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.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
DISTRICT COURT NO. CR 14-173-CAS

GOVERNMENT'S ANSWERING BRIEF
[PUBLIC REDACTED VERSION]

SANDRA R. BROWN
Acting United States Attorney

PATRICK R. FITZGERALD
Assistant United States Attorney
Chief, National Security Division

DANA J. BOENTE
Acting Assistant Attorney General
National Security Division

JEFFREY SMITH
AMY LARSON
Attorneys
National Security Division

ANTHONY J. LEWIS
VICKI CHOU
Assistant United States Attorneys
National Security Division

1500 United States Courthouse
312 North Spring Street
Los Angeles, CA 90012
Telephone: (213) 894-1786
Email: anthony.lewis@usdoj.gov

Attorneys for Plaintiff-Appellee
UNITED STATES OF AMERICA

TABLE OF CONTENTS

TABLE OF CONTENTS (continued)

DESCRIPTION **PAGE**

TABLE OF CONTENTS (continued)

DESCRIPTION **PAGE**

TABLE OF AUTHORITIES

DESCRIPTION **PAGE(S)**

Federal Cases

TABLE OF AUTHORITIES (continued)

DESCRIPTION **PAGE**

TABLE OF AUTHORITIES (continued)

DESCRIPTION **PAGE**

TABLE OF AUTHORITIES (continued)

DESCRIPTION **PAGE**

TABLE OF AUTHORITIES (continued)

DESCRIPTION **PAGE**

TABLE OF AUTHORITIES (continued)

DESCRIPTION **PAGE**

TABLE OF AUTHORITIES (continued)

DESCRIPTION **PAGE**

TABLE OF AUTHORITIES (continued)

DESCRIPTION **PAGE**

Federal Statutes

TABLE OF AUTHORITIES (continued)

DESCRIPTION **PAGE**

Federal Rules

Other Authorities

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.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
DISTRICT COURT NO. CR 14-173-CAS

GOVERNMENT'S ANSWERING BRIEF [PUBLIC REDACTED VERSION]

I

ISSUES PRESENTED

A. Whether, viewed in the light most favorable to the prosecution and after making all reasonable inferences in support of the verdict, evidence was sufficient to support defendant's conviction for knowingly possessing child pornography that was stored on his

computers, meticulously organized by content, backed up repeatedly, and maintained alongside defendant's personal files.

B. Whether probable cause supported any Foreign Intelligence Surveillance Act ("FISA") applications.

C. Whether the district court erred in denying defendant's request for a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978).

D. Whether the district court plainly erred by failing, *sua sponte*, to conclude that agents exceeded the permissible scope of a court-authorized January 2014 search.

E. Whether the district court erred by concluding, after a thorough *ex parte* and *in camera* review of classified materials, that it was not necessary to disclose any applications to the Foreign Intelligence Surveillance Court ("FISC") in order to analyze defendant's legal challenges.

II

STATEMENT OF THE CASE

Following a jury trial, defendant Keith Preston Gartenlaub ("defendant") was convicted of possessing child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). He now challenges that

conviction, claiming that evidence was insufficient to support the verdict and that the district court erred in denying pretrial motions related to the Fourth Amendment and the Foreign Intelligence Surveillance Act ("FISA"), 50 U.S.C. § 1801 *et seq*. Neither the jury nor the district court erred. Defendant's conviction should be affirmed.

A. Jurisdiction, Timeliness, and Bail Status

This Court has jurisdiction pursuant to 28 U.S.C. § 1291. The district court had jurisdiction pursuant to 18 U.S.C. § 3231. Judgment was entered on September 6, 2016. (CR 216; ER 1.)[1] Notice of Appeal was timely filed on September 8, 2016. (CR 220; ER 32.) *See* Fed. R. App. P. 4(b)(1)(A)(i). Defendant is in custody.

[1] "CR" refers to the Clerk's Record in the district court and "Docket No." refers to the electronic docket in this court; each is followed by the docket number. "RT" refers to the reporter's transcript of proceedings and is preceded by the date and followed by applicable page references. "Exh." refers to the government's trial exhibits and is followed by the applicable exhibit number. "ER" refers to the Excerpts of Record filed by defendant, "AOB" refers to Appellant's Opening Brief, "GER" refers to the Government's Excerpts of Record, and "CSER" refers to the Government's Classified Sealed Excerpt of Record; such references are followed by applicable page references.

B. Statement of Facts and Procedural History

In October 2014, defendant was charged with possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B). (CR 36; ER 297.)[2] As the indictment alleged, in August 2014, defendant possessed four hard drives, each of which contained child pornography.

1. June 2013, January 2014, and August 2014 Searches

The specific date alleged in the indictment—August 27, 2014—was the day Federal Bureau of Investigation ("FBI") agents seized defendant's hard drives and computers pursuant to warrants issued by a United States Magistrate Judge. (ER 297, 322-23.) Those warrants, issued under Federal Rule of Criminal Procedure 41, authorized agents to search defendant's home, storage units, and computers for evidence of child pornography (the "August 2014 searches" and "August 2014 warrants"). (*See* ER 322.)

[2] Defendant was also charged with, and ultimately convicted of, receipt of child pornography, in violation of 18 U.S.C. § 2252A(a)(2)(A). (ER 296.) The district court vacated this conviction as multiplicitous. (ER 8; *see* CR 179-181, 208- 210.)

As set forth in the affidavit supporting the August warrants, however, the FBI had performed two prior court-authorized searches relevant to this appeal:

First, in June 2013, a United States Magistrate Judge issued a warrant authorizing the search of defendant's e-mail account (the "2013 e-mail warrant" and "2013 e-mail search"). (ER 327, 362.) In the affidavit supporting this warrant, FBI Special Agent Wesley Harris summarized an investigation into the leak of sensitive design details of the Boeing C-17 military cargo aircraft to the Chinese government, and the evidence pointing to defendant's role therein. (ER 327-32; *see* ER 378-416.) Five e-mails found during the 2013 e-mail search were later referenced in the affidavit supporting the August 2014 warrants, identified as evidence connecting defendant to his former residence, indicating he used certain computer folders, and reflecting the date he purchased a hard drive. (ER 327 n.2.)

Second, in January 2014, agents conducted a court-authorized search without notice of defendant's former residence in Irvine, California. (ER 322.) During that search, agents obtained copies of hard drives on which agents found child pornography. (ER 322-23.)

Specifically, each drive contained a folder labeled "OrigData," subfolders of which contained an organized collection of child pornography. (*Id.*) The affidavit supporting the August 2014 warrants detailed agents' discovery of child pornography on these drives and reviewed evidence indicating defendant's awareness of that pornography. (ER 323-26.)

2. Pretrial Litigation

On August 27, 2014, the same day FBI agents conducted the August 2014 search, defendant was arrested for possession of child pornography. (CR 1; *see* ER 301.) The same day, the government filed a notice of intent to use or disclose information obtained pursuant to FISA. (CR 9; GER 1.)

Following his indictment, defendant filed two relevant pretrial motions, (1) alleging material omissions and misstatements in the affidavits supporting the August 2014 searches and the 2013 e-mail warrant, seeking a hearing pursuant to *Franks v. Delaware*, 438 U.S. 154 (1978) (CR 67, 70, 73), and (2) seeking access to any FISA applications and moving to suppress any fruits thereof (CR 70, 73; GER 3, 858).

a. *Franks* Motion

i. Arguments

In a motion styled as a motion to traverse, defendant sought a *Franks* hearing with respect to the affidavits supporting both the August 2014 warrants and the 2013 e-mail warrant. (CR 73; GER 900, 962.) As relevant here, defendant attacked various statements in the affidavit supporting the 2013 e-mail warrant, the affidavit of FBI Special Agent Wesley Harris ("Harris affidavit").[3] Defendant alleged that the Harris affidavit contained numerous misrepresentations or missions regarding the timeframe in which defendant was assigned to work on the C-17 (GER 890-91), technical details about Boeing's network architecture (GER 891-94), defendant's financial status and transactions (GER 895-96), and defendant's and his wife's contacts with China (GER 897-98).

Defendant supported his motion with only a bare-bones declaration, stating that the motion "set[] forth information concerning

[3] On appeal, defendant has not renewed his additional arguments regarding the affidavit supporting the August 2014 warrant, nor other arguments regarding the legality of that warrant and search. The district court analyzed these claims at length and properly rejected them. (*See* ER 334-38, 342-50.)

the Boeing computer system and the role of myself and my team members." (CR 73 Ex. I; GER 1146.) Defendant likewise purported to adopt counsel's pleading as defendant's own statement. (*Id.*)

In opposition, the government noted defendant's failure to supply any specific evidence, as required to make a preliminary showing that Harris intentionally or recklessly omitted or misstated information in his affidavit. (CR 87; GER 1276-78.) Indeed, the government cited several examples of evidence included by Harris that undermined or were neutral with respect to probable cause, evidencing the affiant's scrupulousness in his disclosures to the magistrate judge. (*Id.*) More broadly, the government rebutted defendant's claimed misstatements with evidence on which Harris relied. (*E.g.*, GER 1290-91, 1355-78.) For example, although defendant took issue with the affiant's description of Boeing's network architecture and personnel, the affiant's description closely followed documents on which he relied, including reports of defendant's own interviews. (GER 1280-83.) And even if some or all of defendant's claims were credited, no statement he identified was material to probable cause; even absent the challenged

statements, the Harris affidavit established probable cause supporting the e-mail warrant. (GER 1280-95.)

ii. Order

The court subsequently denied defendant's motion. (CR 115; ER 321-40; *see also* 8/6/15 RT 21-22; GER 208-09.) In a lengthy written order, the court summarized information from the Harris affidavit. (ER 327-32.) After noting relevant standards, the court concluded that even "assuming arguendo that the Harris Affidavit contained deliberate or reckless misstatements or omissions, a *Franks* hearing would not be required because none of the evidence obtained from the email warrant was necessary to find [] probable cause for the August 2014 searches during which the evidence defendant seeks to suppress was seized." (ER 338 (citing *United States v. Vasey*, 734 F.2d 782, 788 (9th Cir. 1987).) This was because, even without e-mails obtained from the 2013 e-mail search, the affidavit supporting the 2014 warrant established probable cause to believe that defendant lived at his former residence, used particular folders, and possessed a particular drive. (ER 338-39.)

In addition, the court concluded that defendant failed to make the "requisite showing of materiality and untruthfulness so as to justify an

evidentiary hearing." (ER 339.) Instead, several "purported misstatements and omission ignore or misread language in the [Harris] affidavit," while others were "immaterial," and others "challenge the veracity of other persons besides the affiant." (ER 339.) Defendant showed, at most, that the "FBI could have investigated more thoroughly, included additional information in the affidavit beyond what was needed to establish probable cause, or explored alternative inferences." (*Id.*) But, as precedent established, mere "negligence" is "not sufficient to warrant a *Franks* hearing." (*Id.* (quoting *United States v. Burnes*, 816 F.2d 1354, 1357 (9th Cir. 1987).) Nor was a hearing required simply because the affiant "did not include all information in the government's possession" or list "every conceivable conclusion." (ER 339-40 (citing cases).)

