NO. 16-50339

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,

PLAINTIFF-APPELLEE,

v.

KEITH PRESTON GARTENLAUB,

DEFENDANT-APPELLANT.

On Appeal from the United States District Court
for the Central District of California, Santa Ana
Case No. 14-cr-00173-CAS

The Honorable Christina A. Snyder, District Court Judge

BRIEF OF AMICI CURIAE ELECTRONIC FRONTIER FOUNDATION AND AMERICAN CIVIL LIBERTIES UNION IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

Mark Rumold
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Phone: (415) 436-9333
Fax: (415) 436-9993
mark@eff.org

Patrick Toomey
Ashley Gorski
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street
18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654

Counsel for Amici Curiae

DISCLOSURE OF CORPORATE AFFILIATIONS AND OTHER ENTITIES WITH A DIRECT FINANCIAL INTEREST IN LITIGATION

Pursuant to Rule 26.1 of the Federal Rules of Appellate Procedure, amici curiae state that no party to this brief is a publicly held corporation, issues stock, or has a parent corporation.

Amici further state that no party or party's counsel authored this brief or contributed money to fund the preparation or submission of this brief. No person other than amici, their members, and their counsel contributed money to fund the preparation or submission of this brief.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Constitutional Provisions

Statutes

Other Authorities

STATEMENTS OF INTEREST

This brief is filed pursuant to Rule 29(a) of the Federal Rules of Appellate Procedure with the consent of all parties.

The Electronic Frontier Foundation ("EFF") is a member-supported, non-profit civil liberties organization that has worked to protect free speech and privacy rights in the online and digital world for 25 years. With roughly 36,000 active donors, EFF represents the interests of technology users in court cases and broader policy debates surrounding the application of law in the digital age. EFF regularly participates as counsel or amicus in cases addressing the Fourth Amendment and electronic surveillance, including foreign intelligence surveillance. *See, e.g.*, *Jewel v. NSA*, 673 F.3d 902 (9th Cir. 2011).

The American Civil Liberties Union ("ACLU") is a nationwide, nonprofit, nonpartisan organization with more than one million members dedicated to the principles of liberty and equality embodied in the Constitution and this nation's laws. The ACLU has appeared before the federal courts in many cases involving the Fourth Amendment, including cases concerning foreign intelligence surveillance. The ACLU represented the plaintiffs in *Clapper v. Amnesty Int'l USA*, 133 S. Ct. 1138 (2013), and is currently counsel in *Wikimedia v. NSA*, 15-2560 (4th Cir.), and *United States v. Muhtorov*, No. 12-cr-00033 (D. Colo.).

INTRODUCTION

The unusual nature of this prosecution requires little elaboration. A citizen's home and his electronic devices—containing decades' worth of personal information—were secretly searched by federal agents. Yet neither he nor his attorneys have ever seen the authorization for that search. And despite the government's invocation of national security to withhold this information, no national security-related prosecution was ever initiated. Rather, the government relied on its wide-ranging digital searches to initiate a prosecution for offenses related to child pornography.

The digital searches in this case raise unique and profound Fourth Amendment problems. As an initial matter, where the government seeks foreign intelligence information pursuant to the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801, *et seq.*, its searches are premised on relaxed constitutional standards, and they sweep more broadly than searches for evidence of criminal activity. Compounding the problem, the FISA-authorized searches in this case involved forensic searches of electronic devices—which pose their own unique Fourth Amendment concerns, as this Court has already recognized. This confluence of factors requires heightened vigilance to ensure that the government's searches comport with the Constitution. Thus, to satisfy the Fourth Amendment, this Court should prohibit the use of non-foreign intelligence information in

criminal investigations and prosecutions when that information is obtained from FISA-authorized, forensic searches of electronic devices, as is the case here.

In addition, given the unusual nature of this prosecution, and the likelihood that the government improperly converted its foreign intelligence search into one for unrelated criminal activity, it is critical that defendant's counsel have access to relevant FISA materials. Disclosure of this information to the defense will ensure that a meaningful and informed Fourth Amendment challenge may be brought.

FACTUAL AND PROCEDURAL BACKGROUND

In January 2014, the FBI performed a secret search of Gartenlaub's home and computers. E.R. 248. The search was authorized by the Foreign Intelligence Surveillance Court ("FISC"), a court with jurisdiction to authorize covert searches of locations within the United States to obtain foreign intelligence information. 50 U.S.C. §§ 1823, 1824. As part of its search, the FBI made wholesale copies of multiple hard drives and digital devices—devices that contained decades' worth of information and hundreds of thousands of files. E.R. 198, 248-49.

