS PRESENTED

(1) Does a secret, Foreign Intelligence Surveillance Act ("FISA") authorized computer search violate the Fourth Amendment's prohibition against general warrants when the government searches every file on a hard drive in the name of national security?

(2) Does the Fourth Amendment impose use restrictions on non-responsive evidence of regular, non-national security crimes, obtained from a FISA computer search?

(3) Whether the District Court's Denying Gartenlaub a *Franks* Hearing on the secret FISA Warrant Requires Suppression of the Fruits of that Warrant?

(4) Does the fact that Gartenlaub wasn't allowed to investigate, and adversarially challenge, the secret FISA search warrant application and materials used against him violate the Fourth, Fifth, and Sixth Amendments' fundamental criminal procedure protections?

(5) Did the District Court err in denying Gartenlaub's post-trial motion for a judgment of acquittal because the jury never heard the secret FISA evidence, and Gartenlaub never got to challenge it or argue it to the jury, thereby giving the Jury an insufficient picture of the evidence to convict?

TABLE OF CONTENTS

Table of Contents

TABLE OF APPENDICES

TABLE OF CITED AUTHORITIES

Page

CASES

Page

Cited Authorities

Page

STATUTES AND OTHER AUTHORITIES

Cited Authorities

Page

Page

OPINIONS BELOW

On September 6, 2016, after a jury trial, the Federal District Court for the Central District of California entered judgment against Petitioner Keith Preston Gartenlaub.[1] The court entered judgment against Gartenlaub for one count of 18 U.S.C. §§ 2252A(a)(5)(B) and 2252A(b)(2), possession of child pornography.[2] On October 2, 2018, in an unpublished five-page decision, the United States Court of Appeals for the Ninth Circuit affirmed the District Court's judgment.[3] On December 7, 2018, the United States Court of Appeals for the Ninth Circuit denied Mr. Gartenlaub's petition for rehearing *en banc*.[4]

JURISDICTION

On September 6, 2016, the District Court, having jurisdiction under 18 U.S.C. § 3231, entered judgment. On October 2, 2018, the Ninth Circuit affirmed the District Court's judgment. On December 7, 2018, the Ninth Circuit entered its order denying rehearing *en banc*. The Ninth Circuit had jurisdiction under 28 U.S.C. § 1291.

---

1. (App. at 6a-15a); (District Ct. Dkt. No. 216 (*United States v. Keith Preston Gartenlaub*, 14-CR-00173-CAS (C.D. Ca.).)

2. (App. at 7a.)

3. (App. at 1a-5a.)

4. (App. at 16a-17a; (*United States v. Keith Gartenlaub*, No. 16-50339 (9th Cir. 2018), (Appeal Dkt. No. 96.).)

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS

The Fourth Amendment to the United States Constitution reads:

> 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.

The Fifth Amendment to the United States Constitution reads in relevant part "[n]o person shall be . . . be deprived of life, liberty, or property, without due process of law . . . ."

The Sixth Amendment to the United States Constitution reads in relevant part: "[i]n all criminal prosecutions, the accused shall enjoy the right to . . . 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."

The relevant portions of the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. §§ 1804-6, 1821-25, are in the Appendix.

STATEMENT OF THE CASE

In 2013, Wesley Harris, an FBI agent in Los Angeles, read an article on Wired.com.[5] The article speculated that a spy at the Boeing Company, the designer and manufacturer of the U.S. Military's C-17 cargo plane, may have leaked the C-17's blueprints to the Chinese.[6] It suggested that the Chinese Military's Y-20 cargo plane was based on the stolen C-17 blueprints. After reading a second article speculating that "hackers" may have compromised the Boeing C-17 program, Agent Harris launched an investigation.[7] For reasons never revealed, the investigation targeted Petitioner Keith Preston Gartenlaub, a U.S. citizen, who at the time was an Engineering IT Manager at Boeing in Long Beach, California. No evidence exists, then or now, that

---

5. (ER 378.) The following abbreviations refer to appellate filings in *United States v. Keith Preston Gartenlaub*, No. 16-50339 (9th Cir.): "ER" refers to Excerpts from the Record (9th Cir. Dkt. No. 32); "AOB" refers to Appellant's Opening Brief (*Id. at* 31); "GB" refers to the Government's Opposition Brief (*Id. at* 53); "ARB" refers to the Appellant's Reply Brief (*Id.* at 63); "BAC" refers to Brief of Amici Curiae Electronic Frontier Foundation and American Civil Liberties Union in Support of Defendant- Appellant And Reversal (*Id.* at 34). All record cites are in parenthesis.

6. (ER 379.) A previous version of the Wired.com article, published in December 2012, identified the potential Boeing spy as Dongfan Chung. https://www.wired.com/2012/12/china-debuts-giant-transport/. Chung was convicted in 2010 of providing Boeing trade secrets to China (although the conviction did not involve the C-17), and the Ninth Circuit affirmed in 2011. *See U.S. v. Chung*, 659 F.3d 815 (9th Cir. 2011).

7. (ER 378; AOB at 5.)

Gartenlaub provided C-17 designs to China. He has never been charged with any national security crimes.

In July 2016, Chinese Citizen Su Bin was sentenced for his role in plotting to steal the C-17 military cargo plane designs.[8]

Agent Harris's investigation latched onto two principal facts: that Gartenlaub's position at Boeing allegedly gave him access to C-17 data; and, that Gartenlaub's wife, a naturalized U.S. citizen, was born in China. Understandably, Gartenlaub travelled to China and communicated with his family there. He also jointly owned property in China with his wife. Gartenlaub hid none of this.

Gartenlaub disclosed his Chinese travel to Boeing and received its approval. And Agent Harris knew this. He knew that Gartenlaub's communications with China had nothing to do with the C-17 and were explained by his family there. He knew that numerous employees could access Boeings C-17 data. Nonetheless, Agent Harris used Gartenlaub's alleged access—which Harris misunderstood and exaggerated—his Chinese-born wife, and other innocuous facts to concoct a fantasy of Gartenlaub as a Chinese spy.

Agent Harris's investigation was one of many launched at the time under intense pressure on the FBI and DOJ

8. *See, e.g.,* Matt Hamilton, *Chinese Citizen is Sentenced to Prison in the U.S. for Plotting to Steal Military Secrets,* L.A. Times, July 13, 2016, available at http://www.latimes.com/local/lanow/la-me-ln-chinese-boeing-hack-prison-sentencing-20160713-snap-story.html.

to take action against Chinese espionage targeting U.S. military and trade secrets. This pressure led to questionable investigations and prosecutions. Regional DOJ offices used secret FISA search warrants to start several non-national security prosecutions for regular crimes. Many of these prosecutions collapsed for reasons including false evidentiary assumptions and accusations of racism against Chinese Americans.[9]

In November, 2015, these accusations of DOJ racism against Chinese Americans led the U.S. Commission on Civil Rights to send a letter to U.S. Attorney General Loretta E. Lynch asking for an investigation into the targeting of "Asian Americans for investigation, surveillance, and arrest, due to their race or national origin."[10] Eventually, the DOJ's main office in Washington, D.C. addressed these accusations of racially motivated national security investigations.

In 2016, DOJ in Washington, D.C. issued new guidelines governing national security investigations under the Foreign Intelligence Surveillance Act ("FISA"). The guidelines require regional DOJ prosecutors to

---

9. *See, e.g.,* Matt Apuzzo, *Former Espionage Suspect Sues, Accusing F.B.I. of Falsifying Evidence*, N.Y. Times, May 10, 2017 ("Each case raised the specter of Chinese espionage without explicitly charging the suspects as spies."), available at https://www.nytimes.com/2017/05/10/us/politics/fbi-xi-xiaoxing.html.

10. Letter from the United States Commission on Civil Rights to Loretta E. Lynch, United States Attorney General (Nov. 18, 2015) (documenting dubious DOJ espionage investigations targeting Asian Americans), available at https://www.usccr.gov/press/archives/correspd/LettertoDOJreAsianAmericanProsecutions.pdf.

consult with national security prosecutors in Washington, D.C., before proceeding.[11]

But in 2013, these guidelines didn't exist. And, initially, Agent Harris didn't turn to FISA in his hunt for Chinese spies. In June 2013, Agent Harris's applied under Federal Rule of Criminal Procedure 41 ("Rule 41") in the Federal District Court for the Central District of California in Los Angeles for a criminal search warrant targeting Gartenlaub's and his wife's emails for evidence of espionage.[12] The court approved the warrant. The subsequent search of the Gartenlaubs' emails turned up no evidence of national security crimes, or any crimes whatsoever.

Undaunted, Agent Harris applied to the top secret, *ex parte* Foreign Intelligence Surveillance Court for a secret search warrant under FISA.

In 1978, Congress passed FISA because for decades the FBI and CIA engaged in illegal regular surveillance of, and action against, U.S. citizens. Congress intended FISA, and the Foreign Intelligence Surveillance Court, to prevent these abuses of power by federal law enforcement and intelligence agencies. The most infamous abuse being the FBI's COINTELPRO activities that politically

---

11. *See, e.g.,* Tim Cushing, *DOJ Issues New Rules On Espionage Investigations to Keep it From Embarrassing Itself So Often*, Techdirt, May 2, 2016, available at https://www.techdirt.com/articles/20160428/08364934298/doj-issues-new-rules-espionage-investigations-to-keep-it-embarrassing-itself-so-often.shtml.

12. (*See* AOB at 7.)

targeted Americans like Martin Luther King, Jr.[13] Thus, FISA limits searches targeting U.S. citizens to instances where there is probable cause that the citizen is an agent of a foreign power.[14] The holds true whether for targeted surveillance, or a targeted physical search.[15] No such evidence exists in the public record that Gartenlaub was a foreign agent and he's never been charged with a national security crime.

The Foreign Intelligence Surveillance Court approved Agent Harris's secret warrant application, presumably for the surveillance of Gartenlaub and a physical search of his home, computers and hard drives.[16]

The FBI Secretly Enters Gartenlaub's Home and Images His Hard Drives

On January 29 and 30, 2014, FBI agents stealthily entered Gartenlaub's home to execute a secret FISA

---

13. *See, e.g.,* S. Rep. No. 94-755, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, at 11 (April 26, 1976) ("The Church Report") ("[T]he Committee's investigation has uncovered a host of serious legal and constitutional issues relating to [domestic] intelligence activity and it is strong proof of the need for reform to note that scarcely any of those issues have been addressed in the courts."), available at https://upload.wikimedia.org/wikipedia/commons/7/79/Church_Committee_report_%28Book_I%2C_Foreign_and_Military_Intelligence%29.pdf.

14. *See* 50 U.S.C. § 1804 (a)(3)(A).

15. *Compare* 50 U.S.C. § 1804 (surveillance) *with* 50 U.S.C. § 1823 (physical searches).

16. (*See* AOB at 7.)

physical search warrant. Agents secretly searched and digitally imaged three hard drives they found there. Over the following months, the FBI rummaged through every file they found on those hard drives.

In its Opposition Brief before the Ninth Circuit, the government acknowledges that there were no limitations to its secret search of Gartenlaub's hard drives, saying in a header: "The Government Was Permitted to Search Every File on Defendant's Computers . . . ."[17] And nothing in the record indicates that the government used any standard forensic techniques routinely used to particularize computer searches like: date limitations; targeted key word searches; image recognition scans; taint teams, or other routine, well established techniques to limit a digital search to its target and screen out privileged, confidential, and irrelevant information.

Despite its unlimited search, the FBI found no evidence that Gartenlaub had provided C-17 data to China, or otherwise acted as a spy for China. But the FBI did allegedly find, among the tens of thousands of files on the hard drives, a handful of files containing child pornography. Dropping its fantasy that Gartenlaub was a Chinese spy, the FBI turned to the theory he collected child pornography.

The Fed. R. Crim. P. 41 Warrants Based on the Fruits of the FISA Warrant

In August 2014, the FBI obtained a search warrant for Gartenlaub's premises seeking evidence that he

17. (*See* GB at 52.)

received and possessed child pornography.[18] The August 2014 warrant application based its probable cause on the fruits of the secret FISA warrant secretly executed in January 2014, describing it as "a court-authorized search without notice" to the occupants. The probable cause affidavit further stated that the search discovered child pornography on Gartenlaub's hard drives.[19] The district court then granted the application for a normal Rule 41 search warrant.