The court also noted that defendant's cursory declaration, purporting to adopt statements in his counsel's pleading as evidence, arguably violated *Franks*'s requirement that an affidavit or other reliable evidence support defendant's attempt to make a preliminary showing. (ER 339 n.9 (citing *United States v. Wardlow*, 951 F.2d 1115, 1116 (9th Cir. 1991) (rejecting similar declaration)).) It also violated

the Central District of California's Local Criminal Rules, which require that motions to suppress be "supported by a declaration on behalf of the defendant, setting forth all facts then known upon which it is contended the motion should be granted." (*Id.* (citing C.D. Cal. Crim. L-R. 12-1).)

b. Motion for Disclosure and Suppression of FISA Materials

i. Arguments

Defendant, having received the government's FISA notice, likewise moved to suppress any information obtained or derived from FISA search or surveillance (*i.e.*, "FISA information"). (CR 70; GER 3.) Defendant did not have access to any FISA applications; accordingly, he again focused on statements in the Harris affidavit, using those statements as a proxy for what he believed would have been submitted to the FISC. (GER 17, 23, 25, 29, 32.) So doing, he argued that any applications to the FISC failed to establish probable cause and included reckless or intentional material falsehoods requiring a *Franks* hearing. (GER 15, 27-30, 39.) Defendant also claimed that minimization may not have been performed because "agents seemingly did not limit their search to foreign intelligence." (GER 33-34.) He likewise argued that FISA materials should be disclosed, *inter alia*, because they may

include information subject to *Brady v. Maryland*, 373 U.S. 83 (1963), and were necessary to his defense under the Sixth Amendment. (GER 22-25, 36-38.)

The government opposed. (CR 82; GER 58, 60.) In addition to an unclassified opposition available to defendant and his counsel, the government submitted a classified, sealed appendix *ex parte* and *in camera*, as well as a classified version of an opposition brief. (CR 80.) In its unclassified opposition, the government set forth legal requirements for FISA applications and orders, including what must be contained in a FISA application (GER 63-64), required certifications (GER 65-66), minimization procedures (GER 66), and the relevant standard for probable cause (GER 72-73, 84-85, 98-100). *See generally* 50 U.S.C. §§ 1806(e), 1825(f).[4] In addition, the government described the framework for district-court review of such orders. (GER 72.) *See* 50 U.S.C. §§ 1806(e), 1825(f).

[4] Parallel citations are generally to the provisions of FISA permitting surveillance (50 U.S.C. §§ 1802-1806, often referred to as "Title I") and authorizing physical searches (50 U.S.C. §§ 1821-1825, or "Title III"). Defendant received notice pursuant to both Titles, 50 U.S.C. §§ 1806(c), 1825(d). (CR 9; GER 1-2.)

Notably, the government submitted a declaration from the Attorney General stating under oath that disclosure of FISA materials would harm the national security of the United States. (CR 79; GER 41.) Accordingly, under FISA, the district court was required to review FISA materials "in camera and ex parte . . . to determine whether the surveillance if the aggrieved person was lawfully authorized or conducted." 50 U.S.C. §§ 1806(f), 1825(g). (*See* CR 82; GER 73-74.) In addition, the court could disclose FISA materials "only where such disclosure [was] necessary to make an accurate determination of the legality of the surveillance" or search. 50 U.S.C. §§ 1806(f), 1825(g). (*Id.*) Thus, disclosure is authorized only if the district court was unable to determine the legality of any FISA-related surveillance or searches absent the assistance of defense counsel. *Id.* (GER 102-05.) As the government informed the district court, every prior court to have ruled on a motion to disclose FISA materials under this standard—save one district court later reversed on appeal—had held that disclosure was unwarranted. (GER 75-77 (citing cases).)

After discussing minimization standards relevant to FISA (GER 91-95), the government again argued that defendant had failed to make

the required preliminary showing justifying hearing under *Franks* (GER 105-07). Neither any FISA materials nor the Harris affidavit (which defendant presumed to contain similar information) reflected any knowing or reckless false statements or omissions, and the bare allegation of such statements was insufficient to justify disclosure under FISA. (*Id.*)

[CLASSIFIED INFORMATION REMOVED]

ii. Order following review of classified materials

As required by FISA, the district court conducted an *ex parte*, *in camera* review of classified materials submitted by the government. (CR 114; ER 21-31; *accord* 8/29/16 RT 21-22; GER 808 (the court "spent a long time looking at all the stuff" submitted by the government).) Thereafter, it denied defendant's motion, "firmly convinced" that the government did what it was required to do under the law. (8/29/16 RT 21-22; GER 808-09.) At a hearing, the court confirmed it had "reviewed the documents with great care" and stated it "believe[d] the government has complied with the rules in making FISA applications," and that it was "going to sign the proposed order[] submitted by the government because I think it's accurate and is appropriate." (8/6/15 RT 3-4; GER

190-91.) The court was "satisfied that the decision on the FISA warrant and order is appropriate having reviewed the files." (8/16/15 RT 21; GER 208.)

In the later-issued order, the court found that each application satisfied FISA's requirements and that disclosure was not warranted. (ER 23-25.) Under either a *de novo* or deferential standard, the court found that materials established probable cause under FISA. (ER 28.) Specifically, the court found that each application "contained facts establishing probable cause to believe that the target of the electronic surveillance, physical searches, or both, was at the time an agent of a foreign power," 50 U.S.C. §§ 1801(b)(2), 1805(a)(2)(A), 1824(a)(2)(A). (ER 23-24.) Likewise, each application established probable cause to believe that the "facilities or places at which the electronic surveillance was directed" and the "premises or property to be searched" was under requisite control by a foreign power, *id.* §§ 1805(a)(2)(B), 1824(a)(2)(B), and "contained foreign intelligence information," *id.* §§ 1823(a)(3)(B), 1824(a)(4). (ER 24 ¶¶ 5-7.)

The court also found that neither FISA nor due process required disclosure of the materials. The court "d[id] not require the assistance

of the defense to make an accurate determination of the legality of the electronic surveillance and physical searches." (ER 27.) Thus, there was no "legal reason for disclosure of any of the FISA materials to the defendant." (*Id.* (citing cases).) Instead, those materials themselves "provide[d] all the information needed to address the defendant's motion." (*Id.*) Due process also did not require disclosure of the FISA materials to defendant. (ER 28.) Although the court considered whether the materials "contain any information that due process requires to be disclosed to the defendant (*e.g.*, *Brady* material)," the court found, "They d[o] not." (ER 26 n.3.)

Finally, no *Franks* hearing was warranted. (ER 29.) Defendant made no substantial showing "that a false statement knowingly and intentionally, or with reckless disregard for the truth, was included in the FISA materials," nor that any such statement was "necessary to the FISC's approval of the application." (ER 29-30 (punctuation omitted)). Although defendant had not himself reviewed the FISA materials, the court itself made "an independent review of all the materials and . . . determined that there is no indication of any false statements having

been included in the FISA materials." (ER 30 (citing case endorsing this approach).)[5]

3. Trial

Defendant proceeded to trial in December 2015.

Evidence presented at trial showed that defendant possessed four different devices containing child pornography: (1) an Acer computer seized from his home, (2) an external hard drive seized from an Extra Storage unit, and (3-4) two hard drives inside a Dell computer, seized from a Public Storage unit. (12/8/2015 RT 27-29, 48, 53-54, 74-75, 106; GER 228-30, 249, 254-55, 275-76, 298.) On these devices were multiple copies of nearly 100 unique child-pornographic files. Most of the children depicted in this collection were under 12; some were as young

[5] Months later, at a hearing on defendant's post-trial motions, the court expressed "some personal questions regarding the propriety of the FISA court proceeding even though that certainly seems to be legally authorized." (4/18/16 RT 9-10; GER 777-78.) However, notwithstanding these "personal questions," the court affirmed that it was "firmly of the belief that in securing the warrant which lead to the discovery of the information that is the subject of the current indictment, the government did comply with the law." (4/18/16 RT 9; GER 777.) The government did "exactly what it's required to do under the law," (4/18/16 RT 11; GER 779.)

as four. (12/8/2015 RT 148-50, 153-54, 211, 214-15; 12/9/2015 RT 381-83, 386; GER 337-39, 342-43, 347, 350-51.)

Evidence supporting defendant's possession of these devices was overwhelming. The Acer computer was in defendant's home, where he was present when officers executed their search. (12/8/2015 RT 29, 48-49, 59; GER 230, 249-50, 260; *see* 12/8/2015 RT 55-58; GER 256-59.) Likewise, defendant rented each of the public storage units in his own name (Ex. 12-16, 32-33; 12/8/2015 RT 55-58; GER 256-59, 418-26, 428-39) and stored other personal items there (12/8/2015 RT 32-33; Ex. 26; GER 233-34, 427). Defendant logged onto Extra Space's website from his work computer, reviewing information regarding the unit he rented there. (12/8/2015 RT 129-31, Ex. 47; GER 321-23, 481-514.).

The organization of defendant's child pornography collection reflected that his possession was neither unknowing nor inactive. In each of defendant's hard drives, a forensic examiner found one or multiple copies of a large, user-created folder called "OrigData." (12/8/2015 RT 168-69, 181-82; Ex. 55 at 6; ER 56-57, 69-70; GER 529.) These copies were made or transferred at various times between 2005 and 2013. (*See* 12/8/2015 RT 172-81; Ex. 55; ER 60-69.) In total, the

forensic examiner found seven copies of "OrigData" on the seized devices. (12/8/2015 RT 181-83, Ex. 55 at 6; ER 69-71; GER 529.)

Inside each "OrigData" folder was a meticulously organized set of subfolders containing both child pornography and defendant's personal files. Child pornography—nearly 100 unique files—was organized in content-based subfolders, including "yg" (containing files depicting "young girls") and "vi" (containing videos from the "Vicky" series). (12/8/2015 RT 189-91, 205-06; 12/9/2015 RT 281-82; ER 77-79, 93-94, 152-53.) Incompletely downloaded files were in the subfolder "partials." (12/8/2015 RT 217-18, 222-23, 226, 231-32; ER 98-99, 103-04, 107, 112-13.) Many of the files had names descriptive of or commonly seen in child pornography, including "pedophilia," "babyj," preteen," "childlover," and "9yr." (12/8/2015 RT 194-198; ER 82-86.) But even files with non-descriptive names (such as "15 (2)" and "137.mpg") were sorted, reflecting that defendant manually moved them into a desired, content-based folder after viewing them. (12/8/2015 RT 191, 205-09; Ex. 68 at 15; ER 79, 93-97; GER 545.)

Data indicated that these child pornographic files were first downloaded, likely from a peer-to-peer file sharing service, in 2002 and

2003. (12/8/2015 RT 217-20, Ex. 85; ER 98-101; GER 710-16.) During that time, given slower internet speeds, it could have taken days to download each video. (12/9/2015 RT 370-71; ER 231-32.) Over the following years, defendant repeatedly accessed, moved, and altered his collection. Partially downloaded files in the "partials" folder—including titles such as "real kiddie," "pedo," underage" and "7 YO kidandpolicemen . . . child porn sex underage illegal incest"—evidenced continued peer-to-peer downloading efforts through July 2004. (12/8/2015 RT 222-24, Exs. 77-81; ER 103-05; GER 669-706.) Likewise, between backups in March 2005 and March 2006, one of the "parent" sub-folders within "OrigData" containing child pornography was renamed from "tmp" to "nmp." (12/8/2015 RT 236, 251-52; ER 117, 132-33.) Within the "yg" child pornography folder, two new sub-folders were created. (12/9/2015 RT 284-85; ER 155-56.) Nearly 2,000 files were also added to "OrigData" in that period, the bulk of them being adult pornography. (12/9/2015 RT 271-72; ER 142-43.)