The FBI retained and later searched its copies of those devices. The search of three of the hard drives revealed images of child pornography stored on the drives. In August 2014, eight months after its initial search, the FBI obtained a second search warrant, this time from a magistrate judge in the Central District of California, to search for additional child pornography-related evidence in

Gartenlaub's house, car, and storage units. E.R. 243.

Gartenlaub was indicted for receipt and possession of child pornography. E.R. 296. Through pretrial motions, he moved for disclosure of the government's application to the FISC and the FISC's order authorizing the search of his home and computers—information necessary to an informed Fourth Amendment challenge to the FISA searches. The district court denied that motion, adopting verbatim an 11-page proposed order submitted by the government. E.R. 21.

ARGUMENT

I. FISA-AUTHORIZED SEARCHES OF ELECTRONIC DEVICES PRESENT UNIQUE FOURTH AMENDMENT PROBLEMS.

Two types of searches are implicated by this case: FISA-authorized searches and electronic searches of digital devices. Both raise unique and profound Fourth Amendment problems.

"Indiscriminate searches and seizures conducted under the authority of 'general warrants' were the immediate evils that motivated the framing and adoption of the Fourth Amendment." *Payton v. New York*, 445 U.S. 573, 583 (1980). To guard against those prohibited invasions, the Fourth Amendment requires searches of private spaces to satisfy three familiar requirements: they must be authorized by warrants, based "upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or

things to be seized." U.S. Const. amend. IV. The probable cause requirement ensures that "fruits, instrumentalities, or evidence of a crime will be found" in the place to be searched. *Zurcher v. Stanford Daily*, 436 U.S. 547, 554 (1978); *see also Illinois v. Gates,* 462 U.S. 213, 238 (1983). The particularity requirement ensures that "the search will be carefully tailored to its justifications" and does not "take on the character of the wide-ranging exploratory searches the Framers intended to prohibit." *Maryland v. Garrison*, 480 U.S. 79, 84 (1987). Taken together, these requirements ensure that warrants, and the searches conducted pursuant to them, are not "so bountiful and expansive . . . that they constitute a virtual, all-encompassing dragnet." *United States v. Bridges*, 344 F.3d 1010, 1016 (9th Cir. 2003).

A. FISA authorizes broad searches, based on relaxed Fourth Amendment standards, where the government seeks foreign intelligence information.

Searches conducted for foreign intelligence purposes, pursuant to FISA, modify and relax these established constitutional imperatives. *See In re Sealed Case*, 310 F.3d 717, 741 (FISCR 2002) (acknowledging that "a FISA order may not be a 'warrant' contemplated by the Fourth Amendment").

First, FISA-authorized searches are based on an altered probable-cause standard. Generally, probable cause to search exists when there is a fair probability that a search will result in evidence of a crime being discovered. *Gates*, 462 U.S. at

238. In the context of FISA searches, however, the government need not show that *any* evidence will be discovered, or even that a crime has been committed. *In re Sealed Case*, 310 F.3d at 738 ("Congress clearly intended a lesser showing of probable cause for these activities than that applicable to ordinary criminal cases."). Rather, FISA search authorizations "shall" issue if a judge finds there is probable cause to believe "the target of the physical search is a foreign power or an agent of a foreign power," and that "the premises or property to be searched" is owned, used, possessed or in transit to an "agent of a foreign power or a foreign power." 50 U.S.C. § 1824(a)(2)(A), (B). Neither of these showings requires evidence of criminal activity.[1]

Second, FISA search authorizations are not particularized in the same way that traditional search warrants must be. As the Fourth Amendment commands, warrants must particularly describe the place to be searched and the persons or things to be seized. U.S. Const. amend. IV. In a typical case, the object of a search may be "to recover specific stolen or contraband goods" or to seize evidence of a crime. *Camara v. Mun. Court of City & Cty. of San Francisco*, 387 U.S. 523, 535 (1967). In contrast, the object of a FISA-authorized search, "foreign intelligence information," is exceedingly broad. Under FISA, "foreign intelligence

[1] FISA's definitions of "foreign power" and "agent of a foreign power" encompass some criminal activity, but the definitions do not require it. *See* 50 U.S.C. § 1801(a), (b).

information" includes:

> information that relates to, and if concerning a United States person is necessary to, the ability of the United States to protect against . . . actual or potential attack or other grave hostile acts of a foreign power or an agent of a foreign power; . . . sabotage, international terrorism, or the international proliferation of weapons of mass destruction by a foreign power or an agent of a foreign power; or . . . clandestine intelligence activities by an intelligence service or network of a foreign power or by an agent of a foreign power; or . . . information with respect to a foreign power or foreign territory that relates to, and if concerning a United States person is necessary to . . . the national defense or the security of the United States; or . . . the conduct of the foreign affairs of the United States.