With its August 2014 search warrant the FBI seized the three hard drives that it had already secretly imaged and searched for months under the FISA warrant. It also seized a fourth hard drive from Gartenlaub that contained a copy of the "Origdata" folder structure that allegedly contained the same files as the other three hard drives.

On October 23, 2014, a grand jury indicted Gartenlaub for receipt and possession of child pornography in violation of 18 U.S.C. §§ 2252A(a)(2) and 2252A(a)(5).[20]

Through pretrial motions, he:

1. Challenged and sought suppression of the fruits of the January 2014 FISA search and the August 2014 searches of his home, computers, and hard drives, on Fourth Amendment and other grounds,

2. Requested a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), to establish that the FISA

18. (ER 243.)

19. (ER 248-49.)

20. (*See* ER 243, 248-49, 296-97; AOB at 7).

application, and the August 2014 search warrant application contained intentional or reckless material falsehoods and omissions, and

3. Sought disclosure of the underlying FISA application and order.[21]

In response, the government submitted a largely classified, *ex parte* opposition to Gartenlaub's FISA challenges.[22] The defense received a heavily redacted version of the government's opposition. The District Court reviewed the FISA application and order, together with the classified portions of the government's opposition, *in camera* and *ex parte*.

On August 6, 2015, in an 11-page opinion drafted by the government that the District Court signed unaltered, the court refused to disclose to the defense the FISA application and order, and denied Gartenlaub's motion to suppress the fruits of the FISA search.[23] Later, however, the court expressed misgivings, stating "I do have some personal questions regarding the propriety of the FISA court proceeding even though that certainly seems to be legally authorized."[24]

An enormous folder on Gartenlaub's drives with multiple subfolders called "Origdata" contained less than 100 child pornography files among thousands of other files.

---

21. (District Ct. Dkt. Nos. 67, 70, 73.)

22. (District Ct. Dkt. No. 82.)

23. (ER 21, 321.)

24. (District Ct Tr. at 9-10 (4/18/16).)

The exact number isn't clear. A review by the National Center for Missing and Exploited Children identified 22 files. An additional 70 or so alleged child pornography files were identified by non-expert agents.[25]

The evidence at trial showed that the files date to 2005, when numerous people had access to Gartenlaub's computer.[26] No one knows who initially downloaded the files, or to what hard drive, or on to what computer initially.[27] No new files were added after 2005, nor is there any definitive evidence that any of these files were opened until the FBI opened them in 2014.[28] The child pornography files were copied—along with tens of thousands of other files in an enormous folder structure—to three other of Gartenlaub's hard drives. The files' presence on four hard drives is consistent with someone copying the entire contents of an old hard drive to a newly purchased hard drive. No evidence, such as log files, screen shots, cached data, or chat logs of Mr. Gartenlaub ever visiting any sites related to child pornography exists. Likewise, there's no evidence or testimony of any type that Gartenlaub groomed, solicited, or had sex with, minors. There is no evidence of the type that one would expect to find related to someone who collects child pornography.

---

25. (*See, e.g.,* District Ct. Tr. at 72, 92-94 (12/4/15).)

26. (*See* ARB at 1-8.); (District Ct. Tr. at 403-05, 412-16, 421-23 (12/9/15).)

27. (*See* ARB at 1.); (ER 193-95, 217)

28. (See AOB at 8.); (ER 194-95, 199-200.); (*See generally* ER 193-230 (cross-examination of government computer forensic expert Bruce Pixley).)

As the District Court stated at sentencing, this is a "one-of-a-kind" child pornography case.[29] The court noted the absence of evidence that Gartenlaub downloaded the child pornography files, the lack of evidence that the collection was ever added to from 2005 until the FBI seized it in 2014, and the lack of evidence he ever opened those files.[30]

Verdict

The jury found Gartenlaub guilty on both counts. The District Court dismissed the receipt count (Count 1) as multiplicitous.[31] On August 29, 2016, the court sentenced Gartenlaub to 41 months imprisonment and $3,430 in restitution.[32] The District Court, and the Ninth Circuit, denied Gartenlaub's motion for bail pending appeal. On February 14, 2017, he self-surrendered into custody. He currently is out on supervised release.[33]

Ninth Circuit Appeal

On appeal to the Ninth Circuit, Gartenlaub sought review of:

1. The District Court's order denying his motion for judgment of acquittal[34]

---

29. (District Ct. Tr. at 7 (8/29/16).)

30. (District Ct. Tr. at 5-7 (8/29/16).)

31. (District Ct. Dkt. No. 210.)

32. (ER 1.)

33. (District Ct. Dkt. No. 247.)

34. (ER 8.)

2. The District Court's order finding that the government's secret FISA application established probable cause to believe that Gartenlaub was an agent of a foreign power[35]

3. The District Court's refusal to order a *Franks* hearing[36] and,

4. The District Court's order denying Gartenlaub's motion for disclosure of the government's FISA application, and the Foreign Intelligence Surveillance Court's order authorizing the search of Gartenlaub's home, computers and hard drive.[37] Gartenlaub's trial counsel didn't raise the issue concerning the scope of the government's search and seizure under the Foreign Intelligence Surveillance Court Order; thus the Ninth Circuit reviewed the issue only for plain error.[38]

On October 2, 2018, the Ninth Circuit affirmed the District Court's judgment. On December 7, 2018, the Ninth Circuit, in an unpublished opinion, denied Gartenlaub's petition for rehearing *en banc*.[39]

---

35. (ER 23-24, 28.)

36. (ER 25, 29-30.)

37. (ER 25-28.)

38. (App. at 3a.)

39. (*United States v. Keith Preston Gartenlaub*, No. 16-50339 (Appeal Dkt. No. 96))

REASONS FOR GRANTING THE PETITION

This Court has never reviewed the relationship between the Fourth, Fifth, and Sixth Amendments' fundamental criminal procedure protections and the Foreign Intelligence Surveillance Act ("FISA"). The Court has only heard one FISA case, involving the NSA's bulk collection of phone metadata under FISA.

In *Clapper v. Amnesty International*, this Court reversed the Second Circuit's holding that the plaintiffs' had standing to challenge the constitutionality of FISA's surveillance provisions targeting foreigners.[40] Standing is not an issue here because this is a criminal case. The core issue here is whether the government can use secret FISA investigations and search warrants to prosecute regular, non-national security crimes, thereby bypassing, in the name of national security, the Constitution's core criminal procedural guarantees.[41]

As this Court has long recognized, the primary purpose of the Fourth Amendment is to "secure the privacies of life against arbitrary power . . . and relatedly, that a central aim of the Framers was to place obstacles in the way of a too permeating police surveillance."[42] Gartenlaub's case shows how, in the talismanic name of national security, FISA and the Foreign Intelligence Surveillance Court are contrary to this primary purpose.

---

40. *See Clapper v. Amnesty Intern. USA*, 568 U.S. 398 (2013) (holding plaintiffs lacked standing to challenge the NSA's warrantless surveillance of U.S. citizens.)

41. "Regular crimes" refers to non-national security crimes.

42. *Carpenter v. United States*, 138 S. Ct. 2206, 2213–14 (2018) (citations and internal quotation marks omitted).

The government's use of the fruits of a secret FISA search warrant to prosecute an unrelated regular crime, as happened here, is a recipe for governmental abuse. In the 33 years between 1979 and 2012, the Foreign Intelligence Surveillance Court denied only 11 secret FISA applications and granted the rest. The Foreign Intelligence Surveillance Court has a 99.97% approval rating for warrant applications.[43]

Gartenlaub's case demonstrates how easy it is to bypass the Constitution's criminal procedure guarantees by getting a secret FISA search warrant and using it to prosecute regular crimes. And it is impossible for a criminal defendant to challenge a secret FISA warrant because the defendant cannot access any of the information underlying the FISA warrant due to its secrecy. This thwarts a criminal defendant's Due Process right to test the government's case in adversarial proceedings. For these reasons alone the Court should grant certiorari to clarify the use of non-responsive FISA evidence in regular criminal proceedings.

FISA contradicts the primary purpose of the Bill of Rights criminal procedure amendments – the Fourth, Fifth, and Sixth – in the name of national security. The primary purpose of curtailing arbitrary police power and pervasive government surveillance of citizens.[44] Using

---

43. *See* Conor Clarke, *Is the Foreign Intelligence Surveillance Court Really a Rubber Stamp?* 66 Stan. L. Rev. Online 125, 125 (2014); *see also,* Fed'n Am. Scientists, *Foreign Intelligence Surveillance Act*, available at https://www.fas.org/irp/agency/doj/fisa (last visited Mar. 06, 2019) (collecting the Foreign Intelligence Surveillance Court's annual reports to Congress).)

44. *Carpenter*, 138 S. Ct. at 2214.

FISA, the government can use national security concerns to override these purposes. This is a new phenomenon.

National security concerns existed at the time of the writing of the Bill of Rights, just as they exist now. The Constitution's criminal procedure rights are older than the Republic, with Due Process dating back to the Magna Carta. They are nothing new.

What is new is the emergence in 1978 of FISA and the Foreign Intelligence Surveillance Court. They exhibit curious features relative to our legal traditions.

For instance, despite its awesome power to order secret surveillance and searches of U.S. citizens, the secret, *ex parte* Foreign Intelligence Surveillance Court isn't a normal Article III court, if it is an Article III court at all. The court doesn't hear any cases or controversies, and appears to have no adversarial proceedings.[45] And it has a feature shared only by this Court - it is unchallengeable for a criminal defendant.

Another curiosity is the Foreign Intelligence Surveillance Court's infallibility. FISA provides for disclosure of Foreign Intelligence Surveillance Court applications and orders to defendants.[46] But, in the 41-

45. *See* U.S. Constitution, Art. III, § 2 (promulgating the judicial power of the U.S.).

46. 50 U.S.C. § 1806(f) ("In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.")

year history of the Foreign Intelligence Surveillance Court that's never happened. Recently, some of Carter Page's FISA materials were released in redacted form, but that was an exceptional circumstance in which the FBI responded to congressional and political pressure.[47] But the fact remains that no defendant has ever been able to subject their case's FISA application and materials to investigation and adversarial testing at trial. This doesn't seem right, because no one bats 1000.

Gartenlaub's case is an example of how the government can abuse a national security investigation under FISA to prosecute unrelated non-national security crimes. Because of this risk, the government should not be permitted to use secret national security warrants to prosecute regular crimes if it won't submit those warrants and supporting materials to investigation and the adversarial process the criminal procedure amendments require. This Court should grant certiorari to analyze and clarify the scope of the 1978 FISA's encroachment upon the fundamental, centuries old, criminal procedure protections of the Fourth, Fifth, and Sixth Amendments.

I. The Court Should Grant Certiorari Because the FISA Search Warrant in this Case is a General Warrant

The Framers despised general warrants:

---

47. *See, e.g.,* Charlie Savage, *Carter Page FISA Documents are Released by Justice Department*, N.Y. Times, July 21, 2018, available at https://www.nytimes.com/2018/07/21/us/politics/carter-page-fisa.html

> Vivid in the memory of the newly independent Americans were those general warrants known as writs of assistance under which officers of the Crown had so bedeviled the colonists." Writs of assistance were despised, as they gave customs officials unlimited authority to search where they wished for anything imported in violation of tax laws. James Otis denounced writs of assistance as "the worst instrument of arbitrary power, the most destructive of English liberty, and the fundamental principles of law, that ever was found in an English law book," because they placed "the liberty of every man in the hands of every petty officer." The use of writs of assistance birthed the movement toward independence. "Then and there," said John Adams, "then and there was the first scene of the first act of opposition to the arbitrary claims of Great Britain. Then and there the child Independence was born."[48]

This Court has never held that FISA warrants are an exception to the Fourth Amendment's strict prohibition on general warrants. The search of Gartenlaub's hard drives has the hallmarks of a general warrant. There was no practical limitation to it. The government rummaged

---

48. *Payton v. New York*, 445 U.S. 573, 584, 639 n. 21 (1980) (quoting *Boyd v. United States*, 116 U.S. 616 (1886); *Stanford v. Texas*, 379 U.S. 476, 481-82 (1965)); *see also Riley v. California*, 573 U.S. 373, 403, (2014) "(Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.").

through every file on his hard drives. There were no date range limitations, key word searching, taint teams, or other routine procedures used to limit a computer search. The question isn't: Why is the search of Gartenlaub's hard drives a general warrant? It's: Why isn't it? The government's answer is "national security."