Other files were deleted, moved, or renamed, reflecting continuing organizational efforts. (12/9/2015 RT 273-78; ER 144-49.) For example, one copy of "vicky_good_daughter_2" was deleted between two backups,

and a copy of "Vicky complete" was moved to the more specific "vi" folder (and also manually renamed to "Vicky completeR"). (12/9/2015 RT 273-75; Ex. 85 at 1-2; ER 144-46, GER 710-11.) Three other child pornography files were moved from "LStemp" to the "anp" subfolder of "yg," and a "kiddy wow" file was moved from "LStemp" to a new folder called "check," and did not appear at all in another version of "OrigData." (12/9/2015 RT 275-76, 297; Ex. 85 at 1-2; ER 146-47, 168, GER 710-11.) A file called "childlover - anya complete" was renamed "anya complete." (12/9/2015 RT 297, Ex. 85; ER 168, GER 710-16.) In general, all the files moved from "LStemp" to a "more specific folder." (12/9/2015 RT 278; ER 149.)

Digital logs reflected that, when "OrigData" was backed up, so too were defendant's personal files and Internet favorites. (12/8/2015 RT 182-83, 241, 249-50; Exs. 68-76; ER 71, 122, 130-31, GER 531-668.) Among these were materials related to defendant's job at Boeing, organized in a sub-folder labeled "boeing." (12/8/2015 RT 191; ER 79.) In another sub-folder called "fla," defendant stored naked photographs of himself—photographs he e-mailed to himself as recently as April 2010. (12/8/2015 RT 40-45, 234-38; Exs. 34, 38A-40A, 47; ER 119-23,

GER 241-46, 440-55.) Other files in versions of "OrigData" included a message providing defendant's e-mail address. (12/9/2015 RT 291-93, Ex. 42; ER 162-64, GER 473; *see* 12/8/15 RT 40-45; Exs. 43-45; GER 241-46, 475-80.) Likewise, in another folder ("data") backed up the same day as "OrigData," agents found other personal photos of defendant taken with the same camera as the naked photographs. (12/8/2015 RT 245-247; Ex. 41; ER 126-28; GER 456-72.)

Finally, defendant used the computers containing child pornography. On the Dell computer, for example, there was a password-protected user account called "Keith." (12/9/2015 RT 298-300; ER 169-71.) "Keith" accessed the folder structure for "OrigData" in October 2012 and December 2013, including specific folders containing child pornography, such as "vi." (12/9/2015 RT 301-02, 316-18, 322-23, 377; ER 172-73, 177-79, 183-84, 238.)[6] A forensic examiner demonstrated that, when accessing these subfolders, "Keith" navigated through parent folders also containing child pornography, including

[6] Because of the settings of the media player, it was impossible to tell which individual child pornography videos had been accessed. (12/9/2015 RT 314-16; GER 175-77.)

files with explicit names such as "pedofilia," "xchild porn kiddy underage," and "R@ygold." (12/9/2015 RT 317-20, 377, Ex. 84; ER 178-81, 238, GER 707-09.) The Acer seized from defendant's home similarly had a password-protected user account called "Keith." (12/9/2015 RT 321; ER 182.) "Keith" copied the entire "OrigData" folder onto the Acer, by transferring the file from the Dell computer. (12/9/2015 RT 321-22; ER 182-83.) "Keith" made one such copy in October 2013, just an hour after accessing a folder of child pornography on the Dell computer itself. (12/9/2015 RT 322-23, Ex. 84 at 1; ER 183-84, GER 707.)

4. Defense Case

Defendant called three witnesses, a former landlord and two friends, who testified that defendant previously lived in a beachside apartment where he had many social visitors who at times could access his computer. (12/9/2015 RT 401-05, 412-17, 419-24; GER 378-82, 389-94, 396-401.) He also previously dated a woman whose adolescent son had free access to defendant's house. (*Id.*) Each witness also vouched for defendant's good character. (*Id.*)

5. Verdict and Sentencing

The jury found defendant guilty. (CR 167; GER 409-11.)

The court denied defendant's subsequent motions to set aside the verdict, concluding that the government "presented significant circumstantial evidence that defendant knew his computer contained child pornography." (ER 11; *see* CR 172 (motion).) The court sentenced defendant to 41 months' imprisonment, to be followed by a lifetime period of supervised release. (CR 216; ER 1-2.)

III

SUMMARY OF ARGUMENT

Defendant's conviction should be affirmed. Far more than sufficient evidence supported defendant's conviction for knowing possession of child pornography. A forceful "chain of logic" linked defendant to the collection of child pornography on his computers—reflecting his sorting, copying, and curation of that collection over time. *United States v. Begay*, 673 F.3d 1038, 1043-45 (9th Cir. 2011) (*en banc*). Defendant's contrary arguments on appeal are foreclosed by the standard of review.

The district court's rulings with respect to any FISA applications were likewise correct. Probable cause supported any such applications, as the district court confirmed after a thorough *in camera* and *ex parte*

review. Defendant failed to make the requisite showing justifying a hearing under *Franks v. Delaware*, 438 U.S. 154 (1978), demonstrating no false statements or omissions, much less any that were deliberate, reckless, or material. Agents did not plainly exceed the scope of any FISA order. Finally, defendant has not shown why the district court's *in camera* and *ex parte* review—consistent with procedures mandated by FISA and upheld by every court to address them—was insufficient. Disclosure of classified materials to defendant was neither necessary nor compelled by due process.

IV

ARGUMENT

A. Evidence Supports Defendant's Conviction for Possession of Child Pornography

Defendant challenges the sufficiency of evidence supporting his convictions by rearguing inferences that the jury rejected, emphasizing the purported "absence of evidence" that defendant downloaded or accessed child pornography stored on his computers (AOB 15) and the possibility that other people put it there (AOB 2-3). These contentions are foreclosed by the standard of review. "[I]n determining the sufficiency of circumstantial evidence, the question is not whether the

evidence excludes every hypothesis except that of guilt but rather whether the trier of fact could reasonably arrive at its conclusion." *United States v. Nevils*, 598 F.3d 1158, 1165 (9th Cir. 2010) (*en banc*). Accordingly, the Court begins any sufficiency analysis by "construe[ing] the evidence at trial in the light most favorable to the prosecution," resolving any conflicts in favor of—not contrary to—the verdicts. *Id.*; *accord Begay*, 673 F.3d at 1043-45. Viewed under this standard, the evidence against defendant was far more than sufficient. His conviction must be affirmed.

1. Standard of Review

The sufficiency of evidence to support a conviction is governed by *Jackson v. Virginia*, 443 U.S. 307, 319 (1979), under which this Court determines, "after the viewing the evidence in the light most favorable to the prosecution," whether "*any* rational trier or fact could have found the essential elements of the crime beyond a reasonable doubt." *Id.* The Court first considers evidence "in the light most favorable to the prosecution." *Nevils*, 598 F.3d at 1164. Doing so, the Court "may not usurp the role of the [jury] by considering how it would have resolved the conflicts, made the inferences, or considered the evidence at trial,"

but must presume "that the [jury] resolved any such conflicts in favor of the prosecution, and must defer to that resolution." *Id.* (punctuation omitted). As a result, the government does not "need to rebut all reasonable interpretations of the evidence that would establish the defendant's innocence" or rule out every exculpatory hypothesis. *Id.*

After viewing the evidence in this light, the Court analyzes whether "*any* rational" juror could find proof beyond a reasonable doubt. *Id.* The Court may reverse only if "all rational fact finders would have to conclude" that evidence was insufficient. *Id.* at 1165.

2. Evidence Supported the Verdict

Particularly under this deferential standard, there was more than sufficient evidence to support the jury's verdict.

First, child pornography was found on multiple computers in defendant's home and storage units. (12/8/2015 RT 27-29, 48, 53-54, 74-75, 106; GER 228-30, 249, 254-55, 275-76, 298.) Defendant has never—and could not reasonably—contest his possession of these devices. Nor is his characterization of the scope of his collection accurate. Although defendant claims that only a "handful" of files among "tens of thousands of other files in OrigData" constituted child pornography (AOB 7-8), in

the version of "OrigData" copied in 2005 there were nearly 100 files containing child pornography out of fewer than 1,000 files total—*i.e.*, almost one in every ten files in "OrigData" contained child pornography in 2005. (12/9/15 RT 333, Ex. 68; ER 194, GER 531-48.) Ultimately, across seven copies of "OrigData," defendant kept nearly 700 child pornography videos on his computers.

Second, the contents of "OrigData" and other folders show defendant knowingly possessed this collection. Defendant kept his own personal correspondence, his social security number, his own naked photographs, and other personal files in "OrigData" alongside subfolders containing child pornography. (12/8/2015 RT 234-35, 238-41; ER 115-16, 119-22.) Indeed, defendant e-mailed himself some of the naked photographs stored within sub-folders of "OrigData" in 2009. (Exs. 38A-40A; GER 442-55.) The camera used to take those naked photographs was the same one used to take photographs of defendant and his family and friends. (12/8/2015 RT 245-247; Ex. 41; ER 126-28; GER 456-72.) Likewise, when "OrigData" was backed up, it was backed up at the same time as a "Data" and a "Favourites" folder—both with

files tied to defendant. (12/8/2015 RT 182-83, 241, 249-50; Exs. 68-76; ER 71, 122, 130-31, GER 531-668.)

Third, the meticulous organization of defendant's files—including personal files, adult pornography, and child pornography—further supported the jury's verdict. Defendant's files were organized into folders by content, whether Boeing files in a "Boeing" folder or young girl videos in a "yg" folder. (12/8/2015 RT 189-91; ER 77-79.) Significantly, even non-descriptive child pornography files, such as "15 (2)" and "137.mpg" were in folders according to their content. (12/8/2015 RT 191, 205-09; Ex. 68 at 15; ER 79, 93-97; GER 545.) The keeper of "OrigData" would have had to view those files to organize them accurately, as defendant did. *See United States v. Ganoe*, 538 F.3d 1117, 1123 (9th Cir. 2008) ("The fact that even those files that were not explicitly titled *also* turned out to contain child pornography and were *likewise* placed in the 'z' folder strongly suggests that the images had to have been viewed in order to be categorized.")

Fourth, the continued grooming of "OrigData" shows that defendant was the person returning to the folder and making changes. Child pornography was downloaded on multiple days in 2002 and 2003,

with continued download attempts made using peer-to-peer software in 2004. (12/8/2015 RT 217-20, Ex. 85; ER 98-101; GER 710-16.) Between 2005 and 2006, the child pornography—already sorted to some degree according to content—was reorganized; folders were renamed and created, files were moved to more specific folders, other files were renamed. (12/8/2015 RT 251-52, 271-85, 297, Ex. 85; ER 132-33, 142-56, 168, GER 710-16.) One of the changes made to "OrigData" during this period was the addition of a document containing defendant's e-mail account. (12/9/2015 RT 291-93; Exs. 42, 71 at 40, 74 at 40; ER 162-64, GER 473, 593, 650; *see* 12/8/15 RT 40-45, Exs. 43-45; GER 241-46, 475-80.) This re-shaping of "OrigData," its sub-folders, and the child pornography therein evidenced that defendant was the person who both created and continued to maintain those files.