50 U.S.C. § 1801(e). Thus, under FISA, although the government must identify the place it intends to search and the types of materials it intends to seize, *see* 50 U.S.C. § 1824(c)(1)(A) - (C), the object of its search is "foreign intelligence information"—an unspecific and elastic category of information that encompasses "the foreign affairs of the United States" and the "national defense or the security of the United States," among other broad categories. 50 U.S.C. § 1801(e)(2)(A), (B).

Unsurprisingly, in practice, FISA's relaxed requirements result in broad and intrusive searches. As the FISC itself has observed, FISA countenances far more sweeping searches of places and property than a typical warrant. *See In re All Matters Submitted to the FISC*, 218 F. Supp. 2d. 611, 617 (FISC 2002) (describing the "breadth" accorded the FBI in FISA searches of a target's "residence, office, vehicles, computer, safe deposit box and U.S. mails"), *rev'd on other grounds*, *In*

re Sealed Case, 310 F.3d 717. Indeed, because of the foreign intelligence needs that FISA searches serve, courts allow these searches to be more permissive along almost every axis—from their initial authorization, to their execution, to the government's retention and analysis of seized material. *See id.* (cataloging the "practices and provisions" of FISA that render such searches exceptionally broad and intrusive).

Finally, one element of FISA renders these invasive searches especially susceptible to misuse: under the statute, obtaining "foreign intelligence information" need not be the only, or even the primary, purpose of a FISA search. Instead, since 2001, the statute has required only that a "significant purpose" of a search be "to obtain foreign intelligence information." 50 U.S.C. § 1823(a)(6)(B); *see In re Sealed Case*, 310 F.3d at 736-746 (upholding "significant purpose" test while warning that "the FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes"); *see also Mayfield v. United States*, 504 F. Supp. 2d 1023, 1042-43 (D. Or. 2007) (finding "significant purpose" standard violated Fourth Amendment), *vacated*, 588 F.3d 1252 (9th Cir. 2009). To be sure, there may be cases where the foreign intelligence information sought by a FISA search would also constitute evidence of criminal activity, and therefore is in service of a specific and overlapping criminal investigation. But this flexibility presents a considerable risk that investigators will use FISA—and the broad

searches it permits—as an end-run around the more restrictive Fourth Amendment rules governing criminal investigations. *Cf. United States v. Truong Dinh Hung*, 629 F.2d 908, 915 (4th Cir. 1980) (rejecting the government's view that "if surveillance is to any degree directed at gathering foreign intelligence, the executive may ignore the warrant requirement of the Fourth Amendment").[2]

In sum, FISA searches are, at best, countenanced on constitutionally expansive showings of probable cause and particularity, predicated on the theory that those searches are carried out to obtain foreign intelligence information, broadly defined.

B. Because of their breadth, FISA searches of personal electronic devices raise unique Fourth Amendment problems.

Because FISA searches are broader and predicated on a lower standard than traditional search warrants, they raise serious constitutional concerns. The problem is compounded when those searches involve electronic devices containing vast amounts of private information.

[2] The Congress that enacted FISA was well aware of these risks. "Congress was concerned about the government's use of FISA surveillance to obtain information not truly intertwined with the government's efforts to protect against threats from foreign powers." *In re Sealed Case*, 310 F.3d at 725. The "significant purpose" amendment did not reflect a retreat from this concern, nor did it grant the government permission to use FISA to pursue unrelated criminal investigations. *See id.* at 736 ("[W]e see not the slightest indication that Congress meant to give that power to the Executive Branch.").

1. The Fourth Amendment protects information held in private places, like computers and hard drives.

The Fourth Amendment expressly protects a person's right to be "secure" in their "papers" and "effects" from government intrusion. U.S. Const. amend. IV. It "embod[ies] a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates." *United States v. Jones*, 565 U.S. 400, 406 (2012).

The Fourth Amendment extends to information stored digitally as well as in tangible papers and effects. "The papers we create and maintain not only in physical but also in digital form reflect our most private thoughts and activities." *United States v. Cotterman*, 709 F.3d 952, 957 (9th Cir. 2013) (en banc). Indeed, because of their immense storage capacity and increasing importance in daily tasks, computers, cell phones and other digital devices hold "a digital record of nearly every aspect of [users'] lives—from the mundane to the intimate." *Riley v. California*, 134 S. Ct. 2473, 2490 (2014).