But national security is a limitation on the search of Gartenlaub's hard drives only in name. That's why the Ninth Circuit's decision ignores the Fourth Amendment's particularity clause and focuses on probable cause. There was no particularity to the government's FISA search, so there was nothing to discuss.

By invoking national security to justify its search, the government is essentially using a limitation that FISA imposes on surveillance and searches - that they're bounded by national security concerns - and saying it's a justification for unbounded searching. Viewed this way, the government's justification begs the question. National Security as a limiting principal for searches becomes national security as an unlimiting principal for searches.

But FISA is meant to limit secret national security searches to situations where there's probable cause to think that an agent of a foreign power is committing a national security crime.[49] It's meant to limit the government's search powers, not expand them. The Ninth Circuit skirts this issue when denying Gartenlaub's appeal:

> The idea that the government can decide that someone is a foreign agent based on secret

49. (App. at 24a; 50 U.S.C. § 1805(a)(2); *See also United States v. Muhtorov*, 187 F. Supp. 3d 1240 (D. Colo. 2015).)

> information; on that basis obtain computers containing "[t]he sum of [that] individual's private life," *Riley v. California*, 134 S.Ct. 2473, 2489 (2014); and then prosecute that individual for completely unrelated crimes discovered as a result of rummaging through that computer comes perilously close to the exact abuses against which the Fourth Amendment was designed to protect.[50]

Gartenlaub's case doesn't "come perilously close" to the Fourth Amendment's protections, it's the exact fact pattern the Fourth Amendment prohibits. The Ninth Circuit offers no explanation for why we're just "perilously" close to a Fourth Amendment violation rather than right in the middle of one. Gartenlaub's case has the earmarks of potential violations of the Fourth Amendment Probable Cause and Particularity clauses:

1. A secret, unlimited government search

2. Executed under a secret national security warrant, based on the probable cause that Gartenlaub is the agent of a foreign power

3. That turns up no evidence that Gartenlaub is a foreign agent

4. But does turn up evidence of an unrelated non-national security crime

---

50. (App. at 4a. (*United States v. Gartenlaub*, No. 16-50339, 2018 WL 4761630, at *1 (9th Cir. Oct. 2, 2018) (Appeal Dkt. 94.).)

5. Which then is used as probable cause for regular Rule 41 search warrants,

6. Resulting in Gartenlaub's conviction for the unrelated, non-national security crime.

One is left to wonder how there could be probable cause for the FISA warrant when a methodical, months long rummaging through all of the files on Gartenlaub's hard drives turned up no evidence he was a spy.

FISA warrants do enjoy a degree of flexibility that normal regular criminal warrants do not possess.[51] But precisely because this flexibility is limited to matters of national security. And the fact that FISA searches are secret, easy to abuse, and prone to turning into general warrants, argue for more stringent review of probable cause determinations for FISA warrants rather than the lax ones. FISA warrants are only appropriate in particular circumstances, and the Fourth Amendment limits the scope of FISA. Courts recognize the government's interest in speed, stealth, and secrecy in surveillance in national security investigations.[52] But FISA doesn't permit searches for evidence of regular crimes.[53] FISA is not a license for the government to conduct fishing expeditions into the lives and data of private individuals.

---

51. (*See* BAC at 7-8.)

52. *United States v. Troung Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980).

53. *See* 50 U.S.C. § 1804(a)(3)(a) (requiring that the applicant for a Foreign Intelligence Surveillance Court warrant have a justified belief that "the target of the electronic surveillance is a foreign power or an agent of a foreign power . . . .").

The Ninth Circuit doesn't discuss the Fourth Amendment's particularity clause in analyzing Gartenlaub's secret FISA search. The Ninth Circuit only says its *ex parte*, *in camera* review, with the helpful presence of the government, supported the Foreign Intelligence Surveillance Court's probable cause determination.[54] But analyzing probable cause is just one part of the general warrant analysis. The analysis has to include the clause that specifically targets general warrants: the Particularity Clause.

The Fourth Amendment's Probable Cause Clause and Particularity Clause are two logically, albeit interrelated, distinct clauses. A warrant can be supported by probable cause and still violate the Particularity Clause:

> To satisfy the demands of the Warrant Clause, a warrant must comply with two related but distinct rules. First, it must describe the place to be searched or things to be seized with sufficient particularity, taking account of "the circumstances of the case and the types of items involved. Second, it must be no broader than the probable cause on which it is based. The particularity rule and the probable cause rule serve a common purpose: to protect privacy by prohibiting a general, exploratory rummaging in a person's belongings. Although the two rules serve the same ultimate purpose, they achieve the purpose in distinct ways. [55]

54. (*Id.*)

55. *United States v. Weber*, 923 F.2d 1338, 1342 (9th Cir. 1990) (citations omitted).

There is good reason to think the FISA warrant at issue here lacked particularity. The government admits in its Opposition Brief that there was no practical limitation to the FISA warrant, and that it could search each and every file on Gartenlaub's computer.[56] The government makes no mention that it ever placed any of the recognized, standard limitations for digital searches like date limitations, key word searching, or taint teams, on its search of Gartenlaub's digital storage devices. It just asserts it could search everything it wanted to, and it did so.

This Court should grant certiorari to prevent the government from using national security pretexts to make an end run around the Fourth Amendment's prohibitions on general warrants.

II. The Court Should Grant Certiorari to Impose Use Restrictions on Non-Responsive Evidence of Non-National Security Crimes Obtained Through FISA Computer Searches

Computer searches are especially prone to turning into rummaging that amounts to a general warrant, and this Court, and others, have repeatedly expressed their concerns on this front.[57] This has led courts and leading

56. (*See* GB at 52.)

57. *See, e.g., Riley v. California*, 573 U.S. 373, 403 (2014); *United States v. Ganias*, 824 F.3d 199 (2nd Cir 2016); *United States v. Richards*, 659 F.3d 527 (6th Cir. 2011); *United States v. Comprehensive Drug Testing, Inc.*, 621 F. 3d 1162 (9th Cir. 2010); *United States v. Mann*, 592 F.3d 779 (7th Cir 2010); *United States v. Carey*, 172 F.3d 1268 (10th Cir 1999); *United States v. Tamura*,

computer law scholars to propose use restrictions upon digital information non-responsive to a search warrant.[58] In the case of secret FISA evidence, these use restrictions would be on top of FISA's required minimization techniques meant to limit the use of non-national security evidence.[59] The Court should grant certiorari to consider these type of use restrictions on non-responsive evidence derived from FISA computer searches.

As this Court recently held in *Carpenter*, computer searches implicate two of the Framer's core Fourth Amendment concerns: Securing "the privacies of life" against arbitrary police power and "plac[ing] obstacles in the way of a too permeating police surveillance."[60] The government rummaged through "the privacies" of Gartenlaub's life when it examined every file in his hard drives.

Law enforcement is always alert to the broadest possible search methods. That's part of their job. Invoking

---

694 F.2d 591, 595-96 (9th Cir. 1982); *United States v. Jae Shik Kim*, 103 F. Supp. 3d 32 (D.C. 2015); *see also*, *United States v. Perez*, 712 Fed. Appx. 136 (3rd Cir 2017); (BAC at 13-22).

58. *See, id*; Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Texas Tech. L. Rev. 1, at 18 (2015).

59. (App. at 45a-46a, (50 U.S.C. §§ 1801(h) and 1821(4).))

60. *Carpenter v. United States*, 138 S. Ct. 2206, 2213–14, (2018) (citing *Boyd v. United States,* 116 U.S. 616, 630, (1886) and *United States v. Di Re,* 332 U.S. 581, 595 (1948)); *see also Riley v. California*, 573 U.S. 373, 395-96, (2014) ("An Internet search and browsing history . . . could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD.").

national security to search for evidence of a regular crime is a tempting and easy way to get around the Fourth, Fifth, and Sixth Amendments.

The problem of a computer search turning into a general warrant is more acute with a FISA case because the warrants aren't subject to adversarial review. This practically means that the government's actions aren't subject to the defendant's or the publics review. This Court should grant certiorari to impose use restrictions on evidence of non-national security regular crimes discovered during the execution of a secret, general FISA warrant, to prevent government abuse.

III. The Court Should Grant Certiorari to Determine Whether the District Court's Denying Gartenlaub a *Franks* Hearing on the FISA Warrant Requires Suppression of the Fruits of that Warrant

The Fourth Amendment requires all warrants to issue only on probable cause.[61] FISA limits this requirement further, mandating that FISA warrants only issue upon the Foreign Intelligence Surveillance Court's finding of probable cause that someone is an agent of a foreign power.[62] Presumably, the government's application for a FISA warrant argued that Gartenlaub was spying by sending China plans for the U.S. military's C-17 cargo plane. But skepticism is warranted here because there's no evidence in the public record to support it.

61. U.S. Const. Amend. IV (1789).

62. (App. at 24a, (50 U.S.C. § 1805(a)(2).)).

Gartenlaub has never been charged with a national security crime. The original investigation launched during the same period of other false FISA investigations under similar national security pretexts. And it started with a whimper – when an FBI Agent read a magazine article, not with a bang from some dramatic event. The search warrant that resulted from the FBI's online reading turned up nothing after it was executed on the Gartenlaubs' emails. Neither did the FISA search, or it presumably would have led to a national security prosecution.

The defense, and the public, will never know. We must trust that the national security matters involved are so important that they eliminate the constitutional rights to public adversarial challenge. The defense, and the public, must trust that the secret, *ex parte* probable cause determinations made after secret conference between the government and the judiciary, at every step in this process, was free from confirmation bias, or other errors that the defendant could argue to the court or jury.[63]

This is not consistent with the underlying philosophy of the Bill of Rights, nor is it consistent with the adversarial foundation of our criminal justice system. Both are skeptical of government and rely on the adversarial system, as outlined in the Fourth, Fifth, and Sixth Amendments, to test the government. Both are skeptical of *ex parte* evidentiary determinations.

Towards the end of the recording of the Ninth Circuit oral arguments in this case, you can hear the court confirm

63. *See* Adam Benforado, *Unfair: The New Science of Criminal Injustice* (Broadway Books 2015) (discussing confirmation bias and criminal evidence).

its upcoming, *ex parte*, meeting with the government to secretly review the FISA materials.[64] The *ex parte* review of search warrants, to say nothing of secret search warrants, is precisely what the Framers sought to limit when they drafted the Fourth Amendment's warrant clause. The Framers were seeking to minimize *ex parte* search warrants issued by the judiciary and government when they wrote the Fourth Amendment—not maximize their use—because of the abuse they suffered under such warrants. The history of the Foreign Intelligence Surveillance Court is validating the Framer's concerns on this front.[65] To study the drafting and intent of the Fourth Amendment is to learn how wary the Framers were of *ex parte* search warrants.

The Ninth Circuit's decision analyzes the issues in Gartenlaub's case solely from the perspective of probable cause. But the probable cause analysis can't be properly evaluated because the opinion provides no reasoning or factual basis to evaluate whether the execution of the warrant was broader than that justified by its probable cause.[66] An adversarial proceeding would have solved that issue.

---

64. Oral Argument, *United States v. Keith Preston Gartenlaub*, No. 16-50339 (9th Cir., Dec. 4, 2017), available at https://www.ca9.uscourts.gov/media/view.php?pk_id=0000031669.

65. *See* Akhil Reed Amar, *The Constitution and Criminal Procedure: First Principles*, 1-45, 13 (Yale 1997) ("Warrants, then, were friends of the searcher, not the searched. They had to be limited; otherwise, central officers on the government payroll in ex parte proceedings would usurp the role of the good old jury in striking the proper balance between government and citizen after hearing lawyers on both sides.").

66. *See Weber*, 923 F.2d at 1345 (holding that "a blunderbuss warrant [in a CP case] was unjustified.").

That Foreign Intelligence Surveillance Court probable cause determinations for FISA warrants aren't subject to a defendant's adversarial challenge raises the issue of whether evidence outside the scope of the probable cause for a FISA search, discovered as part of the FISA search, should be suppressed when it's used in an unrelated non-national security prosecution. The Court should grant certiorari to review the issue.

IV. The Court Should Grant Certiorari Because In the 41 Year History of FISA No Defendant Has Ever Had Access to Their Case's Secret FISA Application and this Violates the Fourth, Fifth, and Sixth Amendments

Even though FISA provides for disclosing applications to defendants, that's never happened in 41 years.[67] The case law is opaque as to precisely why, because most of the facts are secret and thus aren't in the decisions. This is harmful to *stare decisis*. Because if you don't know the underlying facts to a decision in our common law system, then you don't really know what's been decided. And you cannot use that case to argue for your position, or against your adversaries.