Fifth, logs of more recent access shows defendant knew the contents of the sub-folders containing child pornography—he could not miss it—and chose to make two more copies of "OrigData" in 2013. Sub-folders in "OrigData" containing child pornography were opened in 2012 and 2013 by the password-protected "Keith" user. (12/9/2015 RT 301-02, 316-18, 322-23, 377; ER 172-73, 177-79, 183-84, 238.) Indeed,

"Keith" copied "OrigData" within an hour after opening a subfolder containing child pornography. (12/9/2015 RT 322-23; Ex. 84 at 1; ER 183-84, GER 707.) And to get to the "vi" folder, "Keith" navigated through a parent folder that also contained child pornography files. (12/9/2015 RT 317-20, 377; ER 178-81, 238.) When he did so, "Keith" inevitably saw what the jury saw during a forensic examiner's testimony: immediately apparent file-names like "xchild porn kiddy underage," "pedofilia," and "R@ygold," among others. (Ex. 84; 12/9/15 RT 317-21, 362, 376-78; GER 707-08, ER 178-82, 223, 238.) "Keith" saw these file names, navigated through those folders, and then once again copied them.

In sum, a forceful "chain of logic" supported that defendant knowingly possessed the child pornography found on his multiple computers. *Begay*, 673 F.3d at 1045. Although defendant reargues various purported holes in the evidence—including that a "number of people" had access to defendant's computers (AOB 17) and that defendant's personal files saved in "OrigData" predated the child

pornography files (AOB16)—these arguments are unavailing.[7] "Viewing the evidence in the light most favorable to the government mandates that [the Court] not consider the plausibility of 'exculpatory constructions' advanced by the defendant." *United States v. Lindsey*, 634 F.3d 541, 552-53 (9th Cir. 2011) (rejecting "alternative explanations" for incriminating evidence on appeal). Instead, when "faced with a record of historical facts that supports conflicting inferences," the Court "must presume—even if it does not affirmatively appear in the record—that the trier of fact resolved any such conflict in favor of the prosecution, and must defer to that resolution." *Nevils*, 598 F.3d at 1164 (punctuation omitted) (quoting *Jackson*, 443 U.S. at 319-20, 326).

---

[7] They are also factually inaccurate. Defendant disregards that folders containing child pornography were accessed by his eponymous, password protected account, "Keith," in 2013. (12/9/15 RT 300, 318-21; ER 171, 179-82.) The only evidence of third parties' access to defendant's computers covered the period from 1999 to 2010. (12/9/15 RT 402, 412-15, 420-21; GER 379, 389-92, 397-98.) Defendant also ignores that, when child pornography videos were downloaded in 2002 and 2003, it could have taken days for those downloads to complete. (12/9/2015 RT 370-71; ER 231-32.) Likewise, while some personal files predated the initial saving of child pornography files, not all did. (12/9/2015 RT 291-93 (discussing email06.doc); Exs. 42, 71 at 40, 74 at 40; ER 162-64, GER 473, 593, 650.)

The cases defendant cites are thus inapposite. (AOB 12-15.) Defendant was not prosecuted based on "cached" or "deleted" files. *Cf. United States v. Kuchinski*, 469 F.3d 853, 863 (9th Cir. 2006); *United States v. Flyer*, 633 F.3d 911, 918-20 (9th Cir. 2011). Defendant, instead, possessed numerous, usable copies of an evolving, organized, repeatedly backed-up collection of child pornography. If deleting cached files after viewing them can suffice to show knowing possession, *United States v. Romm*, 455 F.3d 990, 998, 1000-01 (9th Cir. 2006), surely years-long possession of a curated, backed-up collection of nearly 100 usable child pornography videos is sufficient—particularly given evidence that defendant must have viewed those files in order to organize them. (12/8/2015 RT 188-91; ER 76-79.)

Consistent with *Begay*, this Court has affirmed convictions for possession of child pornography based on far weaker circumstantial evidence of dominion and control. *See United States v. Hardrick*, 766 F.3d 1051, 1057 (9th Cir. 2014) (finding evidence sufficient to uphold verdict for possessing just over a dozen videos; the "number, timing, and location of child pornography videos were inconsistent with [defendant's] defense that he had accidentally downloaded the child

pornography videos or that a hacker had downloaded child pornography videos to his computer without [defendant's] knowledge."). Defendant's conviction must be affirmed.

B. FISA Materials Established Probable Cause

1. Standard of Review

This Court reviews *de novo* the district court's denial of a motion to suppress. *United States v. Krupa*, 658 F.3d 1174, 1177 (9th Cir. 2011); *accord United States v. Demeisi*, 424 F.3d 566, 578 (7th Cir. 2005) ("We review the district court's ruling on the propriety of the FISC's orders de novo."); *United States v. Squillacote*, 221 F.3d 542, 553-54 (4th Cir. 2000) (reviewing *de novo* a motion to suppress under FISA). Accordingly, when reviewing FISA rulings by district courts, this Court examines the underlying FISA materials. *See United States v. Cavanaugh*, 807 F.2d 787, 789 (9th Cir. 1987); *United States v. Ott*, 827 F.2d 473, 475 (9th Cir. 1987).

The Court has not previously articulated the standard of review applicable to an underlying finding of probable cause in a FISA case. In the analogous context of search warrants, this Court gives "great deference" to an issuing magistrate judge's findings of probable cause,

reviewing such findings only for "clear error." *Krupa*, 658 F.3d at 1177; *United States v. Hill*, 459 F.3d 966, 970 (9th Cir. 2006) (same); *United States v. Clark*, 31 F.3d 831, 834 (9th Cir. 1994) (same). "In borderline cases, preference will be accorded to warrants and to the decision of the magistrate issuing it." *United States v. Terry*, 911 F.2d 272, 275 (9th Cir. 1990). The same standard applies to this Court's review of the findings in Title III wiretap applications. *United States v. Brown*, 761 F.2d 1272, 1275 (9th Cir. 2002).

Consistent with these standards and with FISA itself, the Second and Fifth Circuits have held that the "established standard of judicial review applicable to FISA warrants is deferential," particularly given that "FISA warrant applications are subject to 'minimal scrutiny by the courts,' both upon initial presentation and subsequent challenge." *United States v. Abu-Jihaad*, 630 F.3d 102, 130 (2d Cir. 2010); *accord United States v. El-Mezain*, 664 F.3d 467, 567 (5th Cir. 2011) (noting that representations and certifications in FISA application should be "presumed valid"). Other courts, reviewing district court orders *de novo*, have not discussed what deference applies to the FISC. *See, e.g.*, *Demeisi*, 424 F.3d at 578; *Squillacote*, 221 F.3d at 553-54.

The government submits that the appropriate standard should be deferential. Consistent with findings of probable cause in other cases, the Court should review only for "clear error," giving "great deference" to the initial conclusion that a FISA application established probable cause. *Krupa*, 658 F.3d at 1177. Nevertheless, as the district court itself found here, under any standard of review any FISA applications were sufficient in this case. (ER 28.)

2. Legal Standards

The standard of probable cause under FISA is not the same as it is in the criminal context. *See generally Cavanaugh*, 807 F.2d at 790; *Abu-Jihaad*, 630 F.3d at 122-23, 130-31; *United States v. United States District Court* ("*Keith*"), 407 U.S. 297, 322-23 (1972) ("[T]he warrant application may vary according to the governmental interest to be enforced and the nature of citizen rights deserving protection."). Specifically, FISA does not require probable cause to believe that "surveillance will in fact lead to the gathering of foreign intelligence information" or evidence of crime. *United States v. Duggan*, 743 F.2d 59, 73 (2d Cir. 1984). Instead, FISA's standard focuses on the status of a relevant target and place or facility—requiring probable cause to

believe that (1) the target of a FISA application is a foreign power or an agent of a foreign power and that (2a) for surveillance, each facility or place at which electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power, or (2b) for a search, that the property or premises 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. 50 U.S.C. §§ 1804(a)(3), 1805(a)(2), 1823(a)(3), 1824(a)(2). *See generally In re Sealed Case*, 310 F.3d 717, 738 (FISA Ct. Rev. 2002) (discussing this standard). "Agents of a foreign power" include United States persons who engage in certain clandestine intelligence activities. 50 U.S.C. §§ 1801(b)(2)(A)-(E).

In general, "probable cause" requires an "issuing [judge] . . . simply to make a practical, common-sense decision whether, given all the circumstances set forth in the affidavit . . . there is a fair probability" that requisite facts are true. *Illinois v. Gates*, 462 U.S. 213, 238 (1983). Whether there is such a fair probability depends upon the totality of the circumstances, including reasonable inferences, and is a 'commonsense, practical question.'" *United States v. Kelley*, 482 F.3d 1047, 1050 (9th Cir. 2007) (quoting *United States v. Gourde*, 440 F.3d

1065, 1069 (9th Cir. 2006) (*en banc*)); *id.* at 1071 (noting the "principles of *Gates*" are "practicality, common sense, a fluid and non-technical conception of probable cause"). This standard requires less than a preponderance of evidence. *United States v. Terry*, 911 F.2d 272, 275 (9th Cir. 1990). Thus, in the Rule-41 context (where the government must establish probable cause to believe evidence of certain crimes will be found), the government need not establish that it is "more likely than not" that requisite facts are true; instead, the affidavit need only enable the magistrate to "conclude that it would be reasonable to seek . . . evidence in the place indicated by the affidavit." *Id.*

3. Any FISA Applications Satisfied This Standard

Defendant's claim that any FISA applications did not establish probable cause to believe that defendant was an agent of a foreign power rests on the premise that the FISA materials merely "recycled" details that were found in the Harris affidavit.[8] (AOB 23.) Defendant strains to attack various aspects of the "Harris Affidavit" and asserts

[8] **[CLASSIFIED INFORMATION REMOVED]**

that it fell "far short of establishing probable cause to believe that Gartenlaub was a spy for China." (*Id.*)

Gartenlaub's argument is flawed for a number of reasons.

First, defendant seeks to attack the Harris affidavit as a substitute for any FISA applications. But the magistrate's finding of probable cause that evidence of a crime—the compromise of C-17 data on Boeing's network—would be found in defendant's e-mail account was well-supported. (*See* CR 87; GER 1216-17.)

[CLASSIFIED INFORMATION REMOVED]

4. Agents Reasonably Relied on Any Orders or Warrants

Even assuming *arguendo* that there was not sufficient probable cause to support any FISA applications, any evidence obtained or derived from FISC-approved electronic surveillance and physical searches is nonetheless admissible under the "good faith" exception to the exclusionary rule. *United States v. Leon*, 468 U.S. 897 (1984); *United States v. Ning Wen*, 477 F.3d 896, 897 (7th Cir. 2007) (applying *Leon* to FISA); *United States v. Duka*, 671 F.3d 329, 346-47 (3d Cir. 2011) (same). As set forth below, there is no basis to conclude that any statement made to the FISC was false, material, and deliberately or

recklessly made, and none of *Leon*'s other exceptions applies. *Leon*, 468 U.S. 923-26; *United States v. Crews*, 502 F.3d 1130, 1136 (9th Cir. 2007). Thus, even if this Court were to conclude that any applications to the FISC were deficient, there is no basis for suppression of evidence.

