ORAL ARGUMENT REQUESTED
No. 19-3043

IN THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT

UNITED STATES OF AMERICA,

Plaintiff-Appellee

v.

PATRICK EUGENE STEIN,

Defendant-Appellant

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS
THE HONORABLE ERIC F. MELGREN, NO. 6:17-CR-10045-EFM

BRIEF FOR THE UNITED STATES AS APPELLEE

ERIC S. DREIBAND
Assistant Attorney General

THOMAS E. CHANDLER
ERIN H. FLYNN
ALISA C. PHILO
Attorneys
Department of Justice
Civil Rights Division
Appellate Section
Ben Franklin Station
P.O. Box 14403
Washington, D.C. 20044-4403
(202) 616-2424

TABLE OF CONTENTS

PAGE

TABLE OF CONTENTS (continued):

TABLE OF AUTHORITIES

CASES: **PAGE**

CASES (continued): **PAGE**

CASES (continued): **PAGE**

STATUTES:

RULES:

STATEMENT OF RELATED CASES

This appeal is related to Stein's pending appeal of his conviction and sentence for conspiring to use a weapon of mass destruction and to violate civil rights, Case No. 19-3030. That appeal has been consolidated with the appeals of Stein's two co-conspirators, Case Nos. 19-3034 and 19-3035, and the government's cross-appeal of the defendants' sentences, Case No. 19-3053. While some of the facts and procedural history of Stein's two cases are intertwined, the issues on appeal do not overlap.

IN THE UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT

No. 19-3043

UNITED STATES OF AMERICA,

Plaintiff-Appellee

v.

PATRICK EUGENE STEIN,

Defendant-Appellant

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF KANSAS
THE HONORABLE ERIC F. MELGREN, NO. 6:17-CR-10045-EFM

BRIEF FOR THE UNITED STATES AS APPELLEE

STATEMENT OF JURISDICTION

This appeal is from the entry of final judgment in a criminal case in the District of Kansas. 1R.446-452.[1] The district court had jurisdiction under 18 U.S.C. 3231. The court entered final judgment against defendant-appellant Patrick Stein on February 26, 2019. 1R.446-452. On the same day, Stein filed a timely notice of appeal. 1R.453-454. This Court has jurisdiction under 28 U.S.C. 1291.

---

[1] "__R.___" refers to the Record on Appeal with the first number corresponding to volume and the second to page(s). "Br. ___" refers to page numbers in Stein's opening brief.

INTRODUCTION AND STATEMENT OF THE ISSUES

Defendant Patrick Stein pleaded guilty to one count of possession of child pornography in violation of 18 U.S.C. 2252A(a)(5)(B). Stein reserved the right to appeal the district court's denial of his motion to suppress evidence of child pornography found on electronic devices seized from his home. Officers seized the devices pursuant to a search warrant obtained as part of an investigation into a plot by Stein and two co-conspirators to use a weapon of mass destruction at an apartment complex because it housed Muslim immigrants. When officers conducted an off-site search of the devices for digital evidence of the conspiracy, an agent searching image files observed child pornography. The agent stopped her search of the image files until officers obtained a second search warrant, not challenged here, to search for evidence specific to child pornography.

Stein challenges the original search warrant and accompanying affidavit on multiple grounds. Specifically, he argues that there was no probable cause to believe that digital evidence of the conspiracy would be found on electronic devices, beyond cell phones, in his home; that the warrant's grant of authority to search his computer lacked particularity; that the good-faith exception to the exclusionary rule does not apply in this case; and that the affidavit omitted four statements concerning his "need" for a computer that allegedly negated probable cause to search for such a device. This appeal presents the following questions:

1. Probable Cause And Franks

a. Whether the district court correctly concluded that the affidavit accompanying the search warrant established probable cause to believe that any electronic devices found at Stein's home would contain digital evidence of the group's ongoing conspiracy to use a weapon of mass destruction.

b. Whether the district court correctly concluded that four omissions from the affidavit that Stein challenged under *Franks* v. *Delaware*, 438 U.S. 154 (1978), were immaterial to the probable cause determination.

2. Particularity

a. Whether Stein waived his challenge to the particularity of specific paragraphs of the warrant authorizing the search of computers by not asserting—and, in fact, affirmatively disavowing—this argument in the district court.

b. Whether, on the merits, the warrant was sufficiently particular in its description of digital evidence to appropriately limit the off-site review of any electronic devices to the crime alleged or to certain types of specified material.

3. Good-Faith Exception To The Exclusionary Rule

Whether, in any event, the good-faith exception under *United States* v. *Leon*, 468 U.S. 897 (1984), applied because officers reasonably relied on a judicially authorized warrant and acted within its scope.