FISA is distorting our adversarial, precedential, and common law system in subtle ways. For instance, in its denial of Gartenlaub's appeal, the Ninth Circuit stated

---

67. With the recent exception of Carter Page's FISA materials. But that was outside the context of a criminal trial. *See,* Jeremy Herb and David Shortell, *FBI Releases Carter Page Surveillance Warrant Documents*, CNN, July 23, 2018, available at https://www.cnn.com/2018/07/21/politics/fbi-carter-page-surveillance-warrant/index.html

that "[n]o controlling authority dictates the conclusion that the government's [FISA] search and subsequent use of FISA-derived materials in a non-national security prosecution violates the Fourth Amendment, such that the district court's failure to follow it was plain error."[68] But how is a defendant supposed to find case law for that proposition when the case law is factually opaque? Judicial decisions based on secret, undisclosed fact finding are inimical to *stare decisis* and the truth finding function of our adversarial system.

Because facts in FISA cases are murky, it's hard to tell how many cases involve computer searches like in Gartenlaub's. None are readily apparent.[69] Most reported FISA cases involving non-national security prosecutions seem to involve incidental surveillance of the regular crime as it happened, or a non-national security crime like wire fraud or money laundering, that was directly related to the national security investigation.

---

68. (App. at 3a.) (*United States v. Gartenlaub*, No. 16-50339, 2018 WL 4761630, at *1 (9th Cir. Oct. 2, 2018).)

69. *See United States v. Chi Ping Ho,* No. 17 CR. 779 (LAP), 2018 WL 5777025, at *8 (S.D.N.Y. Nov. 2, 2018) (denying suppression motion of evidence derived from FISA authorized physical search without detailing any facts); *United States v. Hawamda,* No. Crim. 89-56-A, 1989 WL 235836, at *2 (E.D. Va. Apr. 17, 1989) (requiring that those requesting information obtained from FISA warrants be a target of the surveillance)*; see also Matter of Kevork,* 788 F.2d 566, 570 (9th Cir. 1986) (holding FISA did not bar use of surveillance evidence in foreign criminal prosecution); *United States v. Muhtorov,* 187 F. Supp. 3d 1240, 1250 (10th Cir) (stating the purpose of the surveillance cannot be a ruse); *United States v. Johnson*, 952 F.2d 565, 572 (FISA cannot be used as a run around to the Fourth Amendment's prohibition of warrantless searches); *United States v. Troung Dinh Hung,* 629 F.2d 908, 916 (4th Cir. 1980).

The 27 year old FISA case of *United States v. Isa* appears to be one of the few instances where a prosecutor used the non-responsive fruits of a FISA search for an unrelated regular criminal prosecution.[70] *Isa* upheld the use of a FISA surveillance recording, in a state prosecution, of the surveillance target's murder of his 16-year-old daughter.[71] During the course of the surveillance the murder occurred and was incidentally recorded. Unlike Gartenlaub's case, the evidence was not obtained via the methodical rummaging over the course of months through the target's computers.

Gartenlaub couldn't access the secret FISA application and materials pre-trial and had no way to forensically authenticate the government's search. FBI forensics labs have a documented history of falsifying evidence and testimony spanning decades.[72] And the government has withheld *Brady* evidence in cases.[73]

---

70. *United States v. Isa*, 923 F.2d 1300 (8th Cir. 1991)

71. *Id.* at 1302.

72. See, e.g., Spencer S. Hsu, *FBI Admits Flaws in Hair Analysis Over Decades* Wash. Post, April 18, 2015, available at: https://www.washingtonpost.com/local/crime/fbi-overstated-forensic-hair-matches-in-nearly-all-criminal-trials-for-decades/2015/04/18/39c8d8c6-e515-11e4-b510-962fcfabc310_story.html?noredirect=on&utm_term=.96fe7c98dfd4

73. *See, e.g.*, Anna Stolley Persky, *A Cautionary Tale: The Ted Stevens Prosecution*, DC Bar, Oct. 2009, available at: https://www.dcbar.org/bar-resources/publications/washington-lawyer/articles/october-2009-ted-stevens.cfm; *Brady v. Maryland*, 373 U.S. 83, 87 (1963).

The Court should grant certiorari to review how the District Court's denying Gartenlaub access to the secret FISA application and materials impacts his fundamental criminal procedure rights under the Fourth, Fifth, and Sixth Amendments. And whether that merits suppression of the fruits of the FISA warrant.[74]

V. The Court Should Grant Certiorari Because FISA Contradicts our Republic's Legal Traditions

In the 1630's the infamous Star Chamber tried and convicted English Lawyer William Prynne. For the crime of "writing books and pamphlets," Prynne's "ears were first cut off by court order and . . . subsequently, by another court order, . . . his remaining ear stumps [were] gouged out while he was on a pillory."[75]

The Foreign Intelligence Surveillance Court isn't the Star Chamber. Yet. But the fact that even a mild comparison can be made should give pause. The Star Chamber was a secret, virtually infallible, inquisitorial English court that did the monarch's bidding. [76] It too,

---

74. *See, e.g., Wong Sun v. United States*, 371 U.S. 471 (1963) (holding that evidence obtained through the exploitation of an illegal search is fruit of the poisonous tree, which should be suppressed).

75. Akhil Reed Amar, *The Bill of Rights: Creation and Reconstruction*, 82 (Yale University Press 1998)

76. *See Jones v. Sec. & Exch. Comm'n*, 298 U.S. 1, 28 (1936) (discussing the " intolerable abuses of the Star Chamber, which brought that institution to an end at the hands of the Long Parliament in 1640"); *United States v. Gecas*, 120 F.3d 1419, 1446 (11th Cir. 1997) (discussing history of the Star Chamber in depth).

was held in the highest regard and deference by the judiciary. The King's Bench held that "the Court of the Star Chamber was . . . one of the most high and honourable Courts of Justice . . . ."[77] Notably, when the Long Parliament abolished the Star Chamber in 1641, it did so with the statute that enscribed the writ of habeas corpus into the law books for the first time. Habeas corpus, "the great writ" is the fundamental guarantor of our right to challenge government prosecution, and the Constitution's only named privilege.[78] It was no coincidence.

FISA and the Foreign Intelligence Surveillance Court contradict our Republic's traditions. The Framers had ample opportunity and cause to establish secret national security courts in the early days of our Republic. Despite the threats to our country at the time, they chose not to.

George Washington was no stranger to national security threats and President of the Constitutional Convention. When the Framers drafted the Constitution the U.S. faced threats on all sides. Ten thousand British troops were still stationed on the Northwestern Frontier encouraging the Native Americans to engage in border warfare with the States. The Spanish controlled Florida and the mouth of the Mississippi. Shay's Rebellion had just occurred, and our disgruntled European creditors were making rumblings of war over our unpaid Revolutionary

77. William F. Duker, *A Constitutional History of Habeas Corpus*, 46-47 (Greenwood Press 1980) (quoting *Chamber's Case*, 79 Eng. Rep. 746, 747 (K.B. 1630).)

78. Duker, at 47; U.S. Const. Art. I, §9, cl. 2.

War debts.[79] George Washington knew better than anyone the risks our nation faced. Yet none of them instituted a secret court like Foreign Intelligence Surveillance Court. They would rightly view the Foreign Intelligence Surveillance Court, and FISA, with suspicion and concern.

Because they fought a revolution against secrecy, arbitrary government power, and government prying in our private lives. And they fixed these values in the criminal procedural protections of the Fourth, Fifth. and Sixth Amendments. The Constitution would never have passed without these protections. The States wouldn't have ratified the Constitution if they hadn't been promised the Bill of Rights and its criminal procedural guarantees.

FISA and the Foreign Intelligence Surveillance Court are newcomers to this tradition. It's only in 1978, over 200 years after the founding of our nation and the multiple wars we've fought and threats we've faced, that a secret national security court emerges. The irony of FISA and the Foreign Intelligence Surveillance Court is that Congress created them to protect us from an internal threat, but only made that threat worse.

FISA came into being not as a response to any new external threat to our national security. Congress passed

---

79. *See,* Joseph J. Ellis, *American Dialogue: The Founders and Us*, 194 (Alfred A. Knopf 2018); Tor Ekeland, *Suspending Habeas Corpus: Article I, Section 9, Clause 2, of the United States Constitution and the War on Terror*, 74 Fordham L. Rev. 1475, 1482 (2005 ("On May 14, 1787, when the Federal Constitutional Convention assembled, the United States faced substantial threats to its security on all sides."), available at https://ir.lawnet.fordham.edu/cgi/viewcontent.cgi?article=4129&context=flr.

FISA because of the FBI's and CIA's illegal spying and actions against U.S. citizens that the courts failed to address. The Church Committee Report, which led to FISA's passage details this in depth.[80] But now, as Gartenlaub's case demonstrates, history is repeating itself and the FISA is slowly eroding the fundamental protections of the Constitution's criminal procedure guarantees.

This Court should grant certiorari to strike the right balance between the Fourth, Fifth, and Sixth Amendments' criminal procedure protections and our national security interests. And to keep those national security interests from encroaching on our Liberty.

---

80. *See* S. Rep. No. 94-755, *Final Report of the Select Committee to Study Governmental Operations with Respect to Intelligence Activities*, at 11 (April 26, 1976) ("[T]he Committee's investigation has uncovered a host of serious legal and constitutional issues relating to [domestic] intelligence activity and it is strong proof of the need for reform to note that scarcely any of those issues have been addressed in the courts."), available at https://upload.wikimedia.org/wikipedia/commons/7/79/Church_Committee_report_%28Book_I%2C_Foreign_and_Military_Intelligence%29.pdf; *see also*, Elizabeth Goitein and Faiza Patel, *What Went Wrong With the FISA Court*, Brennan Center for Justice (2015), available at https://www.brennancenter.org/sites/default/files/publications/What_Went_%20Wrong_With_The_FISA_Court.pdf.

CONCLUSION

This case shows how easily the government can bypass the fundamental criminal procedure protections of the Fourth, Fifth, and Sixth Amendments by invoking national security under FISA. This Court should grant certiorari to review the proper balance between the fundamental criminal procedure protections of the Fourth, Fifth, and Sixth Amendments, FISA, and the Foreign Intelligence Surveillance Court, and to reverse Gartenlaub's conviction.

Respectfully submitted,

Tor Ekeland
Counsel of Record
Mark Jaffe
Lydia Fields
Tor Ekeland Law PLLC
195 Montague Street, 14th Floor
Brooklyn, NY 11201
(718) 737-7264
tor@torekeland.com

Counsel for Petitioner

APPENDIX

APPENDIX A — MEMORANDUM OF THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT, FILED OCTOBER 2, 2018

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

Docket No. 16-50339

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

KEITH PRESTON GARTENLAUB,
AKA KEITH PRESON GARTENLAUB,

Defendant-Appellant.

December 4, 2017, Argued
and Submitted, Pasadena, California;
October 2, 2018, Filed

Appeal from the United States District Court for the Central District of California. D.C. No. 8:14-cr-00173-CAS-1. Christina A. Snyder, District Judge, Presiding.

Appendix A

MEMORANDUM[*]

Before: WARDLAW and GOULD, Circuit Judges, and PIERSOL,[**] District Judge.

Keith Gartenlaub appeals his conviction for knowingly possessing child pornography in violation of 18 U.S.C. § 2252A(a)(5)(B). We have jurisdiction under 28 U.S.C. § 1291, and we affirm.[1]

1. There was sufficient evidence to sustain Gartenlaub's conviction for knowing possession of child pornography. Viewing the evidence in the light most favorable to the prosecution, any rational trier of fact could have found the essential elements of the crime—including knowledge—beyond a reasonable doubt. The government presented sufficient evidence that Gartenlaub knew the child pornography was present on his computers. *See* 18 U.S.C. § 2252A(a)(5)(B) (requiring that the defendant must "knowingly possess[] . . . any . . . computer disk, or any other material that contains an image of child pornography that has been . . . transported using any means or facility of interstate or foreign commerce . . . including by computer").

---

[*] This disposition is not appropriate for publication and is not precedent except as provided by Ninth Circuit Rule 36-3.

** The Honorable Lawrence L. Piersol, United States District Judge for the District of South Dakota, sitting by designation.