With respect to any evidence ultimately obtained in the August 2014 searches, this is doubly true. Agents were entitled to rely on the face of the August 2014 warrant itself, which merely incorporated facts derived from prior authorized searches. (*See generally* ER 243-95.) As the district court already held in assessing a different challenge, officers acted in objectively reasonable reliance on the August 2014 warrant, which was facially valid. (ER 349-50 (applying *Leon*).) Defendant's arguments that the "affiant knowingly or recklessly misled the magistrate judge [were] unpersuasive," there was no evidence that the magistrate "abandoned his . . . neutral role," and the warrant had no obvious "facial deficiency." (*Id.*) Instead, the "detailed affidavit established a fair probability that defendant was in possession of and used computers containing evidence of child pornography crimes, and had rented and placed some items in storage lockers[.]" (ER 350.) A "well-trained officer could reasonably have relied on the magistrate

judge's issuance of the warrants." (*Id.*) Accordingly, even if the August 2014 warrant were to have incorporated evidence obtained from other approved searches later found deficient, there is no basis for suppression of any evidence from the August 2014 searches.

C. The District Court Properly Denied Defendant's Request for a *Franks* Hearing

The district court correctly ruled that defendant failed to make the required showings under *Franks*, and thus no hearing was warranted with respect to any FISA applications. (CR 114; ER 25).

1. Standard of Review

A district court's denial of a *Franks* hearing is reviewed de novo. *United States v. Christie*, 825 F.3d 1048, 1069 (9th Cir. 2016). The district court's underlying finding that the government did not intentionally or recklessly make false statements is reviewed for clear error. *See United States v. Meek*, 366 F.3d 705, 716 (2004); *United States v. Elliott*, 322 F.3d 710, 714 (9th Cir. 2003). Whether probable cause existed notwithstanding any alleged misstatements or omissions is reviewed de novo. *United States v. Perkins*, 850 F.3d 1109, 1115 (9th Cir. 2017).

"Clear error requires a 'definite and firm conviction that a mistake' occurred. *United States v. Gardenhire*, 784 F.3d 1277, 1280 (9th Cir. 2015) (quoting *United States v. Hinkson*, 585 F.3d 1247, 1260 (9th Cir. 2009) (*en banc*)). A district court's factual findings may only be reversed when they are illogical, implausible, or without support in inferences that may be drawn from facts in the record. *Hinkson*, 585 F.3d at 1251; *United States v. Fitch*, 659 F.3d 788, 797 (9th Cir. 2011).

2. Legal Standards

To obtain a *Franks* hearing, a defendant must make a "substantial preliminary showing" that a challenged affidavit contained an actual falsity or omission that was both (1) deliberately or recklessly included in the affidavit and (2) material to the district court's finding of probable cause. *United States v. Shryock,* 342 F.3d 948, 977 (9th Cir. 2003); *United States v. Reeves*, 210 F.3d 1041, 1044 (9th Cir. 2000) (same); *United States v. Collins*, 61 F.3d 1379, 1384 (9th Cir. 1995) (same). Typically, a defendant must specifically identify which portions of the affidavit are false or misleading and present a detailed offer of proof to support his allegations. *United States v. Perdomo*, 800 F.2d 916, 920 (9th Cir. 1986); *United States v. DiCesare*, 765 F.2d 890, 894-

95 (9th Cir. 1985). Failure to make a substantial showing with respect to either element defeats a request for a hearing. *United States v. Martinez-Garcia*, 397 F.3d 1205, 1215 (9th Cir. 2005); *United States v. Fowlkes*, 770 F.3d 748, 763 (9th Cir. 2014); *United States v. Bertrand*, 926 F.2d 838, 841 (9th Cir. 1991).

"The *Franks* standard is a high one." *Riviera v. United States*, 928 F.2d 592, 604 (2d Cir. 1991). Ultimately, defendant's burden is to prove the allegations of intentional or reckless falsity by a preponderance of the evidence. *United States v. Smith*, 588 2d 737, 739 (9th Cir. 1978); *Martinez-Garcia*, 397 F.3d at 1215; *Franks*, 438 U.S. at 156, 170. That showing is to be made by "point[ing] out specifically the portion of the warrant affidavit that is claimed to be false," with "a statement of supporting reasons" and "[a]ffidavits or sworn or otherwise reliable statements of witnesses or their absence satisfactorily explained." *Franks*, 438 U.S. at 171.

"Allegations of negligence or innocent mistake are insufficient." *Id.*; *Perkins*, 850 F.3d at 1116. Indeed, even "recklessness" requires that the affiant have a high degree of awareness of probable falsity. *United States v. Senchenko*, 133 F.3d 1153, 1158 (9th Cir. 1998); *see*

United States v. Williams, 737 F.2d 595, 602 (7th Cir. 1984) ("reckless disregard for the truth," under *Franks*, means that the affiant "in fact entertained serious doubt as to the truth of his" allegations). Moreover, "[t]he deliberate falsity or reckless disregard whose impeachment is permitted [in a *Franks* motion] is only that of the affiant, not of any nongovernmental informant." *Franks*, 438 U.S. at 171.

3. Defendant Was Not Entitled to a Franks *Hearing*

Defendant could not satisfy this standard. As the district court held after making an "independent review of all the materials" submitted *in camera*, there was "no indication of any false statements having been included in [any] FISA materials." (ER 30.) Specifically, defendant could make "no . . . substantial preliminary showing" with respect to any false statements, "whether any such false statements were material, and whether any such false statements were made knowingly, intentionally, or with reckless disregard for their truth[.]" (*Id.*) Accordingly, defendant was "not entitled to a *Franks* hearing." (*Id.*) The district court likewise so held with respect to the Harris affidavit; defendant did not "ma[ke] the requisite showing of materiality and untruthfulness so as to justify an evidentiary hearing." (ER 339.)

a. Defendant's arguments regarding the Harris affidavit fail

On appeal, as before the district court, defendant uses the Harris affidavit as a proxy for his *Franks* arguments regarding any FISA materials, claiming that the Harris affidavit contains an "an astonishing array of material falsehoods . . . covering virtually every aspect of Agent Harris' 'Gartenlaub as spy' theory." (AOB 29.) But, in violation of *Franks*'s requirements, defendant's one-page argument fails to treat any alleged misstatement or omission in detail and cites *no* evidence supporting such alleged falsity—much less presenting a detailed offer of proof supporting defendant's allegations. (*Id.*) *But see Perdomo*, 800 F.2d at 920; *DiCesare*, 765 F.2d a 894-95.

In the district court, defendant did no better. Although his motion repeatedly cited to "Exhibit I," that exhibit was only defendant's bare-bones declaration that purported to adopt the entire motion (signed three days *after* defendant's declaration) as fact. (CR 73; GER 891-94, 1146.) As the district court recognized, this "arguably violate[d] *Franks*'s requirement that 'affidavits or otherwise reliable statements of witnesses should be furnished or their absence satisfactorily explained,'" and it likewise fell short of the Central District of

California's local rules requiring that motions to suppress be "supported by a declaration on behalf of the defendant." (ER 339 n.9.) On this ground alone, the district court justifiably denied a *Franks* hearing; defendant had not even "begun to make the showing necessary for a *Franks* hearing." (8/6/15 RT 21; GER 208.) *See United States v. Wardlow*, 951 F.2d 1115, 1116 (9th Cir. 1991) (per curiam) (affirming refusal to hold evidentiary hearing on motion where defendant failed to follow local rule requiring evidence).

Even disregarding this foundational defect, defendant's arguments fail. Each of his four claimed "examples" of falsehoods or omissions was rebutted by the government and ultimately rejected by the district court (AOB 29-30; *see* ER 338-40).

First, citing to a four-page section of a trial pleading, defendant broadly asserts that Harris "misstated [defendant's] access to the relevant Boeing documents." (AOB 29 (citing GER 891-94).) Defendant fails to acknowledge the government's detailed evidence answering each of his claims on this topic. (CR 87; GER 1279-84, 1290-92, 1355-76.) For example, a comparison of Harris's description and the documents on which he relied shows his high fidelity to that evidence, with Harris's

description at times tracking underlying documents word for word. (*E.g.*, GER 1011-12, 1370). Moreover, defendant's arguments do not ultimately challenge *Harris*'s credibility—only the credibility of documents and Boeing employees on which Harris relied. As the district court thus recognized, defendant thus improperly "challenge[d] the veracity of other persons besides the affiant." (ER 339.) *See Franks*, 438 U.S. at 171 ("The deliberate falsity or reckless disregard whose impeachment is permitted [in a *Franks* motion] is only that of the affiant, not of any nongovernmental informant.").

Second, defendant claims Harris omitted information concerning Boeing employees' emails about "missing" files." (AOB 29 (citing GER 894-95).) The Harris affidavit was prepared in the course of the investigation into the compromise of C-17 data. It cited two e-mails in which defendant's colleague informed defendant, first, that there were 900 missing C-17 part files, and second, that "data is being compromised" and that "[s]omeone is moving data around and causing problems." (GER 998, 1011.) Defendant did not inform the FBI of these facts. (*Id.*) Defendant points to no specific "omission," in this description, however; he points only to counsel's speculation. (GER

895.) Furthermore, the Harris affidavit disclosed that agents had requested—but not yet received—information from Boeing surrounding those two e-mails, indicating that the meaning of those e-mails remained inconclusive. (GER 1014.)

Third, defendant claims the Harris affidavit omitted information concerning defendant's finances that "would have refuted the sinister innuendo Agent Harris sought to foster." (AOB 29 (citing GER 895-97).) But defendant does not dispute the evidence showing defendant and his wife's access to cash, his wife's apparent attempt to avoid a transaction reporting requirement, and his wife's ownership of real estate in China. (GER 1001, 1017-19.) Likewise, defendant does not dispute that, the same day that he was interviewed by the FBI, he enrolled in a feature that allowed him to execute wire transfers over $1000 internationally. (GER 994, 1293, 1378.) The FBI's assessment based on other evidence summarized was just that—an assessment. As the district court recognized, the affidavit was not required to "list every conceivable conclusion." *Burnes*, 816 F.2d at 1358. (ER 340.)

Finally, defendant claims Agent Harris omitted "exculpatory information" concerning the "fish fork" e-mail that his wife forwarded to

his Boeing account, apparently seeking advice about a device that could be used to land a helicopter on a warship. (AOB 29 (citing GER 898).) The only "omission" defendant ever identified was that "the affidavit fails to note that Mr. Gartenlaub did not respond to the e-mail." (GER 898.) But that is exactly what the Harris affidavit said: "Gartenlaub did not respond to this e-mail using his Boeing e-mail account or otherwise using his Boeing computer." (GER 1007.) Defendant also suggested that the suspiciousness of the "fish fork" e-mail was undermined by the availability of similar patents online. (GER 898.) Again, the Harris affidavit reflected just that; a Chinese aviation company had applied for a Chinese patent. (GER 1006.)