STATEMENT OF THE CASE

1. Factual Background

a. The search warrant at issue in this appeal followed an eight-month federal investigation into a conspiracy to use a weapon of mass destruction. In February 2016, the Federal Bureau of Investigation (FBI) received a tip from a confidential informant that a small cell of militia members who called themselves "the Crusaders" were planning a violent attack on the local Muslim community in Garden City, Kansas. 1R.50, 60-61. With the help of the confidential informant, the FBI captured months of secret recordings between defendant Patrick Stein and two co-conspirators that revealed a hate-filled and increasingly detailed plan to bomb an apartment complex and mosque primarily used by Muslim immigrants. 1R.60-61; see generally 1R.61-71.

On October 14, 2016, the FBI arrested Stein as he delivered 300 pounds of fertilizer to an undercover agent posing as a black-market source who could manufacture an explosive device. 1R.66, 70, 397. The same day, the FBI submitted an application for a search warrant with an accompanying affidavit requesting permission to search, among other places, Stein's truck and home for evidence related to the group's plan to use a weapon of mass destruction. 1R.48-71. Based on the information provided in the affidavit, the magistrate judge approved the search warrant. 1R.72-75.

b. The affidavit supporting the search warrant included statements describing the group's preparations and plans, many of which included the use of electronic devices. At a meeting in which the group "proposed and discussed a wide range of potential targets," for example, Stein's co-conspirator "pulled up Google Maps on the computer at his business and began dropping pins on the map at these various locations using the label 'cockroaches'" to indicate areas densely populated with Muslims. 1R.64. The group discussed conducting surveillance at various locations because "[t]hey wanted to get photos and videos of the places" (1R.63), and Stein told the informant that he had surveilled potential targets on three separate occasions (1R.61). The co-conspirators ultimately settled on an apartment complex as their target because it housed a mosque and a large number of Somali Muslims. 1R.65.

The affidavit stated that the co-conspirators used electronic technology to research when and how to conduct their planned attack. "The group researched mosque prayer times online to determine when the most people would be around." 1R.65. One co-conspirator "researched guides for making explosives and printed off a substantial number of pages of this material." 1R.64. Another co-conspirator watched YouTube videos "depicting the process of manufacturing explosives." 1R.68. Together, the group "decided that they would obtain four vehicles, fill

them with explosives, and park them at the four corners of the apartment complex to create a big explosion," potentially detonated remotely by cell phone. 1R.65.

The affidavit in support of the warrant made clear that, throughout this planning, the group was in close contact. They "regularly use[d] their cell phones to arrange the meetings and also utilize[d] them to engage in additional discussion and coordination of their plans via a conference call app[lication] called Zello." 1R.51. Stein told the confidential informant that he intended "to begin discussing project strategies via an encrypted mobile messaging application." 1R.66. Stein also communicated "via a smartphone application" with the purported black-market source about delivering the fertilizer to manufacture an explosive device. 1R.70.

c. Based on the FBI's knowledge of the group's communications, surveillance, and planning, the affidavit sought, among other things, authority to search Stein's house and truck for 16 categories of "evidence, fruits, and instrumentalities" of the group's plan to use a weapon of mass destruction.[2] 1R.51.

As relevant here, six of these categories encompassed records that could be found on electronic devices:

- Any and all documents, photographs, papers, written materials, books, diagrams, schematic drawings, video tapes, *computer-generated or stored information* or other materials that *relate to manufacture,*

[2] This omnibus affidavit was also used to apply to search the residence and vehicle of one of Stein's co-conspirators as well as two storage units. See 1R.50.

construction and/or assembly of improvised explosive devices, or any of the components thereof. [Paragraph G]

- Any and all receipts, invoices, purchase orders, sales slips or other documents and materials *relating to the purchase or procurement of any and all materials and tools that have been used, can be used, or intended to be used in the design, manufacture and construction of improvised explosive devices*; said documents would include, but are not to be limited to, those that denote the purchase or obtainment of any or all items previously listed in the previous paragraphs. [Paragraph H]

- Any writing or printed word items or *computer files*, in whatever format, that may *relate to terrorist individuals, explosives, bombs, terrorism, or terrorist attacks*. [Paragraph I]

- Any and all records, information, diaries, address books, names, and lists of names and addresses of individuals who may have contacted [the co-conspirators] *by use of the computer* or by other means *for the purpose of conspiring to commit an act of terrorism*. [Paragraph M]

- Any and all records, information, documents, invoices and materials, in any format or medium (including, but not limited to, * * * *email messages, chat logs and electronic messages, and other digital data files*) that *concern online storage or other remote computer storage*, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage, and any internet search history. [Paragraph N]

- Any and all records, information, documents, or correspondence, in any format or medium (including, but not limited to, * * * *email messages, chat logs and electronic messages, and other digital data files*), *pertaining to occupancy or ownership of the premises described above*, including, but not limited to, mortgage documents, utility and telephone bills, mail envelopes, or addressed correspondence. [Paragraph O]

1R.52-53 (emphases added); see also 1R.73-74. The affidavit stated that "[o]ne form in which the records might be found is data stored on a computer's hard drive or other storage media including wireless telephones," and sought "permission to search for records that might be found on any electronic devices * * * found, in whatever form they are found." 1R.55-56.