Because of the wealth of private information digital devices contain, the Supreme Court and this Court have emphasized that searches of personal electronic devices are different than searches in the physical world, requiring special attention to constitutional limitations. *See In re Grand Jury Subpoena, JK-15-029*, 828 F.3d 1083, 1090 (9th Cir. 2016).

This is true for several reasons. First, as the Supreme Court held in *Riley*,

digital searches are not analogous to those of physical containers because digital devices have "immense storage capacity," so the "intrusion on privacy is not physically limited in the same way when it comes to [digital devices]." *Riley*, 134 S. Ct. at 2489. Second, these devices have an "element of pervasiveness" in daily life; nearly everyone uses cell phones and computers on a regular basis for a wide variety of purposes, and a single device will routinely contain many different types of data unlikely to be stored in one place in the physical world. *Id*. at 2490. "Searches of computers therefore often involve a degree of intrusiveness much greater in quantity, if not different in kind, from searches of other containers." *United States v. Payton*, 573 F.3d 859, 862 (9th Cir. 2009). The "uniquely sensitive nature of data on electronic devices" thus renders "an exhaustive exploratory search more intrusive than with other forms of property." *Cotterman*, 709 F.3d at 966.

2. This Court and others have imposed limitations on the searches of digital devices to ensure those searches do not violate the Fourth Amendment.

This Court has recognized the potential for abuse—and the concomitant need for limitations—in searches of vast repositories of electronically stored private information.

Traditionally, courts have viewed the solution to circumscribing intrusive searches as "simple": requiring the government to "get a warrant." *Riley*, 134 S. Ct.

at 2495. However, as early as 1982, this Court recognized that electronic storage might result in intermingling of items described in a warrant and other material that the government had no probable cause to seize. *United States v. Tamura*, 694 F.2d 591, 595-96 (9th Cir. 1982).

In *Tamura*, the government obtained a warrant to seize evidence of payments received by the defendant from records held by his employer. *Id*. at 594. In order to find this evidence, however, agents needed to peruse a lengthy printout of records, identify specific transactions, and obtain corresponding vouchers. Rather than doing so onsite, the government seized the entire set of records and sorted through them later. *Id*. at 595.

The Court held that this violated the Fourth Amendment. *Id*. It noted that "all items in a set of files may be inspected during a search, provided that sufficiently specific guidelines for identifying the documents sought are provided in the search warrant and are followed by the officers conducting the search." *Id*. But "the wholesale seizure for later detailed examination of records not described in a warrant is significantly more intrusive, and has been characterized as 'the kind of investigatory dragnet that the fourth amendment was designed to prevent.'" *Id*. (quoting *United States v. Abrams*, 615 F.2d 541, 543 (1st Cir. 1980)). To protect against "overseizure," the Court outlined a protocol that would allow for offsite sorting and segregation of material not covered by the warrant. *Id*. at 596 & n.3.

In the last 35 years, the problem of overseizure has gone from the "comparatively rare instance[]" described in *Tamura*, 694 F.2d at 595, to "an inherent part of the electronic search process." *United States v. Comprehensive Drug Testing, Inc*. ("*CDT*"), 621 F.3d 1162, 1177 (9th Cir. 2010) (en banc). Indeed, "almost every hard drive encountered by law enforcement will contain records that have nothing to do with the investigation." Department of Justice, Searching and Seizing Computers and Obtaining Evidence in Criminal Investigations 87 (2009).[3] As a result, the government routinely applies for and receives "two-stage search" warrants: first to physically seize a digital storage device and make a complete digital copy or "image" of its contents, and then to analyze the copy using forensic software. *Id*. at 76, 86-87.

Even if overseizure is often necessary when conducting searches of digital devices, it cannot be exploited to evade the Fourth Amendment's restrictions. No matter how investigators conduct a search, they must "avoid turning a limited search for particular information into a general search of office file systems and computer databases." *CDT*, 621 F.3d at 1170; *see also United States v. Galpin*, 720 F.3d 436, 447 (2d Cir. 2013) (risk of digital searches becoming too general "demands a heightened sensitivity to the particularity requirement in the context of digital searches").

[3] *Available at* https://www.justice.gov/sites/default/files/criminal-ccips/legacy/2015/01/14/ssmanual2009.pdf.

This Court's opinion in *CDT* is an instructive example of why digital searches demand heightened sensitivity to the Fourth Amendment's requirements. In that case, government investigators obtained a warrant for drug-testing records of ten Major League Baseball players. 621 F.3d at 1166-67. However, they seized electronic storage devices and copied a directory containing information about hundreds of players, in addition to the ten mentioned in the warrant, and searched all of the files in the directory, despite conditions in the warrant that precluded them from doing so. *Id*. at 1167-68. Nevertheless, the government argued it had complied with the conditions in the warrant and this Court's guidance in *Tamura* because *Tamura* permitted overseizure in certain circumstances. *Id.* at 1170. The government therefore contended that the information it possessed about players outside the search warrant was nonetheless "lawfully seized" and in "plain view," allowing it to be further retained, searched, and used in criminal investigations and prosecutions. *Id*.