1. The government's motion to file an oversized brief, Dkt 51, is GRANTED.

The government demonstrated that an individual intentionally downloaded child pornography, copied it onto Gartenlaub's hard drives, and organized and reorganized the child pornography into folders reflecting the content of the videos. *See* 18 U.S.C. § 2252A(a)(5)(B). A rational jury could have concluded beyond a reasonable doubt that the user of the password-protected "Keith" account opened a folder containing obviously child-pornographic filenames and then copied those files onto a new computer, that "Keith" knowingly downloaded and organized the child pornography collection in the first place, and that "Keith" was Keith Gartenlaub himself. *See United States v. Nevils*, 598 F.3d 1158, 1164 (9th Cir. 2010) (en banc); *United States v. Willard*, 230 F.3d 1093, 1095 (9th Cir. 2000) (citing *Jackson v. Virginia*, 443 U.S. 307, 319, 99 S. Ct. 2781, 61 L. Ed. 2d 560 (1979)).

2. The district court did not commit plain error by failing to suppress the evidence from Gartenlaub's computer as inadmissible for violating the Fourth Amendment.[2]

No controlling authority dictates the conclusion that the government's Foreign Intelligence Surveillance Act ("FISA") search and subsequent use of FISA-derived materials in a non-national security prosecution violates the Fourth Amendment, such that the district court's failure to follow it was plain error. *See United States v.*

2. Plain error review is the appropriate standard because Gartenlaub did not assert the Fourth Amendment argument predicated on alleged misuse of the FISA warrant before the district court.

Gonzalez-Aparicio, 663 F.3d 419, 428 (9th Cir. 2011), *as amended* (Nov. 16, 2011). Our decision in *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (en banc), *abrogation recognized by Demaree v. Pederson*, 887 F.3d 870 (9th Cir. 2018) (per curiam), is inapposite; it did not decide the question presented by this case and, in fact, addressed no national security concerns particular to the FISA context.

The idea that the government can decide that someone is a foreign agent based on secret information; on that basis obtain computers containing "[t]he sum of [that] individual's private life," *Riley v. California*, 134 S. Ct. 2473, 2489, 189 L. Ed. 2d 430 (2014); and then prosecute that individual for completely unrelated crimes discovered as a result of rummaging through that computer comes perilously close to the exact abuses against which the Fourth Amendment was designed to protect.[3] However, the district court did not commit plain error by concluding otherwise.

3. Based upon our independent review of the classified record evidence, we conclude that the FISA warrant was supported by probable cause. The FISA application and supporting materials demonstrated probable cause to believe that Gartenlaub was an agent of a foreign power when the FISA order was issued. *See* 50 U.S.C. §§ 1801(b), 1821(1), 1824(a)(2).[4] The district court did not

3. We thank amici curiae, Electronic Frontier Foundation and American Civil Liberties Union, for their thought-provoking briefing.

4. Although there is a split in the circuits as to what deference to afford a district court's determination that a FISA order was based

err in denying Gartenlaub a *Franks* hearing. The district court did not err in "finding that the government did not intentionally or recklessly make false statements." *United States v. Christie*, 825 F.3d 1048, 1069 (9th Cir. 2016) (citation omitted); *see Franks v. Delaware*, 438 U.S. 154, 98 S. Ct. 2674, 57 L. Ed. 2d 667 (1978).

4. We have conducted an *in camera* review of the underlying FISA materials. We conclude that the disclosure of the FISA materials to Gartenlaub was not "necessary to make an accurate determination of the legality of the search." 50 U.S.C. § 1825(g); *see also United States v. Ott*, 827 F.2d 473, 476-77 (9th Cir. 1987) (finding "no indications of possible misrepresentation of fact, vague identification of the persons to be surveilled, or surveillance records which include a significant amount of non-foreign intelligence information, or any other factors that would indicate a need for disclosure" (internal quotation marks omitted)). In point of fact, disclosure was not necessary even under a less rigorous standard than that proposed by the government. As well, the non-disclosure violated neither Gartenlaub's due process nor *Brady* rights. *See Brady v. Maryland*, 373 U.S. 83, 83 S. Ct. 1194, 10 L. Ed. 2d 215 (1963); *Ott*, 827 F.2d at 476-77.

AFFIRMED.

---

on probable cause, we do not resolve here which level of deference is appropriate as we are convinced probable cause existed under either a de novo or an abuse of discretion standard of review. *See United States v. Turner*, 840 F.3d 336, 340 (7th Cir. 2016) (applying a de novo standard of review); *United States v. Hassan*, 742 F.3d 104, 139 n.29 (4th Cir. 2014) (noting that the Fourth Circuit applies a de novo standard although the Fifth and Second Circuits apply a more deferential standard).

APPENDIX B — JUDGMENT AND PROBATION/ COMMITMENT ORDER OF THE UNITED STATES DISTRICT COURT FOR THE CENTRAL DISTRICT OF CALIFORNIA, FILED SEPTEMBER 6, 2016

UNITED STATES DISTRICT COURT
CENTRAL DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA vs.

Defendant KEITH PRESTON GARTENLAUB

akas: N/A

Docket No. SACR14-173-CAS

Social Security No. 9 4 2 9 (Last 4 digits)

JUDGMENT AND PROBATION/ COMMITMENT ORDER

In the presence of the attorney for the government, the defendant appeared in person on this date. **MONTH 08 DAY 29 YEAR 2016**

COUNSEL	**Mark Werksman, Retained** (Name of Counsel)
PLEA	☐ **GUILTY,** and the court being satisfied that there is a factual basis for the plea. ☐ **NOLO CONTENDERE** ☐ **NOT GUILTY**

Appendix B

FINDING	There being a finding/verdict of **GUILTY,** defendant has been convicted as charged of the offense(s) of: Possession of Child Pornography in violation of 18 U.S.C. § 2252A(a)(5)(B), 2252a(b)(2), as charged in Count 2 of the Indictment.
JUDGMENT AND PROB/ COMM ORDER	The Court asked whether there was any reason why judgment should not be pronounced. Because no sufficient cause to the contrary was shown, or appeared to the Court, the Court adjudged the defendant guilty as charged and convicted and ordered that: Pursuant to the Sentencing Reform Act of 1984, it is the judgment of the Court that the defendant is hereby committed to Count 2 of the 2-Count Indictment to the custody of the Bureau of Prisons to be imprisoned for a term of: **FORTY-ONE (41) MONTHS.**

It is ordered that the defendant shall pay to the United States a special assessment of $100.00, which is due immediately. Any unpaid balance shall be due during the period of imprisonment, at the rate of not less than $25.00 per quarter, and pursuant to the Bureau of Prisons' Inmate Financial Responsibility Program.

The defendant shall comply with General Order No. 01-05.

All fines are waived as it is found that such sanction would place an undue burden on the defendant's dependent.

It is ordered that the defendant shall pay restitution in the total amount of $3,430.00, pursuant to 18 U.S.C. § 3663A.

The amount of restitution ordered shall be paid to the victim as set forth in a separate victim list prepared by the probation office which this Court adopts and which reflects the Court's determination of the amount of restitution due to each victim. The victim list, which shall be forwarded to the fiscal section of the clerk's office, shall remain confidential to protect the privacy interests of the victim. Restitution shall be due during the period of imprisonment, at the rate of not less than $25.00 per quarter, and pursuant to the Bureau of Prisons' Inmate Financial Responsibility Program. If any amount of the restitution remains unpaid after release from custody, nominal monthly payments of at least $100.00 or ten percent of the defendant's gross monthly income, whichever is greater, shall be made during the period of supervised release. These payments shall begin 30 days after the commencement of supervision. Nominal restitution payments are ordered as the Court finds that the defendant's economic circumstances do not allow for either immediate or future payment of the amount ordered.

Pursuant to 18 U.S.C. § 3612(f)(3)(A), interest on the restitution ordered is waived because the defendant does not have the ability to pay interest. Payments may be subject to penalties for default and delinquency pursuant to 18 U.S.C. § 3612(g).

Appendix B

Upon release from imprisonment, the defendant shall be placed on supervised release for a term of life under the following terms and conditions:

1. The defendant shall comply with the rules and regulations of the United States Probation Office, General Order 05-02, and General Order 01-05, including the three special conditions delineated in General Order 01-05;

2. The defendant shall refrain from any unlawful use of a controlled substance. The defendant shall submit to one (1) drug test within 15 days of release from imprisonment and at and at least two (2) periodic drug tests thereafter, not to exceed eight (8) tests per month, as directed by the Probation Officer;

3. As directed by the Probation Officer, the defendant shall pay all or part of the costs of the defendant's mental health treatment to the aftercare contractors during the period of community supervision, pursuant to 18 U.S.C. § 3672. The defendant shall provide payment and proof of payment as directed by the Probation Officer;

4. During the period of community supervision, the defendant shall pay the special assessment in accordance with this judgment's orders pertaining to such payment;

5. The defendant shall cooperate in the collection of a DNA sample from the defendant;

6. The defendant shall possess and use only those computers and computer-related devices, screen user names, passwords, email accounts, and internet service providers (ISPs) that have been disclosed to the Probation Officer upon commencement of supervision. Any changes or additions are to be disclosed to the Probation Officer prior to the first use. Computers and computer-related devices include personal computers, personal data assistants (PDAs), internet appliances, electronic games, cellular telephones, and digital storage media, as well as their peripheral equipment, that can access, or can be modified to access, the internet, electronic bulletin boards, and other computers;

7. All computers, computer-related devices, and their peripheral equipment, used by the defendant shall be subject to search and seizure. This shall not apply to items used at the employment's site, which are maintained and monitored by the employer;

8. The defendant shall comply with the rules and regulations of the Computer Monitoring Program. The defendant shall pay the cost of the Computer Monitoring Program, in an amount not to exceed $32.00 per month per device connected to the internet

9. The defendant shall register as a sex offender, and keep the registration current, in each jurisdiction where he resides, where he is an employee, and where he is a student, to the extent the registration procedures have been established in each jurisdiction.

When registering for the first time, the defendant shall also register in the jurisdiction in which the conviction occurred if different from his jurisdiction of residence. The defendant shall provide proof of registration to the Probation Officer within three days of release from imprisonment;

10. The defendant shall participate in a psychological counseling or psychiatric treatment or a sex offender treatment program, as approved and directed by the Probation Officer. The defendant shall abide by all rules, requirements, and conditions of such program;

11. The defendant shall not view or possess any materials, including pictures, photographs, books, writings, drawings, videos, or video games depicting and/or describing "sexually explicit conduct", as defined at 18 U.S.C. § 2256(2);

12. The defendant shall not view or possess any materials, including pictures, photographs, books, writings, drawings, videos, or video games depicting and/or describing child pornography, as defined at 18 U.S.C. § 2256(8). This condition does not prohibit the defendant from possessing materials solely because they are necessary to, and used for, a collateral attack, nor does it prohibit him from possessing materials prepared and used for the purposes of his Court-mandated sex offender treatment, when the defendant's treatment provider or the probation officer has approved of his possession of the materials in advance;

13. The defendant shall not own, use or have access to the services of any commercial mail-receiving agency, nor shall he open or maintain a post office box, without the prior written approval of the Probation Officer;

14. The defendant shall not frequent, or loiter, within 100 feet of school yards, parks, public swimming pools, playgrounds, youth centers, video arcade facilities, or other places primarily used by persons under the age of 18, unless the defendant receives written permission from the Probation Officer;

15. The defendant shall not associate or have verbal, written, telephonic, or electronic communication with any person under the age of 18, except: (a) in the presence of the parent or legal guardian of said minor; and (b) on the condition that the defendant notify said parent or legal guardian of his conviction in the instant offense. This provision does not encompass persons under the age of 18, such as waiters, cashiers, ticket vendors, etc., whom the defendant must interact with in order to obtain ordinary and usual commercial services;

16. The defendant shall not affiliate with, own, control, volunteer or be employed in any capacity by a business and/or organization that causes the defendant to regularly contact persons under the age of 18;

17. The defendant shall not affiliate with, own, control, or be employed in any capacity by a business whose principal product is the production or selling of

materials depicting or describing "sexually explicit conduct," as defined at 18 U.S.C. § 2256(2);

18. The defendant's employment shall be approved by the Probation Officer, and any change in employment must be pre-approved by the Probation Officer. The defendant shall submit the name and address of the proposed employer to the Probation Officer at least ten days prior to any scheduled change; and

19. The defendant shall submit his person, and any property, house, residence, vehicle, papers, computer, other electronic communication or data storage devices or media, and effects to search at any time, with or without warrant, by any law enforcement or Probation Officer with reasonable suspicion concerning a violation of a condition of supervised release or unlawful conduct by the defendant, and by any Probation Officer in the lawful discharge of the officer's supervision function.