In addition, four categories in the affidavit specified the types of devices on which such digital evidence might be found:

- Computer(s), computer hardware, smart TVs, tablets, gaming consoles, computer software, computer related documentation, computer passwords and data security devices. [Paragraph J]
- Any and all computer storage media including any physical object upon which computer data can be recorded. Examples include, hard disks, RAM, floppy disks, flash memory, CD-ROM's and other magnetic or optical media. [Paragraph K]
- Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics or spreadsheet programs), utilities, compilers, interpreters, and communication programs including, but not limited to Skype. [Paragraph L]
- Any and all wireless telephones. [Paragraph P]

1R.53; see also 1R.74. In accordance with Federal Rule of Criminal Procedure 41(e)(2)(B), the affidavit specifically requested that the warrant authorize the seizure of electronic storage media for subsequent off-site review. 1R.56, 58.

d. On October 14, 2016, the magistrate judge approved the warrant and officers executed the search of Stein's home and truck. 1R.75, 80. As relevant

here, officers seized three cell phones, eight thumb drives, one laptop, and two tablets from Stein's home. 1R.81-82. During the off-site search of the electronic devices, an agent searching for image files related to the conspiracy to use a weapon of mass destruction observed images of child pornography. 2R.8. The agent stopped her review of image files in order to obtain a second search warrant to examine the electronic devices for evidence of child pornography. 2R.8. Upon executing the second warrant, officers "discovered approximately 10 to 149 images of child pornography" on Stein's laptop and on two of the thumb drives. 1R.437.

2. Procedural History

a. On October 19, 2016, Stein and two co-defendants were indicted for conspiring to use a weapon of mass destruction. Doc. 25, *United States* v. *Stein*, No. 6:16-cr-10141-EFM (D. Kan. Oct. 19, 2016). On March 15, 2017, the grand jury returned a second superseding indictment that included an additional count against the group for conspiring to violate the civil rights of the residents of the target apartment complex. See Doc. 89, *United States* v. *Stein*, No. 6:16-cr-10141-EFM (D. Kan. Mar. 16, 2017). The next day, Stein was separately indicted in this case for possessing child pornography. 1R.11-12.

b. Before trial in the conspiracy case, Stein moved to suppress all physical evidence seized during the search of his home and truck. Doc. 203, *United States* v. *Stein*, No. 6:16-cr-10141-EFM (D. Kan. Jan. 11, 2018). Among other

arguments, Stein argued that the affidavit used to obtain the search warrant failed to establish probable cause that he owned a computer, that a computer would be found in his home, and that evidence of the conspiracy would be found on a computer. Doc. 204, at 23, *United States* v. *Stein*, No. 6:16-cr-10141-EFM (D. Kan. Jan. 11, 2018). As a result, according to Stein, the warrant's inclusion of a computer rendered the warrant overbroad in its entirety. *Id.* at 25. In addition, Stein requested a *Franks* evidentiary hearing, arguing that the affidavit failed to include information known to the FBI that Stein did not want an informant using a computer and that Stein himself needed a laptop. See *id.* at 2-4, 20-21.

The district court resolved Stein's motion over the course of three hearings. On February 20, 2018, the court heard argument from counsel on the motion. 1R.138-202. The next day, the court granted Stein's motion in part to permit a *Franks* hearing. 1R.292, 380-383. At the *Franks* hearing on March 19, 2018, the court heard testimony from the officer who signed the affidavit and additional argument from counsel. 1R.205-284. At multiple points in these hearings, Stein's counsel clarified that he was not challenging the search *of* the computer, only the search *for* a computer. See 1R.148-149 ("[W]e are not arguing the search of the computer. I just want to make that clear. We're just arguing the seizure of the computer."); see also 1R.260 ("[W]e have not argued the search of the computer.

We have only argued the seizure of the computer and everything seized in the house * * * should be suppressed.").