These allegations aside, defendant entirely fails to address *Franks*'s other requirements. (AOB 29-30.) Defendant provides no argument at all regarding materiality. (*But see* CR 87; GER 1216-17, 1279-94.) He identifies no evidence that any omission or misstatement was made deliberately or recklessly by Agent Harris. (*But see* GER 1276-78.) Defendant cannot satisfy the *Franks* standard—much less establish clear error—by omission. As the district court correctly

concluded, defendant's challenges to the Harris affidavit fall short of justifying any hearing under *Franks*. (ER 338-40.)

b. Defendant's FISA arguments fare no better

As defendant's proxy arguments regarding the Harris affidavit reflect, he was not entitled to any *Franks* hearing with respect to any FISA applications. Defendant's lack of access to FISA materials does not change the *Franks* standard; the same substantial preliminary showing is required to justify a hearing. *Abu-Jihaad*, 630 F.3d at 130 (following FISA's *in camera* judicial review process, affirming denial of *Franks* hearing, stating that "'the representations and certifications submitted in support of an application for FISA surveillance should be presumed valid' by a reviewing court absent a showing sufficient to trigger a *Franks* hearing"); *El-Mezain*, 664 F.3d at 570 (requiring standard, two-part *Franks* test of a "proper preliminary showing" to conclude "defendants . . . failed to show a basis for a *Franks* hearing"); *United States v. Damrah*, 412 F.3d 618, 625 (6th Cir. 2005) ("Damrah failed to meet his threshold burden under *Franks*"); *see also United States v. Pelton*, 835 F.2d 1067, 1076 (4th Cir. 1987) ("Where, as here, the statutory application was properly made and earlier approved by a

FISA judge, it carries a strong presumption of veracity and regularity in a reviewing court.").

Just as defendant's claims that the Harris affidavit was "rife with material falsehoods and omissions" and "highly likely" to contain "material falsehoods" are unsupported (AOB 6), so too is his speculation that any FISA applications contained such falsehoods and omissions. "[T]he challenger's attack must be more than conclusory and must be supported by more than a mere desire to cross-examine." *Franks*, 438 U.S. at 171; *see also United States v. Craighead*, 530 F.3d 1073, 1081-81 (9th Cir. 2008) (affirming denial of *Franks* hearing where challenge was based on possible alternative theories explaining why child pornography could have been found). The district court was correct in denying a *Franks* hearing and finding that no false statements were made, and its finding that no agent acted "knowingly, intentionally, or with reckless disregard for the[] truth" was not clear error. (CR 114; ER 30.) *See Meek*, 366 F.3d at 716; *Elliott*, 322 F.3d at 714.

[CLASSIFIED INFORMATION REMOVED]

D. The Government Was Permitted to Search Every File on Defendant's Computers and to Use Evidence of Child Pornography Found There

1. Standard of Review

As defendant concedes, he did not challenge the scope of the January 2014 search before the district court. (AOB 35.) It is therefore reviewed, at most, for plain error. Fed. R. Crim. P. 52(b); *United States v. Olano*, 507 U.S. 725, 731 (1993).

To prevail under plain-error review, defendant bears the burden of establishing four things. "First, there must be an error or defect . . . that has not been intentionally relinquished." *Puckett v. United States*, 556 U.S. 129, 135 (2009). Second, "the legal error must be clear or obvious" at the time of appellate consideration. *Henderson v. United States*, 133 S. Ct. 1121, 1130-31 (2013). "Third, the error must have affected the appellant's substantial rights, which in the ordinary case means he must demonstrate that it 'affected the outcome of the district court proceedings.'" *Puckett*, 556 U.S. at 135 (quoting *Olano*, 507 U.S. at 734). Fourth, "if the above three prongs are satisfied, the court of appeals has the discretion to remedy the error—discretion which ought to be exercised only if the error seriously affects the fairness, integrity

or public reputation of judicial proceedings." *Id.* (punctuation omitted). As the Supreme Court has emphasized, "[m]eeting all four prongs is difficult, 'as it should be.'" *Id.*; *see Johnson v. United States*, 520 U.S. 461, 466 (1997) (noting the "limited and circumscribed strictures" of the plain error rule (punctuation omitted)).

2. The Government Was Permitted to Use Evidence It Found During Any FISC-Approved Search

Defendant's claim of plain error founders at the outset; he cannot demonstrate any error at all. Defendant accurately summarizes the government's rationale: "To determine whether defendant's computers contained foreign intelligence information, it was necessary to open and review every file; after all, a foreign spy might cleverly conceal such information in .jpg files with sex-themed names or in other non-obvious places." (AOB 31.)

This Court has previously affirmed exactly this approach. *E.g.*, *United States v. Adjani*, 452 F.3d 1140, 1149-50 (9th Cir. 2006) (rejecting defendant's challenge to the government's "search of the contents of all emails" because a "pinpointed computer search . . . would likely have failed to cast a sufficiently wide net to capture the evidence sought"); *Hill*, 459 F.3d at 977-78 (rejecting that search of defendant's

computers should have been limited to certain file types, like .jpg, because "[c]omputer records are extremely susceptible to tampering, hiding, or destruction," contraband can be concealed using "the simple expedient of changing the names and extensions of files to disguise their content," and "[t]here is no way to know what is in a file without examining its contents"); *United States v. Giberson*, 527 F.3d 882, 889-90 (9th Cir. 2008) (citing *Adjani* and *Hill*; rejecting defendant's argument that search should have been limited to certain file types or a review of directories); *United States v. Flores*, 802 F.3d 1028, 1045-46 (9th Cir. 2015) (denying suppression of warrant that called for production of 11,000 pages from Facebook that resulted in seizure of approximately 100 pages of responsive evidence; citing *Adjani*).

Having lawfully executed a search, the government could—consistent with the statutory provisions that govern information obtained from FISA—retain any inadvertently-discovered evidence of child pornography for law-enforcement investigative purposes. *See* 50 U.S.C. §§ 1801(h)(3), 1821(4)(C) (requiring that court-approved foreign intelligence minimization procedures "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"); *Ning Wen*, 477 F.3d at 898 ("If, while conducting [FISA] surveillance, agents discover evidence of a domestic crime, they may use it to prosecute for that offense," "whether or not they expected to learn about the domestic offense"); *Duggan*, 743 F.2d at 78 ("[W]e emphasize that otherwise valid FISA surveillance is not tainted simply because the government can anticipate that the fruits of such surveillance may later be used, as allowed by [50 U.S.C.] § 1806(b), as evidence in a criminal trial."); *see In re Sealed Case*, 310 F.3d at 731 ("minimization procedures allow . . . the retention and dissemination of non-foreign intelligence information which is evidence of *ordinary* crimes for preventative or prosecutorial purposes.").

Defendant complains that the use of child pornography found in the course of a FISC-authorized search was not permitted because child pornography is not foreign intelligence. (AOB 30-35; *accord* Docket No. 34 at 16-18 (amicus brief).) This argument has been repeatedly rejected. Use of information obtained or derived from FISA searches or surveillance has been upheld in criminal prosecutions for a variety of

offenses, including murder, naturalization fraud, and possessing unregistered firearms. *Ott*, 827 F.2d at 475 (rejecting challenge to FISA information used in court martial for offering to sell classified information); *Damrah*, 412 F.3d at 620 (same, in prosecution for making false statements in citizenship application); *United States v. Isa*, 923 F.2d 1300, 1304 (8th Cir. 1991) (same, in murder prosecution; there "is no requirement that the 'crime' be related to foreign intelligence"); *United States v. Badia*, 827 F.2d 1458, 1460-61 (11th Cir. 1987) (same, in prosecution for conspiracy to possess and manufacture unregistered firearms and machineguns); *see also Matter of Kevork*, 788 F.2d 566 (9th Cir. 1986) (affirming denial of motion to suppress FISA information supporting Canadian criminal conspiracy and attempted murder charges, after noting that FISA's "provisions . . . establish conditions under which such information may be used for law enforcement purposes" domestically).

Moreover, in the FISA context, where national security and counterintelligence interests are reconciled with individual rights, individual rights are protected through "in-depth oversight" and "an expanded conception of minimization that differs from that which

governs law-enforcement surveillance." *United States v. Belfield*, 692 F.2d 141, 148 (D.C. Cir. 1982) (internal quotation omitted); *see Damrah*, 412 F.3d at 625 ("FISA has uniformly been held to be consistent with the Fourth Amendment."); *Keith*, 407 U.S. at 322 (noting that the "gathering of security intelligence is often long range and involves the interrelation of various sources and types of information," and that because the purpose of "domestic intelligence gathering" is preventative, "the focus of domestic surveillance may be less precise than that directed against more conventional types of crime."); *In re Sealed Case*, 310 F.3d at 738 (same), 741; *United States v. Sarkissian*, 841 F.2d 959, 965 (9th Cir. 1988) ("FISA is meant to take into account the differences between ordinary criminal investigations to gather evidence of specific crimes and foreign counterintelligence investigations to uncover and monitor clandestine activities." (punctuation omitted)).

[CLASSIFIED INFORMATION REMOVED]

Barring the use of information obtained or derived from FISA in this criminal prosecution is not only contrary to this framework and other courts' precedent, but it would re-build a wall between criminal

and national security matters and in practical effect foreclose prosecutions where evidence of those crimes is lawfully found. *Abu-Jihaad*, 630 F.3d at 125; *In re Sealed Case*, 310 F.3d at 728 (noting earlier concerns regarding the "primary purpose" test had "inhibited necessary coordination between intelligence and law enforcement officials"). The potentially broad consequences of adopting defendant's argument, raised for first time on appeal, demonstrate both that it is wrong and that it did not constitute a plain error.

Non-FISA precedents also foreclose defendant's claims. Analyzing a Rule 41 search warrant, this Court has held that using child pornography inadvertently discovered during a lawful search is consistent with the Fourth Amendment. *Giberson*, 527 F.3d at 889-90 (ruling that "the pornographic material [the agent] inadvertently discovered while searching for the documents enumerated in the warrant [related to document identification fraud] was properly used as a basis for the third warrant authorizing the search for child pornography"); *United States v. Wong*, 334 F.3d 831, 838 (9th Cir. 2003) (where child pornography files were found on a computer "[w]hile searching the graphics files for evidence of murder, as allowed by the

warrant," subsequent use at trial was permitted under plain view because "the police were lawfully searching for evidence of murder"); *United States v. Nessland*, 601 Fed. Appx. 576, 576 (9th Cir. 2015) (rejecting Fourth Amendment challenge where "[t]he officers were searching for a particular type of photographic image and came across the images in question here, which were in plain view").

[CLASSIFIED INFORMATION REMOVED]

With the benefit of NCMEC's assistance, the government then sought and obtained the August 2014 search warrants, authorizing the search of defendant's residence and storage units for child pornography. (CR 73; GER 901-53). The fruits of this warrant were then used in defendant's prosecution. The use of information discovered during the prior lawful January 2014 search in the subsequent search warrant application was proper. *Giberson*, 527 F.3d at 890.