The *CDT* Court forcefully rejected this argument because it "would make a mockery of *Tamura*." *Id*. at 1171. The Court called for "greater vigilance on the part of judicial officers" and reiterated that "the process of segregating electronic data that is seizable from that which is not must not become a vehicle for the government to gain access to data which it has no probable cause to collect." *Id*. at 1177. In a concurring opinion joined by four other judges, Judge Kozinski offered

more specific guidance for how authorizing magistrates could impose ex ante search conditions to ensure digital searches remain tailored to evidence for which the government has probable cause. *Id*. at 1178 (Kozinski, J., concurring). These conditions include foreswearing reliance on the plain view doctrine,[4] the use of an independent taint team, and use of a search protocol "designed to uncover only the information for which [the government] has probable cause." *Id*. at 1180.

To avoid particularity problems, search warrants for electronic devices should, at the very least, establish at the outset appropriate safeguards—such as the use of taint teams—to ensure that government investigators access only the items for which there is probable cause. *See Groh v. Ramirez*, 540 U.S. 551, 561 (2004).

In addition, courts reviewing searches of electronic devices after the fact must scrutinize the "reasonableness of the officer's acts both in executing the warrant and in performing a subsequent search of seized materials." *United States v. Hill*, 459 F.3d 966, 978 (9th Cir. 2006). In particular, courts should be skeptical of evidence outside the scope of a warrant that the government claims was in plain view and was therefore lawfully obtained. *CDT*, 621 F.3d at 1171.

[4] The plain view doctrine allows an officer who is lawfully present in a place to seize an item if its illegal nature is "immediately apparent." *Horton v. California*, 496 U.S. 128, 136-37 (1990); *United States v. Lemus*, 582 F.3d 958, 964 (9th Cir. 2009). It is not clear how the plain view doctrine should apply in the context of digital searches, if at all. *See CDT*, 621 F.3d at 1171.

II. TO ENSURE COMPLIANCE WITH THE FOURTH AMENDMENT, THE COURT SHOULD IMPOSE STRICT LIMITATIONS ON THE USE OF INFORMATION OBTAINED FROM FISA-AUTHORIZED, FORENSIC SEARCHES OF ELECTRONIC DEVICES.

FISA searches of electronic devices pose an unusually acute risk of becoming general searches for evidence of criminal activity. Thus, to satisfy the Fourth Amendment, this Court should impose strict limitations on the use of information obtained through these searches.

Specifically, the Court should prohibit the government from using *non*-foreign intelligence information in criminal investigations and prosecutions when that information is obtained during a FISA-authorized, forensic search of an electronic device. *See CDT*, 621 at 1178 (noting such restrictions will ensure "future searches of electronic records" do not turn "all warrants for digital data into general warrants") (Kozinski, J., concurring). In this case, such a prohibition would require the exclusion of the evidence of child pornography used to convict Gartenlaub.

This Court has already called for "vigilance" in "striking the right balance between the government's interest in law enforcement and the right of individuals to be free from unreasonable searches and seizures" when searching electronic devices. *CDT*, 621 at 1177. The extraordinary facts of this case require precisely that kind of vigilance. The Court should not allow foreign intelligence searches, with all of their attendant breadth and secrecy, to become a backdoor to the

exploratory rummaging that is plainly forbidden under the Fourth Amendment.

Two rationales independently support such a use restriction. First, as this Court has recognized, reliance on plain view in electronic searches forms a hazardous constitutional basis for obtaining evidence. *See CDT* 621 F.3d at 1171; *see also id*. at 1180 (Kozinski, J., concurring) (recommending that digital search warrants require foreswearing reliance on plain view). It is inconsistent with *CDT* and *Tamura* to argue that "plain view" can apply to files outside the scope of the warrant. A use restriction on non-foreign intelligence information obtained in a FISA search ensures fidelity to the Fourth Amendment limits set out in those cases. Alternatively, even if an initial seizure of information is itself "reasonable"—the ultimate touchstone of the Fourth Amendment—subsequent uses of lawfully seized information can still violate the Fourth Amendment. *See United States v. Jacobsen*, 466 U.S. 109, 124-125 (1984); *United States v. Sedaghaty*, 728 F.3d 885, 914 (9th Cir. 2013) (invalidating computer search where agents sought to retain and use "information beyond the scope of the warrant" and insisting that agents "should have sought a further warrant"); *cf. Terry v. Ohio*, 392 U.S. 1, 19 (1968) ("The scope of the search must be 'strictly tied to and justified by' the circumstances which rendered its initiation permissible.") (quoting *Warden v. Hayden*, 387 U.S. 294, 310 (1967) (Fortas, J., concurring)). Thus, while the seizure of Gartenlaub's devices may have been permissible at the outset, the later use of information