At the end of the *Franks* hearing, the court denied Stein's motion to suppress from the bench. 1R.290. As for whether probable cause existed to include computers in the search warrant, the court noted that the conspiracy with which the defendants were charged "was a complicated and an involved and a complex undertaking that involved many meetings and long periods of time and a fair amount of details." 1R.288. The court reasoned that "it's not unusual that those types of items might have been recorded, inventoried, searched for, organized, or otherwise [present] on a computer in Mr. Stein's home." 1R.288. The court reached the same conclusion even after considering what it stated were "not necessarily irrelevant but somewhat indirect statements that inferred [*sic*] that [Stein] did not have a computer." 1R.288. Even if the omissions had been included, the court found, the magistrate judge "would have still found it reasonable to believe that a computer might exist in the home" and that "it might contain information relating to this issue." 1R.288-289.

The case proceeded to trial and Stein was convicted of conspiracy to use a weapon of mass destruction and to violate civil rights. The court sentenced Stein to 360 months' imprisonment on those charges, and Stein appealed his conviction and sentence. In his opening brief on appeal in the conspiracy case (Case No. 19-

3030), Stein did not challenge the search warrant at issue here or seek to suppress other physical evidence seized from his home and truck.

c. Following the jury verdict in his conspiracy case, Stein moved in the district court in this child pornography case to suppress all physical evidence seized during the search of his home and requested a *Franks* evidentiary hearing. 1R.13-15. Stein abandoned the challenge to the search of his truck, but otherwise raised the same arguments he had raised in his conspiracy case. See 1R.17 n.2, 133-134. As in his conspiracy case, Stein argued that the search warrant was overbroad in its entirety for including a computer among the items to be seized because, in his view, the affidavit did not establish probable cause to believe that he had a computer and omitted information concerning whether he possessed a computer at various points in the conspiracy. See 1R.34-40; see also 3R.12-14.

At a hearing on September 11, 2018, the same district court judge who presided over the conspiracy case heard argument from counsel in this case. 3R.4-21. When the court asked Stein's counsel whether "there [were] any additional matters [he'd] want presented at a *Franks* hearing," counsel replied: "I did look at the issue of the search of the devices and determined that the strongest issues were presented to the Court at the prior hearing and that those were probably the only issues that were relevant." 3R.6. In other words, in the district court in this case, Stein continued to challenge only the search of his home for electronic devices

beyond cell phones. He did not challenge the search of such devices once they had been seized. The court granted Stein's request for a *Franks* hearing and, with the parties' agreement, took judicial notice of the *Franks* hearing from the conspiracy case. 3R.20; see also 1R.399.

In a written order, the district court denied Stein's motion to suppress. 1R.394-418. The court explained that Stein's argument that the search warrant was overbroad for including computers without sufficient probable cause was "more appropriately analyzed as a question of probable cause," not overbreadth. 1R.405-406.

As to probable cause, the court found that "if Stein did possess a computer, there was a reasonable likelihood that the computer would contain information related to the conspiracy, even if Stein did most of his online activity on his phone." 1R.407. The court also concluded that the contested omissions from the affidavit regarding Stein's "need" for a computer were immaterial as they "d[id] not negate probable cause to seize any computers found in Stein's residence." 1R.407; see also 1R.403-405. As a result, the court held "the search warrant affidavit did not violate *Franks*." 1R.405. Finally, the court held that "the good-faith exception to the exclusionary rule provides an independent reason to deny Stein's motion to suppress regarding the search of Stein's residence for a computer and other items related to the conspiracy." 1R.417.

d. Stein pleaded guilty to possession of child pornography, in violation of 18 U.S.C. 2252A(a)(5)(B), but "retain[ed] the right to appeal the decision rendered by the Court (reflected in Doc. 43) in denying his motion to suppress." 1R.439. The court sentenced Stein to 44 months' imprisonment to run consecutively to his sentence in the conspiracy case. 1R.447. Stein filed a timely notice of appeal. 1R.453.

SUMMARY OF ARGUMENT

This Court should affirm the district court's denial of Stein's motion to suppress. The warrant is based on a showing of probable cause to search for digital evidence of the planned attack on any electronic devices found in Stein's home and is sufficiently particular in its description of this evidence to appropriately limit the search of any electronic devices seized. The probable-cause determination is unaffected by the four omissions from the affidavit that Stein contests, and this Court need not even reach whether the computer search was appropriately limited because Stein waived the issue. On both probable cause and particularity, though, this Court can easily resolve this appeal by affirming on the basis of good faith, a topic to which the Court can turn immediately. See pp. 39-44, *infra*.

1. Probable cause existed to believe that digital evidence of Stein and his co-conspirators' plan to use a weapon of mass destruction would be found on any

electronic devices, beyond cell phones, found in Stein's home. A sufficient nexus existed between the alleged conspiracy, digital evidence, and Stein's home as a result of (1) the extent to which this conspiracy was researched and developed online with various technology; (2) the nature of the digital evidence on Stein's cell phone that could be transferred to other electronic devices; and (3) reasonable inferences as to where defendants are likely to keep electronic devices with such digital evidence.