Defendant relies on *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162 (9th Cir. 2010) (*en banc*) ("*CDT*"), but that case provides no basis to suppress the evidence seized here. *CDT* involved a warrant for information concerning ten clients of a company; the government, however, had seized information about hundreds of clients

in what this Court described as "an obvious case of deliberate overreaching by the government in an effort to seize data as to which it lacked probable cause." *Id.* at 1172. Here, in stark contrast, the government properly executed the search of defendant's "entire computer system and all his digital storage devices" that were found at his residence. *United States v. Schesso*, 730 F.3d 1040, 1049 (9th Cir. 2013). And "the search did not involve an over-seizure of data that could expose sensitive information about other individuals not implicated in any criminal activity," *id.*, the principal transgression in *CDT*. *Accord Nessland*, 601 Fed. Appx. at 576 (*CDT*'s holding inapplicable where "there was no real risk of exposing other people's data, and there was no sign of overreaching"). In any event, the government obtained a subsequent search warrant used to seize the evidence offered at trial.

The concurring opinion in *CDT*, upon which defendant relies, does not aid him. That concurrence is not "binding circuit precedent" or a "constitutional requirement," much less one binding on the FISC. *Schesso*, 730 F.3d at 1049 (the "search protocol" set forth in the *CDT* concurrence is not "binding circuit precedent," not a[] constitutional

requirement[]," and provides "no clear-cut rule"); *see CDT*, 621 F.3d at 1178 (observing that "[d]istrict and magistrate judges must exercise their independent judgment in every case"); *Nessland*, 601 Fed. Appx. at 576 (holding that "no special protocol was required" for a computer search). Defendant thus cannot demonstrate any error relating to any FISC-authorized search.

3. Defendant Cannot Establish the Remaining Elements of Plain Error

Defendant likewise cannot establish that any error was plain. To constitute "plain error," error must be "clear on its face under current law." *United States v. Campos*, 217 F.3d 707, 713 (9th Cir. 2000); *accord United States v. De La Fuente*, 353 F.3d 766, 769 (9th Cir. 2003) (error not plain absent "controlling authority on point"). But the precedents above—none endorsing defendant's constrained interpretation of FISA—foreclose any contention that error could be "clear" here. *See, e.g., United States v. Brigham*, 447 F.3d 665 (9th Cir. 2006) (requiring that, "[f]or error to qualify as 'plain,' it must be 'so clear-cut, so obvious, [that] a competent district judge should be able to avoid it without benefit of objection,'" in part to allow parties and district court to address the issue).

Nor can defendant establish the remaining elements of plain error, including prejudice. Because officers were entitled to rely in good faith on the face of the August 2014 warrant, any defects in underlying searches would not be a basis for suppression of evidence. (*See supra*; *see generally* ER 348-50 (analyzing good-faith exception with respect to the August 2014 warrant).) As a result, even if officers *had* exceeded the permissible scope of the January 2014 search, no suppression of trial evidence would result. *See generally Leon*, 468 U.S. at 897. For the same reason, defendant cannot demonstrate a serious effect on the fairness, integrity, or public reputation of judicial proceedings. *Puckett*, 556 U.S. at 135.

E. The District Court Correctly Declined to Order Disclosure of the FISC Application and Order

1. Standard of Review

The district court's denial of defendant's motion for disclosure of FISA materials is reviewed for abuse of discretion. *United States v. Omar*, 786 F.3d 1104, 1111 (8th Cir. 2015); *El-Mezain*, 664 F.3d at 567; *Duggan*, 743 F.2d at 78; *Damrah*, 412 F.3d at 624.

2. The District Court's Decision Was Correct and Complied with FISA

When a defendant moves for disclosure of FISA materials that led to evidence being used against him, the government may respond by filing a declaration from the Attorney General stating that "disclosure or an adversary hearing would harm the national security of the United States." 50 U.S.C. §§ 1806(f), 1825(g). If the Attorney General files such a declaration—as occurred in this case—the district court must review the FISA materials *ex parte* and *in camera* and may order disclosure of portions of the FISA materials "only where such disclosure is *necessary* to make an accurate determination of the legality of the surveillance." *Id.* (emphasis added). Thus, FISA "requires the judge to review the FISA materials *ex parte in camera* in *every* case, and on the basis of that review decide whether any of those materials must be disclosed to defense counsel." *United States v. Daoud*, 755 F.3d 479, 482 (7th Cir. 2014); *accord El-Mezain*, 664 F.3d at 565; *Abu-Jihaad*, 630 F.3d at 129.

The district court did exactly what was required. The court conducted a "thorough, *in camera*, *ex parte* examination" of the FISA materials and concluded that it did "not require the assistance of the

defense to make an accurate determination of the legality of the electronic surveillance and physical searches." (ER 27.) The court's conclusion was no abuse of discretion, as the lawfulness of the electronic surveillance and physical search was apparent from the FISA materials. *See Daoud*, 755 F.3d 485 ("Our own study of the classified materials has convinced us . . . that their disclosure to the defendant's lawyers is . . . not necessary."). Because the district court "was 'capable' of making the [lawfulness] determination, disclosure was not 'necessary' under any definition of that word." *Id.*; *accord Duggan*, 743 F.2d at 78; *cf.* David Kris & J. Douglas Wilson, *National Security Investigations* § 31:3 & n.1 (2d ed. 2012) ("Necessary means 'essential' or 'required,' and therefore the plain language of that provision makes clear that a court may not disclose . . . unless it cannot determine whether the surveillance was unlawful without the assistance of defense counsel and an adversary hearing.").

Courts consistently have held that "'[d]isclosure [of FISA materials] and an adversary hearing are the exception, occurring *only* when necessary.'" *Sarkissian*, 841 F.2d at 964 (quoting *Belfield*, 692 F.2d at 147); *accord El-Mezain*, 664 F.3d at 567 ("Disclosure of FISA

materials is the exception and *ex parte*, *in camera* determination is the rule."); *Abu-Jihaad*, 630 F.3d at 129. Given that the "language of section 1806(f) clearly anticipates that an *ex parte*, *in camera* determination is to be the rule," *Belfield*, 692 F.2d at 147, any need for disclosure must be based on a reason that is both uncommon and case-specific. *See In re Grand Jury Proceedings of Special April 2002 Grand Jury*, 347 F.3d 197, 203 (7th Cir. 2003) (observing that a case in which "disclosure is necessary" is "one-in-a-million").

This is confirmed by FISA's legislative history. The relevant Senate Judiciary Committee report reflects that the "necessary" standard "require[s] more than a showing that the information would be useful or convenient." S. Rep. No. 95-604(I), at 31 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3904, 3933. The Senate Select Committee on Intelligence report elaborates:

> The committee intends to require a showing that the information is both important and required. The use of this standard is intended to mandate that a significant need be demonstrated by those seeking the surveillance [materials].

S. Rep. No. 95-701, at 31 (1977), *reprinted in* 1978 U.S.C.C.A.N. 3973, 4000; *accord* H.R. Rep. No. 95-1283, pt. I, at 47 (1978).

Defendant cites Congressional reports to argue that "necessary" should mean only that disclosure "would substantially promote an accurate determination of legality." (AOB 37-41.) While Congress did consider that standard in earlier bills and reports, in the Conference Report reconciling the Senate bill and the House's amendments, that language was rejected. H.R. Rep. No. 95-1720, at 31-32 (1978), *reprinted in* 1978 U.S.C.C.A.N. 4048, 4060-61. Specifically, Congress rejected the lesser standard in the House amendments calling for disclosure "if there were a reasonable question as to the legality of the surveillance and if disclosure would likely promote a more accurate determination of such legality," and instead adopted the language in the Senate bill allowing for disclosure "only where such disclosure is necessary to make an accurate determination of the legality of the surveillance." *Id.*

Here, defendant can advance no case-specific basis suggesting a "significant need" for any FISA materials. Although defendant contends that the need for disclosure is "particularly stark" when "a defendant challenges a FISC order under *Franks*" (AOB 45), this argument could be raised in nearly every FISA case—eviscerating

Congress's intent that FISA litigation be handled *ex parte*, *in camera*, with disclosure the rare exception. *See Belfield*, 692 F.2d at 147 (rejecting argument that would make disclosure necessary in every case because "[t]he language of section 1806(f) clearly anticipates that an *ex parte*, *in camera* determination is to be the rule"). If anything, defendant's need was *less* than most; although he lacked access to any FISA materials, he had access to substantial materials about the underlying investigation, including the Harris affidavit. As a result, defendant could and did make a focused proffer of facts he believed would justify a *Franks* hearing. *See Daoud*, 755 F.3d at 483 (rejecting *Franks* challenge to FISA materials based on "extensive proffer" by defendant); *accord Abu-Jihaad*, 630 F.3d at 130 (similar).

Judge Rovner's concurring opinion in *Daoud*, on which defendant relies, does not support (much less mandate) a contrary conclusion. (AOB 45-46 (citing *Daoud*, 755 F.3d at 486 (Rovner, J., concurring).) Defendant ignores that Judge Rovner joined the unanimous panel opinion "in full," 755 F.3d at 485, and that her concurrence made clear that a potential *Franks* claim is *not* an automatic basis for disclosure of classified FISA materials. *See* 755 F.3d at 484 ("The drafters of [FISA]

devised a solution: the judge makes the . . . determination, based on full access to all classified materials and the defense's proffer of its version of events, of whether it's possible to determine the validity of the *Franks* challenge without disclosure of any of the classified materials to the defense."); *id.* at 495 (Rovner, J., concurring) ("The court, which has unrestricted access to the FISA application, can make limited and reasonable efforts to do what the defense cannot: determine if the face of the FISA application is consistent with whatever documented statements of the defendant (or his accomplices) that the government might have in its possession."). Moreover, Judge Rovner recognized that judges can make a "meaningful effort to confirm the accuracy of the [FISA] application," satisfying *Franks*'s requirements, where the application is "based in part on . . . documented statements" that could be reviewed by the court. *Daoud*, 755 F.3d 494-95 (Rovner, J. concurring).

[CLASSIFIED INFORMATION REMOVED]

Defendant's "tactic" of citing errors made to the FISC in other cases over the years "is of little use in satisfying *Franks* standard, as it sheds no light on the truth or falsity of the particular FISA application

under review" and does not "substantiate the necessity of disclosure of a FISA application in [this] case." *Daoud*, 755 F.3d at 491-92 (Rovner, J., concurring) (observing defendants' citation for that purpose of *In re All Matters Submitted to the Foreign Intelligence Surveillance Court*, 218 F. Supp. 2d 611, 620 (FISA Ct. 2002), *abrogated by In re Sealed Case*, 310 F.3d at 717)). (*See* AOB 51-53).

At bottom, the district court here performed the review called for by *Daoud* and "determined that there is no indication of any false statements having been included in the FISA materials." (ER 30.) While defendant takes issue with the district court signing the order in the form prepared by the government, the district court made clear that it had conducted a thorough evaluation in reaching its decision. (CR 114; 8/29/16 RT 21-22; ER 27, GER 808-09). The district court's decision not to order disclosure of classified FISA materials was a proper application of FISA's statutory command, the correct analysis of the record, and not an abuse of discretion.