The Court authorizes the Probation Office to disclose the Presentence Report to the substance abuse treatment provider to facilitate the defendant's treatment for narcotic addiction or drug dependency. Further redisclosure of the Presentence Report by the treatment provider is prohibited without the consent of the sentencing judge.

The Court further authorizes the Probation Officer to disclose the Presentence Report, and/or any previous mental health evaluations or reports, to the mental health treatment provider. The treatment provider may provide

information (excluding the Presentence report), to State or local social service agencies (such as the State of California, Department of Social Service), for the purpose of the client's rehabilitation. It is further ordered that the defendant surrender himself to the institution designated by the Bureau of Prisons at or before 12 noon, October 31, 2016. In the absence of such designation, the defendant shall report on or before the same date and time, to the United States Marshal located at United States District Court, 3470 Twelfth Street, Room G122, Riverside, CA 92501.

Defendant is informed of his right to appeal.

Bond is exonerated upon surrender.

The Court hereby recommends that defendant be designated to a facility in Southern California, or as close thereto as possible.

The Court further recommends that defendant be placed in the Bureau of Prisons 500-hour Drug and Alcohol Program, if eligible.

Defendant's oral motion to remain on bond pending appeal is hereby denied.

In addition to the special conditions of supervision imposed above, it is hereby ordered that the Standard Conditions of Probation and Supervised Release within this judgment be imposed. The Court may change the conditions of supervision, reduce or extend the period of supervision,

and at any time during the supervision period or within the maximum period permitted by law, may issue a warrant and revoke supervision for a violation occurring during the supervision period.

September 6, 2016
Date

/s/
Christina A. Snyder,
U. S. District Judge

It is ordered that the Clerk deliver a copy of this Judgment and Probation/Commitment Order to the U.S. Marshal or other qualified officer.

Clerk, U.S. District Court

September 6, 2016
Filed Date

By /s/
C. Jeang, Deputy Clerk

APPENDIX C — ORDER OF THE UNITED STATES COURT OF APPEALS FOR THE NINTH CIRCUIT, FILED DECEMBER 7, 2018

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

No. 16-50339

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

v.

KEITH PRESTON GARTENLAUB,
AKA KEITH PRESON GARTENLAUB,

Defendant-Appellant.

D.C. No. 8:14-cr-00173-CAS-1
Central District of California, Santa Ana
December 7, 2018, Filed

ORDER

Before: WARDLAW and GOULD, Circuit Judges, and PIERSOL,* District Judge.

The panel has voted unanimously to deny the petition for panel rehearing. Judges Wardlaw and Gould vote to

---

* The Honorable Lawrence L. Piersol, United States District Judge for the District of South Dakota, sitting by designation.

deny the petition for rehearing *en banc*, and Judge Piersol so recommends.

The full court has been advised of the petition for rehearing *en banc*, and no judge has requested a vote on whether to rehear the matter *en banc*. Fed. R. App. P. 35.

The petitions for rehearing *en banc* is **DENIED**.

APPENDIX D — RELEVANT STATUTORY PROVISIONS

50 U.S.C.A. § 1804

§ 1804. Applications for court orders

(a) Submission by Federal officer; approval of Attorney General; contents

Each application for an order approving electronic surveillance under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge having jurisdiction under section 1803 of this title. Each application shall require the approval of the Attorney General based upon his finding that it satisfies the criteria and requirements of such application as set forth in this subchapter. It shall include--

(1) the identity of the Federal officer making the application;

(2) the identity, if known, or a description of the specific target of the electronic surveillance;

(3) a statement of the facts and circumstances relied upon by the applicant to justify his belief that--

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or

is about to be used, by a foreign power or an agent of a foreign power;

(4) a statement of the proposed minimization procedures;

(5) a description of the nature of the information sought and the type of communications or activities to be subjected to the surveillance;

(6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive officers employed in the area of national security or defense and appointed by the President with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official--

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the surveillance is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and

(E) including a statement of the basis for the certification that--

(i) the information sought is the type of foreign intelligence information designated; and

(ii) such information cannot reasonably be obtained by normal investigative techniques;

(7) a summary statement of the means by which the surveillance will be effected and a statement whether physical entry is required to effect the surveillance;

(8) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, facilities, or places specified in the application, and the action taken on each previous application; and

(9) a statement of the period of time for which the electronic surveillance is required to be maintained, and if the nature of the intelligence gathering is such that the approval of the use of electronic surveillance under this subchapter should not automatically terminate when the described type of information has first been obtained, a description of facts supporting the belief that additional information of the same type will be obtained thereafter.

Appendix D

(b) Additional affidavits or certifications

The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

(c) Additional information

The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 1805 of this title.

(d) Personal review by Attorney General

(1)(A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, the Director of National Intelligence, or the Director of the Central Intelligence Agency, the Attorney General shall personally review under subsection (a) of this section an application under that subsection for a target described in section 1801(b)(2) of this title.

(B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph may not delegate the authority to make a request referred to in that subparagraph.

(C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in

advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request.

(2)(A) If as a result of a request under paragraph (1) the Attorney General determines not to approve an application under the second sentence of subsection (a) of this section for purposes of making the application under this section, the Attorney General shall provide written notice of the determination to the official making the request for the review of the application under that paragraph. Except when disabled or otherwise unavailable to make a determination under the preceding sentence, the Attorney General may not delegate the responsibility to make a determination under that sentence. The Attorney General shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event the Attorney General is disabled or otherwise unavailable to make such determination.

(B) Notice with respect to an application under subparagraph (A) shall set forth the modifications, if any, of the application that are necessary in order for the Attorney General to approve the application under the second sentence of subsection (a) of this section for purposes of making the application under this section.

(C) Upon review of any modifications of an application set forth under subparagraph (B), the official notified of the modifications under this paragraph shall modify the application if such official determines that such modification is warranted. Such official shall supervise the making of any modification under this subparagraph. Except when disabled or otherwise unavailable to supervise the making of any modification under the preceding sentence, such official may not delegate the responsibility to supervise the making of any modification under that preceding sentence. Each such official shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event such official is disabled or otherwise unavailable to supervise the making of such modification.

Appendix D

50 U.S.C.A. § 1805

§ 1805. Issuance of order

(a) Necessary findings

Upon an application made pursuant to section 1804 of this title, the judge shall enter an ex parte order as requested or as modified approving the electronic surveillance if he finds that--

(1) the application has been made by a Federal officer and approved by the Attorney General;

(2) on the basis of the facts submitted by the applicant there is probable cause to believe that--

(A) the target of the electronic surveillance is a foreign power or an agent of a foreign power: *Provided*, That no United States person may be considered a foreign power or an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power;

(3) the proposed minimization procedures meet the definition of minimization procedures under section 1801(h) of this title; and

(4) the application which has been filed contains all statements and certifications required by section 1804 of this title and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1804(a)(7)(E) of this title and any other information furnished under section 1804(d) of this title.

(b) Determination of probable cause

In determining whether or not probable cause exists for purposes of an order under subsection (a)(2) of this section, a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

(c) Specifications and directions of orders

(1) Specifications

An order approving an electronic surveillance under this section shall specify--

(A) the identity, if known, or a description of the specific target of the electronic surveillance identified or described in the application pursuant to section 1804(a)(3) of this title;

(B) the nature and location of each of the facilities or places at which the electronic surveillance will be directed, if known;

(C) the type of information sought to be acquired and the type of communications or activities to be subjected to the surveillance;

(D) the means by which the electronic surveillance will be effected and whether physical entry will be used to effect the surveillance; and

(E) the period of time during which the electronic surveillance is approved.

(2) Directions

An order approving an electronic surveillance under this section shall direct--

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified communication or other common carrier, landlord, custodian, or other specified person, or in circumstances where the Court finds, based upon specific facts provided in the application, that the actions of the target of the application may have the effect of thwarting the identification of a specified person, such other persons, furnish the applicant forthwith all information, facilities, or technical assistance necessary to accomplish the electronic surveillance in such a manner as will protect its secrecy and produce a minimum of interference with the services that such carrier, landlord, custodian, or other person is providing that target of electronic surveillance;

(C) that such carrier, landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the surveillance or the aid furnished that such person wishes to retain; and

(D) that the applicant compensate, at the prevailing rate, such carrier, landlord, custodian, or other person for furnishing such aid.

(3) Special directions for certain orders

An order approving an electronic surveillance under this section in circumstances where the nature and location of each of the facilities or places at which the surveillance will be directed is unknown shall direct the applicant to provide notice to the court within ten days after the date on which surveillance begins to be directed at any new facility or place, unless the court finds good cause to justify a longer period of up to 60 days, of--

(A) the nature and location of each new facility or place at which the electronic surveillance is directed;

(B) the facts and circumstances relied upon by the applicant to justify the applicant's belief that each new facility or place at which the electronic surveillance is directed is or was being used, or is about to be used, by the target of the surveillance;

(C) a statement of any proposed minimization procedures that differ from those contained in the original application or order, that may be necessitated by a change in the facility or place at which the electronic surveillance is directed; and

(D) the total number of electronic surveillances that have been or are being conducted under the authority of the order.

(d) Duration of order; extensions; review of circumstances under which information was acquired, retained or disseminated

(1) An order issued under this section may approve an electronic surveillance for the period necessary to achieve its purpose, or for ninety days, whichever is less, except that (A) an order under this section shall approve an electronic surveillance targeted against a foreign power, as defined in section 1801(a)(1), (2), or (3) of this title, for the period specified in the application or for one year, whichever is less, and (B) an order under this chapter for a surveillance targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for 120 days, whichever is less.

(2) Extensions of an order issued under this subchapter may be granted on the same basis as an original order upon an application for an extension and new findings made in the same manner as required for an original order, except that (A) an extension of an order under

this chapter for a surveillance targeted against a foreign power, as defined in paragraph (5), (6), or (7) of section 1801(a) of this title, or against a foreign power as defined in section 1801(a)(4) of this title that is not a United States person, may be for a period not to exceed one year if the judge finds probable cause to believe that no communication of any individual United States person will be acquired during the period, and (B) an extension of an order under this chapter for a surveillance targeted against an agent of a foreign power who is not a United States person may be for a period not to exceed 1 year.

(3) At or before the end of the period of time for which electronic surveillance is approved by an order or an extension, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(4) A denial of the application made under section 1804 of this title may be reviewed as provided in section 1803 of this title.

(e) Emergency orders

(1) Notwithstanding any other provision of this subchapter, the Attorney General may authorize the emergency employment of electronic surveillance if the Attorney General--

(A) reasonably determines that an emergency situation exists with respect to the employment of electronic surveillance to obtain foreign intelligence information before an order authorizing such surveillance can with due diligence be obtained;

(B) reasonably determines that the factual basis for the issuance of an order under this subchapter to approve such electronic surveillance exists;

(C) informs, either personally or through a designee, a judge having jurisdiction under section 1803 of this title at the time of such authorization that the decision has been made to employ emergency electronic surveillance; and

(D) makes an application in accordance with this subchapter to a judge having jurisdiction under section 1803 of this title as soon as practicable, but not later than 7 days after the Attorney General authorizes such surveillance.

(2) If the Attorney General authorizes the emergency employment of electronic surveillance under paragraph (1), the Attorney General shall require that the minimization procedures required by this subchapter for the issuance of a judicial order be followed.

(3) In the absence of a judicial order approving such electronic surveillance, the surveillance shall terminate when the information sought is obtained, when the application for the order is denied, or after

the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

(4) A denial of the application made under this subsection may be reviewed as provided in section 1803 of this title.

(5) In the event that such application for approval is denied, or in any other case where the electronic surveillance is terminated and no order is issued approving the surveillance, no information obtained or evidence derived from such surveillance shall be received in evidence or otherwise disclosed in any trial, hearing, or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such surveillance shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(6) The Attorney General shall assess compliance with the requirements of paragraph (5).