The four omissions from the affidavit that Stein challenged under *Franks* v. *Delaware*, 438 U.S. 154 (1978), do not negate probable cause. To be sure, the omissions could be read to imply that Stein did not possess a computer at certain points during the group's planning. But the same statements also show that Stein, aware of the utility of a computer in planning this attack, was actively seeking a laptop. The information available to the FBI did not shed light on whether Stein previously had a computer that he needed to replace, whether he successfully found one thereafter, or whether he used other electronic devices such as tablets or thumb drives to plan the attack or store information related to the conspiracy. In fact, Stein's repeated statements to the informant that he was looking for a computer support the probable cause to believe that digital evidence would be found at his home on any computer that he previously had or later acquired.

2. Before the district court, Stein did not raise—and, in fact, affirmatively disavowed—his current argument that the paragraphs in the warrant authorizing the search of his electronic devices were insufficiently particular. He therefore waived the argument. In any event, the warrant did not authorize a "general rummaging" through Stein's electronic possessions, and the agent conducting the search did not proceed as if it did. Rather, when read in context, the authority to seize and search electronic devices off-site was practically constrained by the highly detailed paragraphs listing the digital evidence sought and by the overarching focus of the warrant and affidavit on evidence related to the group's plot to bomb the targeted apartment complex.

3. Because officers reasonably relied on a search warrant issued by a magistrate judge and acted within its scope, the good-faith exception to the exclusionary rule applies unless limited and specific circumstances exist. Stein argues that the good-faith exception does not apply in this case because the warrant was so lacking in probable cause and particularity. Not so. Even if the affidavit did not establish a sufficient nexus for probable cause to search Stein's home for digital evidence of the conspiracy on electronic devices, it plainly established the minimal nexus required for good faith. And, even if the warrant was insufficiently particular in some respect, it certainly was not facially deficient. Accordingly, the

Court can affirm the denial of the motion to suppress on the basis of a straightforward application of the good-faith exception to the exclusionary rule.

ARGUMENT

THIS COURT SHOULD AFFIRM THE DISTRICT COURT'S DENIAL OF STEIN'S MOTION TO SUPPRESS

Under the Fourth Amendment, "a warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky* v. *King*, 563 U.S. 452, 459 (2011). If a warrant falls short on either basis, the good-faith exception to the exclusionary rule will apply so long as "an officer acting with objective good faith has obtained a search warrant from a judge or magistrate and acted within its scope." *United States* v. *Leon*, 468 U.S. 897, 920 (1984); see also *United States* v. *Leary*, 846 F.2d 592, 607 (10th Cir. 1988) (noting that the good-faith exception applies to errors of both probable cause and particularity). The Court has discretion to "turn[] immediately to a consideration of the officers' good faith" to deny a motion to suppress without resolution of the Fourth Amendment question. *Leon*, 468 U.S. at 925; see also *United States* v. *Danhauer*, 229 F.3d 1002, 1005 (10th Cir. 2000).

Here, Stein challenges the warrant for lacking both probable cause and, if preserved, particularity. As described below, neither argument has merit. In any event, the good-faith exception to the exclusionary rule applies under the facts and circumstances of this case.

A. The Affidavit Accompanying The Search Warrant Established Probable Cause To Search Electronic Devices Found In Stein's Home For Digital Evidence Of His Plot To Blow Up A Predominantly Muslim Apartment Complex

1. Standard Of Review

Questions of law, such as whether a warrant was supported by probable cause and whether contested omissions from the affidavit would negate probable cause under *Franks*, are reviewed de novo. *United States* v. *Ruiz*, 664 F.3d 833, 838 (10th Cir. 2012); *United States* v. *Gonzales*, 399 F.3d 1225, 1228 (10th Cir. 2005).

Like the district court, however, this Court must "accord 'great deference' to the probable-cause assessment of the [magistrate] judge who issued the warrant." *United States* v. *Pulliam*, 748 F.3d 967, 970-971 (10th Cir. 2014). In light of this deference, appellate review "is limited to ensur[ing] the Government's affidavit provided a substantial basis for the issuance of the warrant." *Id.* at 971 (internal quotation marks and citation omitted; brackets in original).