3. Non-Disclosure Complied with Due Process

Due process also did not compel disclosure of any FISA materials. To the extent defendant argues that due process requires disclosure of

FISA materials in all criminal cases, his argument is foreclosed by this Court's holding in *Ott*, 827 F.2d at 476-77, which rejected a due process challenge to a court's refusal to disclose FISA materials. Following *Ott*, this Court has repeatedly rejected other due process challenges to non-disclosure under FISA. *See, e.g.*, *United States v. Mohamud*, 666 Fed Appx. 591, 597 (9th Cir. 2016) (applying *Ott*; upholding *ex parte*, *in camera* review of FISA materials); *see also United States v. Sedaghaty*, 728 F.3d 885, 908 (9th Cir. 2013) (ruling, in CIPA context, that defendant's "broadside challenge to the *in camera* and *ex parte* proceedings is a battle already lost in the federal courts"). Every other circuit to have considered the issue has come to the same conclusion. *See United States v. Ali*, 799 F.3d 1008, 1022 (8th Cir. 2015); *El-Mezain*, 664 F.3d at 567-68; *Abu-Jihaad*, 630 F.3d at 129; *Damrah*, 412 F.3d at 624; *Belfield*, 692 F.2d at 148-49.

Defendant cannot point to any relevant distinction between his case and the cases cited above. Defendant asserts that the relevant analytical framework is the three-factor test set forth in *Mathews v. Eldridge*, 424 U.S. 319 (1976). (AOB 47.) Precedent does not support his assertion. *See Ott*, 827 F.2d at 476-77 (holding that *in camera*, *ex*

parte review of FISA materials satisfied due process without citing *Mathews*); *Mohamud*, 666 Fed. Appx. at 597 (same); *Damrah*, 412 F.3d at 624 ("reliance on *Mathews* is misplaced, however, because FISA's requirement that the district court conduct an *ex parte*, *in camera* review of FISA materials does not deprive a defendant of due process"). Nevertheless, even under the *Mathews* factors, defendant can identify no distinction mandating disclosure in this case.

First, defendant's "private interests" are no greater than those of other similarly situated defendants. (*Cf.* AOB 48.) Privacy interests are implicated in every FISA challenge, and FISA, as this Court has held, complies with the Fourth Amendment. *Cavanaugh*, 807 F.2d at 789-91. Similarly, significant liberty interests are implicated in every criminal case. *See, e.g.*, *Mohamud*, 666 Fed. Appx. at 597 (affirming 30-year sentence, affirming non-disclosure of FISA materials).

Second, the "risk of an erroneous deprivation" of liberty is low or nonexistent. *Mathews*, 424 U.S. at 335. (*Cf.* AOB 49-50.) As discussed above, FISA itself provides for disclosure of materials "where such disclosure is necessary to make an accurate determination of the legality of the surveillance." 50 U.S.C. §§ 1806(f), 1825(g). But where a

court determines that it does "not require the assistance of the defense to make an accurate determination of the legality of the electronic surveillance and physical searches" (ER 27), there is little value for "additional or substitute procedural safeguards," *Mathews*, 424 U.S. at 335. As the Fifth Circuit recognized in *El-Mezain*, "the *in camera* and *ex parte* review by the district court adequately ensured that the defendants' statutory and constitutional rights were not violated." 664 F.3d at 567 (citing "numerous courts" that have held that "FISA's *in camera* and *ex parte* procedures . . . withstand constitutional scrutiny").

Third, the government's interest cuts decisively against disclosure. As Attorney General Holder personally certified in this case, "it would harm the national security of the United States to disclose or hold an adversary hearing with respect to the FISA Materials." (CR 79; GER 45.) The government's interest in protecting the secrecy of information important to national security has long been recognized as a compelling one. *See, e.g., Haig v. Agee*, 453 U.S. 280, 307 (1981).

Advantages of the adversary process were well known to Congress when it enacted FISA, but those benefits were weighed against the exceptional costs of revealing "sensitive . . . intelligence information." S.

Rep. No. 95-604(I), at 58. Congress thus balanced "the interest in full openness of legal proceedings and the interest in national security, which requires a degree of secrecy concerning the government's efforts to protect the nation." *Daoud*, 755 F.3d at 483 ("Conventional adversary procedure thus has to be compromised in recognition of valid social interests"); *accord Belfield*, 692 F.2d at 148 (Congress was "aware" of the difficulties of *ex parte* procedures and made a "thoroughly reasonable attempt to balance the competing concerns of individual privacy and foreign intelligence").

[CLASSIFIED INFORMATION REMOVED]

These judgments, made by national security professionals within the executive branch, "are decisions for which the judiciary has neither aptitude, facilities, nor responsibility." *Chicago & S. Air Lines, Inc. v. Waterman S.S. Corp.*, 333 U.S. 103, 111 (1948); *see also Dep't of Navy v. Egan*, 484 U.S. 518, 527-28 (1988). Courts have "little or no background in the delicate business of intelligence gathering," and should thus give appropriate deference to the executive branch's assessment about the significance of disclosing sensitive information and the repercussions for intelligence gathering and United States foreign policy. *CIA v.*

Sims, 471 U.S. 159, 176 (1985); *see also id.* at 180 ("it is the responsibility of the Director of Central Intelligence, not that of the judiciary, to weigh the variety of complex and subtle factors in determining whether disclosure of information may lead to an unacceptable risk of compromising the Agency's intelligence-gathering process"); *United States v. Yunis*, 867 F.2d 617, 623 (D.C. Cir. 1989) ("Things that did not make sense to the District Judge would make all too much sense to a foreign counter-intelligence specialist who could learn much about this nation's intelligence gathering capabilities from what these documents revealed about sources and methods.").

Moreover, even where a defendant's counsel has a security clearance, the analysis does not change. "Congress has a legitimate interest in authorizing the Attorney General to invoke procedures designed to ensure that sensitive security information is not unnecessarily disseminated to *anyone* not involved in the surveillance operation in question, whether or not she happens for unrelated reasons to enjoy security clearance." *Ott*, 827 F.2d at 477; *El-Mezain*, 664 F.3d at 568 (same); *Mohamud*, 666 Fed. Appx. at 597; *Sedaghaty*, 728 F.3d at 909 (same in CIPA context). "[D]isclosing state secrets to cleared

lawyers" could certainly "harm national security," particularly given that defense attorneys "in their zeal to defend their client, to whom they owe a duty of candid communication, or misremembering what is classified and what [is] not, [may] inadvertently say things that would provide clues to classified material. *Daoud*, 755 F.3d 484.[9]

Defendant claims that the Classified Information Procedures Act ("CIPA") opened a faucet of classified discovery to defense counsel that overrides the statutory mandate of FISA. 18 U.S.C. app. 3. (AOB 54-55.) CIPA was designed to prevent "graymail" by defendants in the discovery and trial process when either involved classified information. *Sarkissian*, 841 F.3d at 965. Contrary to defendant's argument, one of CIPA's often-used provisions allows the government "to delete specified items of classified information from documents to be made available to the defendant through discovery." 18 U.S.C. app. 3 § 4; *Sarkissian*, 841 F.2d at 965 ("Congress intended section 4 to clarify the court's powers

[9] Proceedings in this case likewise illustrate why protective orders are insufficient to protect against disclosures, even inadvertent disclosures, of information they govern. (4/18/16 RT 15-18 (noting disclosures of material that appears to have been covered by protective order); 8/29/16 RT 66-67 (noting additional disclosure); GER 783-86, 853-54; *see also* Docket No. 15 at 2 n.1.)

under Fed. R. Crim. P. 16(d)(1) to deny or restrict discovery in order to protect national security."); *Sedaghaty*, 728 F.3d at 904 (same); *United States v. Klimavicius-Viloria*, 144 F.3d 1249, 1261-62 (9th Cir. 1998) (same). While defendant correctly observes that CIPA was passed after FISA, *Ott*, *Klimavicius-Viloria*, *Daoud*, *El-Mezain*, and *Mohamud* were all decided after CIPA was passed, and each rejected the request to disclose FISA materials to defense counsel, including to cleared counsel.

In *Ott*, this Court held that FISA's *in camera*, *ex parte* review procedures are consistent with due process. Confronted with this facial validity, defendant can offer no case-specific basis for why his case is different. In fact, the *Mathews* factors point strongly against disclosure of any classified FISA materials, particularly given the strong governmental interest in protecting sensitive national security information and the fact that an accurate *ex parte* determination could be made in this case.

4. Brady *Did Not Require Disclosure*

Finally, defendant's argument that disclosure of FISA materials was required by *Brady*, 373 U.S. 83, is without merit. *United States v. Barton*, 995 F.2d 931, 934 (9th Cir. 1993). *Brady* applies to evidence

that is both "favorable to an accused" and "material either to guilt or to punishment." 373 U.S. at 87; *see also Skinner v. Switzer*, 562 U.S. 521, 536 (2011) ("*Brady* evidence is . . . favorable to the defendant and material to his guilt or punishment."). Evidence that goes only to the lawfulness of a search is not material to guilt or punishment, because even "the successful suppression of incriminating evidence is unrelated to the actual culpability of an accused." *Barton*, 995 F.2d at 934. *Brady* simply does not apply in this context because no FISA materials are exculpatory as to guilt or punishment. As the district court found, any FISA materials simply do not contain any *Brady* material with respect to defendant's child pornography offenses. (ER 26 n.3.)

V

CONCLUSION

For the reasons stated herein, this Court should affirm.

DATED: May 9, 2017

Respectfully submitted,

SANDRA R. BROWN
Acting United States Attorney

PATRICK R. FITZGERALD
Assistant United States Attorney
Chief, National Security Division

/s/ Anthony Lewis
/s/ Vicki Chou

ANTHONY J. LEWIS
VICKI CHOU
Assistant United States Attorneys
National Security Division

Attorneys for Plaintiff-Appellee
UNITED STATES OF AMERICA

STATEMENT OF RELATED CASES

The government states, pursuant to Ninth Circuit Rule 28-2.6, that it is unaware of any cases related to this appeal.

CERTIFICATE OF COMPLIANCE

I certify that:

1. This brief is accompanied by a motion for leave to file a longer brief pursuant to Ninth Circuit Rule 32-2 and contains 14,483 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(a)(7)(B)(iii).

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 it has been prepared in a proportionally spaced typeface (14-point Century Schoolbook) using Microsoft Word 2010.

DATED: May 9, 2017 /s/ *Anthony J. Lewis*

ANTHONY J. LEWIS
Attorney for Plaintiff-Appellee
United States of America

9th Circuit Case Number(s) 16-50339

NOTE: To secure your input, you should print the filled-in form to PDF (File > Print > *PDF Printer/Creator*).

****

CERTIFICATE OF SERVICE
When All Case Participants are Registered for the Appellate CM/ECF System

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 (date) May 9, 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.

Signature (use "s/" format) /s/ Anthony J. Lewis

****

CERTIFICATE OF SERVICE
When Not All Case Participants are Registered for the Appellate CM/ECF System

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 (date) .

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

I further certify that some of the participants in the case are not registered CM/ECF users. I have mailed the foregoing document by First-Class Mail, postage prepaid, or have dispatched it to a third party commercial carrier for delivery within 3 calendar days to the following non-CM/ECF participants:

Signature (use "s/" format)