outside the scope of the FISA authorization was not. *See Jacobsen*, 466 U.S. at 125; *see also* Orin S. Kerr, *Executing Warrants for Digital Evidence: The Case for Use Restrictions on Nonresponsive Data*, 48 Texas Tech L. Rev. 1, 27-29 (2015).

Under either rationale, as this Court recognized in *CDT*, "[e]veryone's interests are best served if there are clear rules to follow that strike a fair balance" between the needs of the government in conducting searches and "the rights of individuals . . . to the privacy that is at the heart of the Fourth Amendment." 621 F.3d at 1177. The prohibition on the use of non-foreign intelligence information obtained through a search of an electronic device is precisely this type of necessary "clear rule." *See* Kerr, *Executing Warrants for Digital Evidence* at 18 ("The best way to minimize the unwarranted intrusions upon privacy for computer searches is to impose use restrictions on the nonresponsive data revealed in the course of the search.").

Although the government has not explained how it found the child pornography on the imaged devices, it seems highly likely that investigators employed techniques or software that went beyond the foreign intelligence purpose of the initial FISA search. Forensic software allows investigators to sift through even very large numbers of files in ways that would be impossible unaided by a computer. For example, common software can scan a computer's contents for child pornography by generating an "overview" of all photos on a computer and

automatically flagging images based on "a library of known files previously submitted by law enforcement—most of which are images of child pornography." *United States v. Mann*, 592 F.3d 779, 781 (7th Cir. 2010). Investigators may have also employed other forensic techniques to search for child pornography. For instance, in *United States v. Johnston*, 789 F.3d 934, 941-42 (9th Cir. 2015), officers executing a search warrant for child pornography conducted several different forensic searches: a "forensic preview" that copied the entire contents of the defendant's computer and flagged child pornography "within five to ten minutes," a subsequent scan that resulted in a gallery of all image and video files on the computer, and, years later, an exhaustive scan of email, chat logs, and "unallocated space" on the computer.[5]

Crucially, if the government "abandoned" its foreign intelligence search and affirmatively searched for evidence of unrelated crimes, the search violated the Fourth Amendment. *Johnston*, 789 F.3d at 942; *United States v. Carey*, 172 F.3d 1268, 1273 (10th Cir. 1999); *United States v. Sarkissian,* 841 F.2d 959, 965 (9th Cir. 1988); *see also In re Sealed Case*, 310 F.3d at 736 ("[T]he FISA process cannot be used as a device to investigate wholly unrelated ordinary crimes."). While the exact course of the government's investigation has never been disclosed,

[5] "Unallocated space is space on a hard drive that contains deleted data, usually emptied from the operating system's trash or recycle bin folder, that cannot be seen or accessed by the user without the use of forensic software." *United States v. Flyer*, 633 F.3d 911, 919 (9th Cir. 2011).

this could have occurred in a number of ways. Investigators may have used forensic software that automatically flagged files known or suspected to contain child pornography near the start of their searches of Gartenlaub's hard drives. Or investigators may have decided to apply those tools only once they grew frustrated at their inability to find evidence of espionage, in the hope of leveraging any evidence of unrelated criminal activity into an espionage confession. In either case, the government's FISA searches were necessarily restricted to "foreign intelligence information," so it is difficult to see how an automated scan for child pornography would serve an authorized purpose.

If the government relied on child pornography-detecting software, similar to that used in *Johnston*, 789 F.3d at 941-42, it plainly exceeded the scope of the FISA authorization. But even if the files were identified manually, the search may have been unlawful. For instance, investigators may have opened individual image or video files located in directories or with file names that had no apparent connection to their foreign intelligence search. *See Carey*, 172 F.3d at 1273 (agent executing warrant for information about drug trafficking violated Fourth Amendment by opening files expecting to find child pornography). Or agents may have encountered images that they suspected contained child pornography, and then applied the FBI's own forensic tools to analyze the images or shared them with the National Center for Missing and Exploited Children for analytic

purposes—without first obtaining a criminal warrant. *United States v. Sedaghaty*, 728 F.3d at 914 (government must obtain a "further warrant" in conducting computer search when it seeks information beyond the scope of its original warrant); *see also Sarkissian*, 841 F.2d at 965 ("At no point was this case an ordinary criminal investigation."). Each of these examples represents a way the government's search of Gartenlaub's devices may have transgressed Fourth Amendment limitations.[6]