2. The Affidavit Established A Sufficient Nexus Between Stein's Planned Attack And Electronic Devices At His Home

The district court properly concluded that the affidavit in support of the search warrant established probable cause to believe that electronic devices found in Stein's home, including but not limited to cell phones, would contain digital evidence of Stein and his co-conspirators' plan, developed over eight months, to

bomb an apartment complex during prayer time to kill as many Muslim immigrants as possible.

a. Probable cause supports a search warrant if "there is a fair probability that * * * evidence of a crime will be found in a particular place." *Illinois* v. *Gates*, 462 U.S. 213, 238 (1983); see also *United States* v. *Soderstrand*, 412 F.3d 1146, 1152 (10th Cir. 2005), cert. denied, 547 U.S. 1004 (2006). Beyond allegations that the defendant is guilty of a crime, there must be a "nexus" between the "suspected criminal activity and the place to be searched." *United States* v. *Biglow*, 562 F.3d 1272, 1278-1279 (10th Cir. 2009). Nevertheless, "little 'additional evidence' is generally required to satisfy the Fourth Amendment's strictures." *Id.* at 1279.

This Court has stated that "a 'sufficient nexus' is surely established by a search warrant when the materials supporting it describe 'circumstances which would warrant a person of reasonable caution [to believe] that the articles sought are at a particular place.'" *United States* v. *Harris*, 735 F.3d 1187, 1190 (10th Cir. 2013) (brackets in original) (citing *Biglow*, 562 F.3d at 1279). Factors to consider include "(1) the type of crime at issue, (2) the extent of a suspect's opportunity for concealment, (3) the nature of the evidence sought, and (4) all reasonable inferences as to where a criminal would likely keep such evidence." *Biglow*, 562 F.3d at 1279; see also *United States* v. *Potts*, 586 F.3d 823, 831 (10th Cir. 2009)

(applying these factors to determine whether a sufficient nexus existed to search for evidence of child pornography at defendant's residence).

b. Probable cause existed to search electronic devices found in Stein's home for digital evidence of the conspiracy to use a weapon of mass destruction because of the specifics of this conspiracy, the nature of digital evidence, and reasonable inferences concerning where a criminal would keep electronic devices beyond cell phones. Simply put, the magistrate judge could have reasonably believed that digital evidence of Stein's planned attack—including information on manufacturing an improvised explosive device, computer files on terrorist attacks, computer searches and image files regarding the targeted apartment complex, and contact information of potential terrorist co-conspirators—would be found on any electronic devices found in Stein's home.

i. First, given the nature of the co-conspirators' crime, which involved extensive research, planning, and discussion online, the magistrate judge reasonably could have believed that Stein may have used electronic devices, beyond cell phones, and that they would contain evidence of the group's plot. "The group researched mosque prayer times online" (1R.65), which could be accomplished through any internet-capable device. Likewise, Stein was tasked with obtaining materials to manufacture explosives (1R.65, 67), which could leave a digital trail of search history and purchase receipts. Stein also conducted

surveillance (1R.61), which may have created digital media evidence given the group's desire "to get photos and videos of the [possible targets] during the day" (1R.63). The magistrate judge reasonably could have believed that such evidence could be stored on any computers, tablets, thumb drives, and electronic storage devices found in Stein's home.

Moreover, the affidavit stated that the group used one co-conspirator's business computer to pick a target and that another co-conspirator learned how to make explosives from YouTube. 1R.64, 68. Given the nature of this conspiracy and the extent to which the group relied on technology to research, plan, and discuss their attack, it was reasonable to believe that Stein also used electronic devices beyond a cell phone, including devices that could store any digital information the group already had obtained (*e.g.*, surveillance photos), in the commission of the crime. Following this logic, the district court found that, "[w]hile much of this activity was conducted on Stein's phone, it was reasonable to infer that some of the online activity could have been done on a computer, as well." 1R.407.

ii. Second, the magistrate judge reasonably could have believed that any electronic devices found at Stein's home may have captured evidence the FBI knew to exist on Stein and his co-conspirators' internet-capable cell phones based on its months-long investigation. Stein does not and cannot dispute that digital

evidence of the group's evolving plans would be found on the cell phones belonging to Stein and his co-conspirators. The affidavit made clear that Stein and his co-conspirators "regularly use[d] their cell phones to arrange the meetings and also utilize[d] them to engage in additional discussion and coordination of their plans." 1R.51. In addition, Stein specifically instructed the confidential informant to "begin discussing project strategies via an encrypted mobile messaging application" (1R.66), and discussed "via a smartphone application" the undercover agent's ability to manufacture an explosive device (1R.70).