(f) Emergencies involving non-United States persons

(1) Notwithstanding any other provision of this chapter, the lawfully authorized targeting of a non-

United States person previously believed to be located outside the United States for the acquisition of foreign intelligence information may continue for a period not to exceed 72 hours from the time that the non-United States person is reasonably believed to be located inside the United States and the acquisition is subject to this subchapter or to subchapter II of this chapter, provided that the head of an element of the intelligence community--

(A) reasonably determines that a lapse in the targeting of such non-United States person poses a threat of death or serious bodily harm to any person;

(B) promptly notifies the Attorney General of a determination under subparagraph (A); and

(C) requests, as soon as practicable, the employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 1824(e) of this title, as warranted.

(2) The authority under this subsection to continue the acquisition of foreign intelligence information is limited to a period not to exceed 72 hours and shall cease upon the earlier of the following:

(A) The employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 1824(e) of this title.

(B) An issuance of a court order under this subchapter or subchapter II of this chapter.

(C) The Attorney General provides direction that the acquisition be terminated.

(D) The head of the element of the intelligence community conducting the acquisition determines that a request under paragraph (1)(C) is not warranted.

(E) When the threat of death or serious bodily harm to any person is no longer reasonably believed to exist.

(3) Nonpublicly available information concerning unconsenting United States persons acquired under this subsection shall not be disseminated during the 72 hour time period under paragraph (1) unless necessary to investigate, reduce, or eliminate the threat of death or serious bodily harm to any person.

(4) If the Attorney General declines to authorize the employment of emergency electronic surveillance under subsection (e) or the employment of an emergency physical search pursuant to section 1824(e) of this title, or a court order is not obtained under this subchapter or subchapter II of this chapter, information obtained during the 72 hour acquisition time period under paragraph (1) shall not be retained, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(5) Paragraphs (5) and (6) of subsection (e) shall apply to this subsection.

(g) Testing of electronic equipment; discovering unauthorized electronic surveillance; training of intelligence personnel

Notwithstanding any other provision of this subchapter, officers, employees, or agents of the United States are authorized in the normal course of their official duties to conduct electronic surveillance not targeted against the communications of any particular person or persons, under procedures approved by the Attorney General, solely to--

(1) test the capability of electronic equipment, if--

(A) it is not reasonable to obtain the consent of the persons incidentally subjected to the surveillance;

(B) the test is limited in extent and duration to that necessary to determine the capability of the equipment;

(C) the contents of any communication acquired are retained and used only for the purpose of determining the capability of the equipment, are disclosed only to test personnel, and are destroyed before or immediately upon completion of the test; and:

(D) *Provided*, That the test may exceed ninety days only with the prior approval of the Attorney General;

(2) determine the existence and capability of electronic surveillance equipment being used by persons not authorized to conduct electronic surveillance, if--

(A) it is not reasonable to obtain the consent of persons incidentally subjected to the surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to determine the existence and capability of such equipment; and

(C) any information acquired by such surveillance is used only to enforce chapter 119 of Title 18, or section 605 of Title 47, or to protect information from unauthorized surveillance; or

(3) train intelligence personnel in the use of electronic surveillance equipment, if--

(A) it is not reasonable to--

(i) obtain the consent of the persons incidentally subjected to the surveillance;

(ii) train persons in the course of surveillances otherwise authorized by this subchapter; or

(iii) train persons in the use of such equipment without engaging in electronic surveillance;

(B) such electronic surveillance is limited in extent and duration to that necessary to train the personnel in the use of the equipment; and

(C) no contents of any communication acquired are retained or disseminated for any purpose, but are destroyed as soon as reasonably possible.

(h) Retention of certifications, applications and orders

Certifications made by the Attorney General pursuant to section 1802(a) of this title and applications made and orders granted under this subchapter shall be retained for a period of at least ten years from the date of the certification or application.

(i) Bar to legal action

No cause of action shall lie in any court against any provider of a wire or electronic communication service, landlord, custodian, or other person (including any officer, employee, agent, or other specified person thereof) that furnishes any information, facilities, or technical assistance in accordance with a court order or request for emergency assistance under this chapter for electronic surveillance or physical search.

Appendix D

(j) Pen registers and trap and trace devices

In any case in which the Government makes an application to a judge under this subchapter to conduct electronic surveillance involving communications and the judge grants such application, upon the request of the applicant, the judge shall also authorize the installation and use of pen registers and trap and trace devices, and direct the disclosure of the information set forth in section 1842(d)(2) of this title.

Appendix D

50 U.S.C.A. § 1806

§ 1806. Use of information

(a) Compliance with minimization procedures; privileged communications; lawful purposes

Information acquired from an electronic surveillance conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No otherwise privileged communication obtained in accordance with, or in violation of, the provisions of this subchapter shall lose its privileged character. No information acquired from an electronic surveillance pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Statement for disclosure

No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

Appendix D

(c) Notification by United States

Whenever the Government intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the Government shall, prior to the trial, hearing, or other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the Government intends to so disclose or so use such information.

(d) Notification by States or political subdivisions

Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof, against an aggrieved person any information obtained or derived from an electronic surveillance of that aggrieved person pursuant to the authority of this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(e) Motion to suppress

Any person against whom evidence obtained or derived from an electronic surveillance to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such electronic surveillance on the grounds that--

(1) the information was unlawfully acquired; or

(2) the surveillance was not made in conformity with an order of authorization or approval.

Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(f) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (c) or (d) of this section, or whenever a motion is made pursuant to subsection (e) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials

relating to electronic surveillance or to discover, obtain, or suppress evidence or information obtained or derived from electronic surveillance under this chapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority, shall, notwithstanding any other law, if the Attorney General files an affidavit under oath that disclosure or an adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the surveillance only where such disclosure is necessary to make an accurate determination of the legality of the surveillance.

(g) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (f) of this section determines that the surveillance was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from electronic surveillance of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the surveillance was lawfully authorized and conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(h) Finality of orders

Orders granting motions or requests under subsection (g) of this section, decisions under this section that electronic surveillance was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to a surveillance shall be final orders and binding upon all courts of the United States and the several States except a United States court of appeals and the Supreme Court.

(i) Destruction of unintentionally acquired information

In circumstances involving the unintentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States, such contents shall be destroyed upon recognition, unless the Attorney General determines that the contents indicate a threat of death or serious bodily harm to any person.

(j) Notification of emergency employment of electronic surveillance; contents; postponement, suspension or elimination

If an emergency employment of electronic surveillance is authorized under subsection (e) or (f) of section 1805 of this title and a subsequent order approving the surveillance

is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to electronic surveillance as the judge may determine in his discretion it is in the interest of justice to serve, notice of--

(1) the fact of the application;

(2) the period of the surveillance; and

(3) the fact that during the period information was or was not obtained.

On an ex parte showing of good cause to the judge the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed ninety days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(k) Coordination with law enforcement on national security matters

(1) Federal officers who conduct electronic surveillance to acquire foreign intelligence information under this subchapter may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 1804(a)(7)(B) of this title or the entry of an order under section 1805 of this title.

Appendix D

50 U.S.C.A. § 1821

§ 1821. Definitions

As used in this subchapter:

(1) The terms "foreign power", "agent of a foreign power", "international terrorism", "sabotage", "foreign intelligence information", "Attorney General", "United States person", "United States", "person", "weapon of mass destruction", and "State" shall have the same meanings as in section 1801 of this title, except as specifically provided by this subchapter.

(2) "Aggrieved person" means a person whose premises, property, information, or material is the target of physical search or any other person whose premises, property, information, or material was subject to physical search.

(3) "Foreign Intelligence Surveillance Court" means the court established by section 1803(a) of this title.

(4) "Minimization procedures" with respect to physical search, means--

(A) specific procedures, which shall be adopted by the Attorney General, that are reasonably designed in light of the purposes and technique of the particular physical search, to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information

concerning unconsenting United States persons consistent with the need of the United States to obtain, produce, and disseminate foreign intelligence information;

(B) procedures that require that nonpublicly available information, which is not foreign intelligence information, as defined in section 1801(e)(1) of this title, shall not be disseminated in a manner that identifies any United States person, without such person's consent, unless such person's identity is necessary to understand such foreign intelligence information or assess its importance;

(C) notwithstanding subparagraphs (A) and (B), procedures that allow for the retention and dissemination of information that is evidence of a crime which has been, is being, or is about to be committed and that is to be retained or disseminated for law enforcement purposes; and

(D) notwithstanding subparagraphs (A), (B), and (C), with respect to any physical search approved pursuant to section 1822(a) of this title, procedures that require that no information, material, or property of a United States person shall be disclosed, disseminated, or used for any purpose or retained for longer than 72 hours unless a court order under section 1824 of this title is obtained or unless the Attorney General determines that the information indicates a threat of death or serious bodily harm to any person.

(5) "Physical search" means any physical intrusion within the United States into premises or property (including examination of the interior of property by technical means) that is intended to result in a seizure, reproduction, inspection, or alteration of information, material, or property, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, but does not include (A) "electronic surveillance", as defined in section 1801(f) of this title, or (B) the acquisition by the United States Government of foreign intelligence information from international or foreign communications, or foreign intelligence activities conducted in accordance with otherwise applicable Federal law involving a foreign electronic communications system, utilizing a means other than electronic surveillance as defined in section 1801(f) of this title.

Appendix D

50 U.S.C.A. § 1823

§ 1823. Application for order

(a) Submission by Federal officer; approval of Attorney General; contents

Each application for an order approving a physical search under this subchapter shall be made by a Federal officer in writing upon oath or affirmation to a judge of the Foreign Intelligence Surveillance Court. Each application shall require the approval of the Attorney General based upon the Attorney General's finding that it satisfies the criteria and requirements for such application as set forth in this subchapter. Each application shall include--

(1) the identity of the Federal officer making the application;

(2) the identity, if known, or a description of the target of the search, and a description of the premises or property to be searched and of the information, material, or property to be seized, reproduced, or altered;

(3) a statement of the facts and circumstances relied upon by the applicant to justify the applicant's belief that--

(A) the target of the physical search is a foreign power or an agent of a foreign power;

(B) the premises or property to be searched contains foreign intelligence information; and

(C) the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from a foreign power or an agent of a foreign power;

(4) a statement of the proposed minimization procedures;

(5) a statement of the nature of the foreign intelligence sought and the manner in which the physical search is to be conducted;

(6) a certification or certifications by the Assistant to the President for National Security Affairs, an executive branch official or officials designated by the President from among those executive branch officers employed in the area of national security or defense and appointed by the President, by and with the advice and consent of the Senate, or the Deputy Director of the Federal Bureau of Investigation, if designated by the President as a certifying official--

(A) that the certifying official deems the information sought to be foreign intelligence information;

(B) that a significant purpose of the search is to obtain foreign intelligence information;

(C) that such information cannot reasonably be obtained by normal investigative techniques;

(D) that designates the type of foreign intelligence information being sought according to the categories described in section 1801(e) of this title; and

(E) includes a statement explaining the basis for the certifications required by subparagraphs (C) and (D);

(7) where the physical search involves a search of the residence of a United States person, the Attorney General shall state what investigative techniques have previously been utilized to obtain the foreign intelligence information concerned and the degree to which these techniques resulted in acquiring such information; and

(8) a statement of the facts concerning all previous applications that have been made to any judge under this subchapter involving any of the persons, premises, or property specified in the application, and the action taken on each previous application.

(b) Additional affidavits or certifications

The Attorney General may require any other affidavit or certification from any other officer in connection with the application.

Appendix D

(c) Additional information

The judge may require the applicant to furnish such other information as may be necessary to make the determinations required by section 1824 of this title.

(d) Personal review by Attorney General

(1)(A) Upon written request of the Director of the Federal Bureau of Investigation, the Secretary of Defense, the Secretary of State, the Director of National Intelligence, or the Director of the Central Intelligence Agency, the Attorney General shall personally review under subsection (a) of this section an application under that subsection for a target described in section 1801(b)(2) of this title.

(B) Except when disabled or otherwise unavailable to make a request referred to in subparagraph (A), an official referred to in that subparagraph may not delegate the authority to make a request referred to in that subparagraph.

(C) Each official referred to in subparagraph (A) with authority to make a request under that subparagraph shall take appropriate actions in advance to ensure that delegation of such authority is clearly established in the event such official is disabled or otherwise unavailable to make such request.

(2)(A) If as a result of a request under paragraph (1) the Attorney General determines not to approve an application under the second sentence of subsection (a) of this section for purposes of making the application under this section, the Attorney General shall provide written notice of the determination to the official making the request for the review of the application under that paragraph. Except when disabled or otherwise unavailable to make a determination under the preceding sentence, the Attorney General may not delegate the responsibility to make a determination under that sentence. The Attorney General shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event the Attorney General is disabled or otherwise unavailable to make such determination.