The fact that FISA's minimization procedures anticipate the retention and dissemination of "evidence of a crime" in no way alters this analysis. *See* 50 U.S.C. § 1821(4)(C). Unsurprisingly, Congress's primary impetus for allowing this use was to facilitate the prosecution of crimes related to foreign intelligence and national security. *See In re Sealed Case*, 310 F.3d at 724-25 (citing H.R. Rep. No. 95-1283 at 49 (1978)). But even if Congress also contemplated the retention and dissemination of evidence of crimes wholly unrelated to national security, it could not have anticipated the types of searches and seizures at issue here. Congress adopted this rule long before personal electronic devices, storing vast amounts of private information, became widespread. Indeed, when Congress expanded FISA to include physical searches in 1994, it largely imported the minimization

[6] At a minimum, it is clear that the manner in which the electronic searches were conducted matters immensely, yet none of that information has been provided to the defense. *See* Section III; Appellant's Brief 36.

requirements applicable to FISA electronic surveillance, which dated to 1978. *Compare* 50 U.S.C. § 1801(h), *with* 50 U.S.C. § 1821(4).

Without discounting the intrusiveness of traditional wiretaps or physical searches (intrusions that are, without question, substantial), a search of all the information stored on an individual's electronic device represents "a degree of intrusiveness much greater in quantity, if not different in kind." *Payton*, 573 F.3d at 862. As *Riley* teaches, searches of electronic devices may be even *more* intrusive than a physical search of a person's home: an electronic device "not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form." 134 S. Ct. at 2491; *see also id*. at 2489 (describing types of sensitive data found on electronic devices). Such was the case here: the government obtained, reviewed, and ultimately used information stored on Gartenlaub's devices that spanned nearly two decades. *See* E.R. 256 (describing letters allegedly written in 1997). However reasonable Section 1821(4)(C) may be as a general matter, the provision becomes unreasonable when interpreted to authorize a search through two decades of an individual's digital life—and the subsequent use of that information in a criminal prosecution. *See Jacobsen*, 466 U.S. at 125.

The government has argued that it must be able to search broadly for concealed foreign intelligence information. That may well be true, but it cannot be

that the government thereby obtains a general warrant to search personal electronic devices—with all the private information they contain—and can use the fruits of those general searches in wholly unrelated criminal prosecutions. *CDT*, 621 F.3d at 1176-77. To allow that would only amplify the constitutional problems presented by both FISA searches and digital searches in the first instance.

III. THE DISTRICT COURT ERRED BY REFUSING TO DISCLOSE THE FISA MATERIALS TO DEFENDANT'S COUNSEL.

As described above, this case presents serious questions concerning the constitutionality and scope of FISA-authorized searches of electronic devices. Amici believe that even on the limited public record in this case, this Court should hold that the searches of Gartenlaub's hard drives exceeded the government's authority. But even if the Court does not now hold that the FISA search violated the Fourth Amendment, it cannot overlook that it was difficult—if not impossible—for Gartenlaub to meaningfully challenge the lawfulness of those searches and seizures, because the district court denied his counsel the opportunity to review the underlying FISA materials and other critical information about how those searches were actually carried out. The Court should therefore hold, at minimum, that disclosure was necessary to the resolution of Gartenlaub's motions and remand to the district court. *See* 50 U.S.C. § 1825(g).

The confluence of factors in this case—of constitutionally relaxed FISA-authorized searches; the constitutionally suspect search of electronic devices; and

the unusual nature of this investigation and prosecution—all counsel in favor of the need for disclosure of the FISA materials to the defense.

Gartenlaub seeks access to the FISA application and the FISC order that resulted in the search of his house and the seizure of his electronic devices in January 2014. Opening Br. at 36. For the reasons described above, he should also be entitled to any materials describing the protocols imposed by the FISC on the search of his electronic devices, including the government's statutorily required minimization procedures. *See* 50 U.S.C. § 1821(4)(A) (requiring protocols "to minimize the acquisition and retention, and prohibit the dissemination, of nonpublicly available information concerning unconsenting United States persons"). In addition, Gartenlaub's security-cleared counsel should have the opportunity to review information about how the FISA search was actually carried out, since this is crucial to assessing the constitutionality of the government's discovery and use of the evidence against him in this prosecution. *See Hill*, 459 F.3d at 978.