The nature and quantity of evidence that the FBI expected to find on the group's cell phones increased the likelihood that evidence would be found on other electronic devices. By its nature, digital evidence can be transferred seamlessly, intentionally or otherwise, between electronic devices. For instance, it is now easy to sync a cell phone with a cloud-based storage system, which can automatically update a laptop or tablet. And, even without a laptop or tablet, someone with a cell phone can easily transfer photos from that phone to an electronic storage device for safe keeping. As the district court stressed, "the affidavit established that, based on the affiant's training and experience, such electronic communications are sometimes automatically downloaded to electronic devices with internet access and can be recovered from the device's 'cache.'" 1R.407; see also 1R.56.

Recognizing this link, the Seventh Circuit in *United States* v. *Reichling*, found that a defendant's use of a cell phone in the commission of a crime established probable cause to search for other electronic devices. 781 F.3d 883 (7th Cir.), cert. denied, 136 S. Ct. 174 (2015). In that case, the defendant "concede[d] that the search warrant affidavit established probable cause to believe that he sent the victim the quoted text messages from a cell phone and received naked photos of the victim on a cell phone," but challenged the warrant's authority to seize and search other items, including computers, external hard drives, and thumb drives. *Id.* at 886. The Seventh Circuit rejected this argument given the "common knowledge * * * that images sent via cell phones or Facebook accounts may be readily transferred to other storage devices, such as those identified in the warrants." *Id.* at 887.

The reasoning of *Reichling* applies with equal force to the facts of this case. That is not to say that officers can search other electronic devices any time a defendant uses a cell phone in any capacity. Here, however, given the probable cause to believe that Stein's cell phone contained significant amounts of digital evidence regarding the ongoing conspiracy to use a weapon of mass destruction to kill innocent Muslim immigrants, it was reasonable to infer that some evidence, by its nature, would be transferred to other electronic devices kept at his home.

iii. Finally, the magistrate judge could have reasonably believed that electronic devices with digital evidence of this conspiracy would be found at Stein's home. As the Sixth Circuit recently reasoned, computers are "personal possessions often kept in their owner's residence." *Peffer* v. *Stephens*, 880 F.3d 256, 272 (6th Cir.), cert. denied, 139 S. Ct. 108 (2018). Accordingly, "the averment that [the defendant] used [a computer] in the commission of a crime is sufficient to create the presumption that it would be found at his residence." *Id.* at 273.

c. Stein argues that the affidavit failed to establish probable cause to believe that evidence of any crime would be found on electronic devices found in Stein's home beyond cell phones. Br. 14. He asserts that "[t]he criminal activity alleged had absolutely nothing to do with digital media." Br. 15. In addition, he argues that there is "no indication in the affidavit that the FBI believed Mr. Stein or his codefendants were using electronic devices other than cellular phones to further the conspiracy." Br. 16.

To the contrary, Stein and his co-conspirators planned much of their attack online, researching and discussing everything from where to attack to how to make explosives. Given the specifics of this conspiracy, the nature of digital evidence, and reasonable inferences about where such evidence would be, it was reasonable to believe that Stein used electronic devices beyond cell phones, that they would

contain evidence of the planned attack, and that Stein would keep them at his home.

3. The Four Contested Omissions From The Affidavit Are Immaterial To The Probable Cause Determination Under Franks

Stein next argues that the search warrant is nevertheless invalid under *Franks* v. *Delaware*, 438 U.S. 154 (1978), because of four contested omissions from the affidavit concerning his "need" for a computer. Br. 31-36. This argument fails. The information on which Stein relies is immaterial to the probable cause determination, as the district court recognized. Indeed, if anything, the contested omissions would have *bolstered* probable cause to search Stein's home for electronic devices beyond cell phones.

"Under *Franks*, a Fourth Amendment violation occurs if (1) an officer's affidavit supporting a search warrant application contains a reckless misstatement or omission that (2) is material because, but for it, the warrant could not have lawfully issued." *United States* v. *Herrera*, 782 F.3d 571, 573 (10th Cir. 2015). Below, the district court focused its inquiry on materiality, as we also do. 1R.403-405. An omission is considered material "if it is 'so probative as to negate probable cause.'" *United States* v. *Ruiz*, 664 F.3d 833, 838 (10th Cir. 2012) (citation omitted).

Here, the four pieces of information that Stein argues should have been included in the 22-page affidavit are immaterial to the probable cause

determination. Br. 8 (listing the contested omissions). As the district court explained, "[a]dding the omitted information to the affidavit would not negate probable cause." 1R.405. In fact, "it could have made the Government's application stronger." 1R.405.

First, Stein cites a summary FBI report from April 2016 stating that "Stein did not want [the confidential informant] to make any plans on a computer because he did not want there to be a record." 1R.96; see also 1R.398. Instead, "[Stein] would keep any plans secure, but would make sure people would still have access to plans." 1R.96. This summary does not help him. Stein's instruction to the informant not to use a computer does not affect the likelihood that Stein himself used a computer. To the contrary, Stein suggested that he would be responsible for keeping any records.