(B) Notice with respect to an application under subparagraph (A) shall set forth the modifications, if any, of the application that are necessary in order for the Attorney General to approve the application under the second sentence of subsection (a) of this section for purposes of making the application under this section.

(C) Upon review of any modifications of an application set forth under subparagraph (B), the official notified of the modifications under this paragraph shall modify the application if such official determines that such modification is

warranted. Such official shall supervise the making of any modification under this subparagraph. Except when disabled or otherwise unavailable to supervise the making of any modification under the preceding sentence, such official may not delegate the responsibility to supervise the making of any modification under that preceding sentence. Each such official shall take appropriate actions in advance to ensure that delegation of such responsibility is clearly established in the event such official is disabled or otherwise unavailable to supervise the making of such modification.

Appendix D

50 U.S.C.A. § 1824

§ 1824. Issuance of order

(a) Necessary findings

Upon an application made pursuant to section 1823 of this title, the judge shall enter an ex parte order as requested or as modified approving the physical search if the judge finds that--

(1) the application has been made by a Federal officer and approved by the Attorney General;

(2) on the basis of the facts submitted by the applicant there is probable cause to believe that--

(A) the target of the physical search is a foreign power or an agent of a foreign power, except that no United States person may be considered an agent of a foreign power solely upon the basis of activities protected by the first amendment to the Constitution of the United States; and

(B) the premises or property to be searched is or is about to be owned, used, possessed by, or is in transit to or from an agent of a foreign power or a foreign power;

(3) the proposed minimization procedures meet the definition of minimization contained in this subchapter; and

(4) the application which has been filed contains all statements and certifications required by section 1823 of this title, and, if the target is a United States person, the certification or certifications are not clearly erroneous on the basis of the statement made under section 1823(a)(6)(E) of this title and any other information furnished under section 1823(c) of this title.

(b) Determination of probable cause

In determining whether or not probable cause exists for purposes of an order under subsection (a)(2), a judge may consider past activities of the target, as well as facts and circumstances relating to current or future activities of the target.

(c) Specifications and directions of orders

An order approving a physical search under this section shall--

(1) specify--

(A) the identity, if known, or a description of the target of the physical search;

(B) the nature and location of each of the premises or property to be searched;

(C) the type of information, material, or property to be seized, altered, or reproduced;

(D) a statement of the manner in which the physical search is to be conducted and, whenever more than one physical search is authorized under the order, the authorized scope of each search and what minimization procedures shall apply to the information acquired by each search; and

(E) the period of time during which physical searches are approved; and

(2) direct--

(A) that the minimization procedures be followed;

(B) that, upon the request of the applicant, a specified landlord, custodian, or other specified person furnish the applicant forthwith all information, facilities, or assistance necessary to accomplish the physical search in such a manner as will protect its secrecy and produce a minimum of interference with the services that such landlord, custodian, or other person is providing the target of the physical search;

(C) that such landlord, custodian, or other person maintain under security procedures approved by the Attorney General and the Director of National Intelligence any records concerning the search or the aid furnished that such person wishes to retain;

(D) that the applicant compensate, at the prevailing rate, such landlord, custodian, or other person for furnishing such aid; and

(E) that the Federal officer conducting the physical search promptly report to the court the circumstances and results of the physical search.

(d) Duration of order; extensions; assessment of compliance

(1) An order issued under this section may approve a physical search for the period necessary to achieve its purpose, or for 90 days, whichever is less, except that (A) an order under this section shall approve a physical search targeted against a foreign power, as defined in paragraph (1), (2), or (3) of section 1801(a) of this title, for the period specified in the application or for one year, whichever is less, and (B) an order under this section for a physical search targeted against an agent of a foreign power who is not a United States person may be for the period specified in the application or for 120 days, whichever is less.

(2) Extensions of an order issued under this subchapter may be granted on the same basis as the original order upon an application for an extension and new findings made in the same manner as required for the original order, except that an extension of an order under this chapter for a physical search targeted against a foreign power, as defined in paragraph (5), (6), or (7) of section 1801(a)of this title, or against a foreign power, as defined in section 1801(a)(4) of this title, that is not a United States person, or against an agent of a foreign power who is not a United States person, may be for a period not to exceed one year if the judge

finds probable cause to believe that no property of any individual United States person will be acquired during the period.

(3) At or before the end of the period of time for which a physical search is approved by an order or an extension, or at any time after a physical search is carried out, the judge may assess compliance with the minimization procedures by reviewing the circumstances under which information concerning United States persons was acquired, retained, or disseminated.

(e) Emergency orders

(1) Notwithstanding any other provision of this subchapter, the Attorney General may authorize the emergency employment of a physical search if the Attorney General--

(A) reasonably determines that an emergency situation exists with respect to the employment of a physical search to obtain foreign intelligence information before an order authorizing such physical search can with due diligence be obtained;

(B) reasonably determines that the factual basis for issuance of an order under this subchapter to approve such physical search exists;

(C) informs, either personally or through a designee, a judge of the Foreign Intelligence Surveillance Court at the time of such authorization

that the decision has been made to employ an emergency physical search; and

(D) makes an application in accordance with this subchapter to a judge of the Foreign Intelligence Surveillance Court as soon as practicable, but not more than 7 days after the Attorney General authorizes such physical search.

(2) If the Attorney General authorizes the emergency employment of a physical search under paragraph (1), the Attorney General shall require that the minimization procedures required by this subchapter for the issuance of a judicial order be followed.

(3) In the absence of a judicial order approving such physical search, the physical search shall terminate when the information sought is obtained, when the application for the order is denied, or after the expiration of 7 days from the time of authorization by the Attorney General, whichever is earliest.

(4) A denial of the application made under this subsection may be reviewed as provided in section 1803 of this title.

(5) In the event that such application for approval is denied, or in any other case where the physical search is terminated and no order is issued approving the physical search, no information obtained or evidence derived from such physical search shall be received in evidence or otherwise disclosed in any trial, hearing,

or other proceeding in or before any court, grand jury, department, office, agency, regulatory body, legislative committee, or other authority of the United States, a State, or political subdivision thereof, and no information concerning any United States person acquired from such physical search shall subsequently be used or disclosed in any other manner by Federal officers or employees without the consent of such person, except with the approval of the Attorney General if the information indicates a threat of death or serious bodily harm to any person.

(6) The Attorney General shall assess compliance with the requirements of paragraph (5).

(f) Retention of applications and orders

Applications made and orders granted under this subchapter shall be retained for a period of at least 10 years from the date of the application.

Appendix D

50 U.S.C.A. § 1825

§ 1825. Use of information

(a) Compliance with minimization procedures; lawful purposes

Information acquired from a physical search conducted pursuant to this subchapter concerning any United States person may be used and disclosed by Federal officers and employees without the consent of the United States person only in accordance with the minimization procedures required by this subchapter. No information acquired from a physical search pursuant to this subchapter may be used or disclosed by Federal officers or employees except for lawful purposes.

(b) Notice of search and identification of property seized, altered, or reproduced

Where a physical search authorized and conducted pursuant to section 1824 of this title involves the residence of a United States person, and, at any time after the search the Attorney General determines there is no national security interest in continuing to maintain the secrecy of the search, the Attorney General shall provide notice to the United States person whose residence was searched of the fact of the search conducted pursuant to this chapter and shall identify any property of such person seized, altered, or reproduced during such search.

(c) Statement for disclosure

No information acquired pursuant to this subchapter shall be disclosed for law enforcement purposes unless such disclosure is accompanied by a statement that such information, or any information derived therefrom, may only be used in a criminal proceeding with the advance authorization of the Attorney General.

(d) Notification by United States

Whenever the United States intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, against an aggrieved person, any information obtained or derived from a physical search pursuant to the authority of this subchapter, the United States shall, prior to the trial, hearing, or the other proceeding or at a reasonable time prior to an effort to so disclose or so use that information or submit it in evidence, notify the aggrieved person and the court or other authority in which the information is to be disclosed or used that the United States intends to so disclose or so use such information.

(e) Notification by States or political subdivisions

Whenever any State or political subdivision thereof intends to enter into evidence or otherwise use or disclose in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of a State or a political subdivision thereof

against an aggrieved person any information obtained or derived from a physical search pursuant to the authority of this subchapter, the State or political subdivision thereof shall notify the aggrieved person, the court or other authority in which the information is to be disclosed or used, and the Attorney General that the State or political subdivision thereof intends to so disclose or so use such information.

(f) Motion to suppress

(1) Any person against whom evidence obtained or derived from a physical search to which he is an aggrieved person is to be, or has been, introduced or otherwise used or disclosed in any trial, hearing, or other proceeding in or before any court, department, officer, agency, regulatory body, or other authority of the United States, a State, or a political subdivision thereof, may move to suppress the evidence obtained or derived from such search on the grounds that--

(A) the information was unlawfully acquired; or

(B) the physical search was not made in conformity with an order of authorization or approval.

(2) Such a motion shall be made before the trial, hearing, or other proceeding unless there was no opportunity to make such a motion or the person was not aware of the grounds of the motion.

(g) In camera and ex parte review by district court

Whenever a court or other authority is notified pursuant to subsection (d) or (e) of this section, or whenever a motion is made pursuant to subsection (f) of this section, or whenever any motion or request is made by an aggrieved person pursuant to any other statute or rule of the United States or any State before any court or other authority of the United States or any State to discover or obtain applications or orders or other materials relating to a physical search authorized by this subchapter or to discover, obtain, or suppress evidence or information obtained or derived from a physical search authorized by this subchapter, the United States district court or, where the motion is made before another authority, the United States district court in the same district as the authority shall, notwithstanding any other provision of law, if the Attorney General files an affidavit under oath that disclosure or any adversary hearing would harm the national security of the United States, review in camera and ex parte the application, order, and such other materials relating to the physical search as may be necessary to determine whether the physical search of the aggrieved person was lawfully authorized and conducted. In making this determination, the court may disclose to the aggrieved person, under appropriate security procedures and protective orders, portions of the application, order, or other materials relating to the physical search, or may require the Attorney General to provide to the aggrieved person a summary of such materials, only where such disclosure is necessary to make an accurate determination of the legality of the physical search.

(h) Suppression of evidence; denial of motion

If the United States district court pursuant to subsection (g) of this section determines that the physical search was not lawfully authorized or conducted, it shall, in accordance with the requirements of law, suppress the evidence which was unlawfully obtained or derived from the physical search of the aggrieved person or otherwise grant the motion of the aggrieved person. If the court determines that the physical search was lawfully authorized or conducted, it shall deny the motion of the aggrieved person except to the extent that due process requires discovery or disclosure.

(i) Finality of orders

Orders granting motions or requests under subsection (h) of this section, decisions under this section that a physical search was not lawfully authorized or conducted, and orders of the United States district court requiring review or granting disclosure of applications, orders, or other materials relating to the physical search shall be final orders and binding upon all courts of the United States and the several States except a United States Court of Appeals or the Supreme Court.

(j) Notification of emergency execution of physical search; contents; postponement, suspension, or elimination

(1) If an emergency execution of a physical search is authorized under section 1824(d) of this title and a

subsequent order approving the search is not obtained, the judge shall cause to be served on any United States person named in the application and on such other United States persons subject to the search as the judge may determine in his discretion it is in the interests of justice to serve, notice of--

(A) the fact of the application;

(B) the period of the search; and

(C) the fact that during the period information was or was not obtained.

(2) On an ex parte showing of good cause to the judge, the serving of the notice required by this subsection may be postponed or suspended for a period not to exceed 90 days. Thereafter, on a further ex parte showing of good cause, the court shall forego ordering the serving of the notice required under this subsection.

(k) Coordination with law enforcement on national security matters

(1) Federal officers who conduct physical searches to acquire foreign intelligence information under this subchapter may consult with Federal law enforcement officers or law enforcement personnel of a State or political subdivision of a State (including the chief executive officer of that State or political subdivision who has the authority to appoint or direct the chief

law enforcement officer of that State or political subdivision) to coordinate efforts to investigate or protect against

(A) actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power;

(B) sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or

(C) clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power.

(2) Coordination authorized under paragraph (1) shall not preclude the certification required by section 1823(a)(6) of this title or the entry of an order under section 1824 of this title.