The district court's construction of 50 U.S.C. § 1825(g) conflicts with Gartenlaub's constitutional right to seek suppression of illegally obtained evidence, and this Court should construe Section 1825(g) to require disclosure of FISA materials in at least those cases where, as here, the physical search raises unusually

complex questions of fact and law.[7]

Finally, because due process requires a careful weighing of competing interests in disclosure, this Court should scrutinize the government's claims of privilege closely. Information in the public record undermines the government's repeated, categorical claim that it must withhold all FISA materials from defense counsel. Indeed, it has made identical claims—that *any* disclosure would threaten national security—in every FISA case for the past 35 years. Those general claims of harm are overbroad, given that the government has often disclosed similar information publicly. For example, in this case, the government apparently refused to disclose the relevant FBI minimization procedures to Gartenlaub's counsel even though *other* versions of those minimization procedures are publicly available. *See* Standard Minimization Procedures for FBI Electronic Surveillance and Physical

[7] Both the Fourth and Fifth Amendments require that defendants be afforded a meaningful opportunity to seek suppression of evidence that was obtained illegally. *Sanchez-Llamas v. Oregon*, 548 U.S. 331, 348 (2006); *Franks v. Delaware*, 438 U.S. 154, 155-56 (1978) (hearing on veracity of warrant required where defendant makes "substantial preliminary showing" that affidavit contains false statements or omissions); *see also United States v. Phillips*, 540 F.2d 319, 325–26 (8th Cir. 1976) (due process requires means for defendant to seek suppression remedy). Part of that process, as this Court has held, requires that the government disclose information to a defendant that could affect the outcome of a suppression hearing. *See, e.g.*, *United States v. Gamez-Orduno*, 235 F.3d 453, 461 (9th Cir. 2000).

Search Conducted Under FISA (2008).[8] In other instances, the government has withheld critical information concerning FISA surveillance for years only to inexplicably reverse course when pressed by the courts. *See, e.g.*, Gov't Ex Parte Notice in Response to the Court's Ex Parte Order, *United States v. Mohamud*, No. 14-30217 (9th Cir. Sept. 2, 2016) (ECF 109-2) (explaining that, following court-ordered declassification review, certain FISA information could be released after all). These releases make clear that the Court should not take at face value the government's all-encompassing claim that any disclosure to defense counsel, even under an appropriate protective order, would cause harm.

Under these circumstances, disclosure of FISA materials under appropriate security measures is "necessary" for "an accurate determination of the legality of the physical search." 50 U.S.C. § 1825(g). It is also necessary as a matter of constitutional right.

CONCLUSION

For the reasons explained above, the Court should prohibit the use of non-foreign intelligence information in criminal investigations and prosecutions when

[8] *Available at* https://www.aclu.org/files/pdfs/natsec/faafoia20101129/FAAFBI0707.pdf (obtained via Freedom of Information Act). The government has publicly released other FISA-related minimization procedures as well. *See, e.g.*, FISA 702 Minimization Procedures Used by the FBI (July 24, 2014), *available at* https://www.dni.gov/files/documents/ppd-28/2014%20FBI%20702%20Minimization%20Procedures.pdf.

that information is obtained during FISA-authorized, forensic searches of electronic devices. Alternatively and independently, the Court should require that FISA materials be disclosed to the defense.

Dated: February 15, 2017

Respectfully submitted,

By: /s/ Mark Rumold
Mark Rumold
Andrew Crocker
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
Telephone: (415) 436-9333
mark@eff.org

Counsel for Amici Curiae

Of Counsel:
Patrick Toomey
Ashley Gorski
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Phone: (212) 549-2500
Fax: (212) 549-2654
ptoomey@aclu.org

CERTIFICATE OF COMPLIANCE WITH TYPE-VOLUME LIMITATION, TYPEFACE REQUIREMENTS AND TYPE STYLE REQUIREMENTS PURSUANT TO FED. R. APP. P. 32

Pursuant to Fed. R. App. P. 32(a)(7)(C), I certify as follows:

1. This Brief of Amici Curiae Electronic Frontier Foundation In Support of Defendant-Appellant complies with the type-volume limitation, because this brief contains 6,151 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word 2011, the word processing system used to prepare the brief, in 14 point font in Times New Roman font.

Dated: February 15, 2017

By: /s/ Mark Rumold
Mark Rumold

Counsel for Amici Curiae

CERTIFICATE OF SERVICE

I hereby certify that I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Ninth Circuit by using the appellate CM/ECF system on February 15, 2017.

I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the appellate CM/ECF system.

Dated: February 15, 2017

By: /s/ Mark Rumold
Mark Rumold

Counsel for Amici Curiae