Second, Stein cites an August 2016 recording, in which he asked the informant to let him know if the informant heard of "anybody whose gotta * * * decent laptop they wanna get rid of." 1R.96. He suggests that this statement shows that he did not own or use a computer. See Br. 32. But, Stein's interest in acquiring a laptop in the midst of the group's planning does not negate the possibility that he already had one. Moreover, his interest in obtaining a laptop actually supports the probable cause to believe that he would use a computer if he

had one—and, therefore, that any computers found in his home would contain evidence of the conspiracy to bomb the apartment building.

Third, Stein cites a statement he made three days later when, in response to a question about needing a laptop, he stated that he's "been in desperate need for some time." 1R.98. "[I]f anybody pays attention to shit I do," he said, "I do every * * * bit of it on my phone, all of it." 1R.98. He then stated that he "was lookin' at the Google Chromebook." 1R.100. Although this statement casts doubt on whether he, at that time, was using an electronic device beyond a smart phone, it does not resolve whether he previously had a laptop or whether he successfully acquired one. Moreover, the statement actually bolsters the likelihood that, if he had or acquired a laptop or other computer, he would use it in addition to his cell phone in the commission of this crime.

Fourth, Stein cites a statement the informant made in a September 27, 2016, recording, namely, that "he [Stein] don't have internet, he don't have a computer uh anything." 1R.102.[3] Briefly thereafter, the informant offered some clarification: "I mean he's on the internet (unintelligible)." 1R.103. These statements do not add to Stein's argument because they simply reiterate the same

[3] The transcript in the Record on Appeal reflects an incorrect date of October 25, 2016. 1R.101. The parties and the district court understood this recording to be from September 27, 2016 (see 1R. 398; Br. 8), a few weeks before Stein's October 14, 2016, arrest.

information Stein himself conveyed in the previous recording, *i.e.*, that he did not, at that time, have a computer.

In sum, these statements do not resolve whether Stein previously had a computer or acquired one afterwards. Indeed, they say nothing about whether he owned other electronic devices, such as tablets, or whether he used other electronic devices, such as thumb drives, to save digital files or other electronic information from his cell phone or another person's computer. As the district court correctly concluded, even if these statements were included in the affidavit, probable cause would exist to search for digital evidence on any electronic devices found in Stein's home. 1R.407. As a result, the statements were immaterial to the probable cause determination and their omission does not provide a basis to invalidate the search warrant.

B. Stein Has Waived His Specific Arguments Concerning The Particularity Of The Warrant's Authorized Computer Search And They Are Meritless In Any Event

1. Standard Of Review

This Court reviews de novo a district court's ruling on whether a search warrant describes with sufficient particularity the things authorized to be seized. See *United States* v. *Brooks*, 427 F.3d 1246, 1251 (10th Cir. 2005), cert. denied, 546 U.S. 1222 (2006). New arguments to suppress evidence, however, "are waived absent a showing of good cause for why they were not raised below."

United States v. *Burke*, 633 F.3d 984, 991 (10th Cir.), cert. denied, 563 U.S. 951 (2011); see also *United States* v. *Bowline*, 917 F.3d 1227, 1236 (10th Cir.) (holding that "*Burke* remains good law" after the 2014 amendment to Federal Rule of Criminal Procedure 12), petition for cert. pending, No. 19-5563 (filed Aug. 13, 2019). This "rule applies not only when a defendant fails to file a pretrial motion to suppress, but also when a defendant fails to assert a particular argument in a pretrial suppression motion." *United States* v. *Vance*, 893 F.3d 763, 769-770 (10th Cir. 2018); see, *e.g.*, *United States* v. *Williams*, 942 F.3d 1187, 1191 (10th Cir. 2019) (holding that the defendant's argument regarding "the scope and duration of his laptop search * * * ha[d] been waived as it was not raised in the motion to suppress and [defendant] did not show good cause").

2. Stein Has Waived His Arguments Concerning The Particularity Of The Warrant's Authorized Computer Search By Not Raising Them Before The District Court

To the extent that Stein argues on appeal that the computer search authorized by the warrant was insufficiently particularized because it failed to appropriately limit the digital evidence to be seized, this is a new and distinct argument from the arguments he raised in the district court. As such, the argument is waived absent a showing of good cause, which Stein cannot establish. See *Burke*, 633 F.3d at 991.

In the district court, Stein made two particularity arguments. First, he argued that the warrant was overbroad because it allowed officers to search his

entire home for "common household items," such as nails, staples, and twine. See 1R.40-42. As to this argument, Stein specifically challenged paragraphs A, D, and E of the warrant. 1R.40-41. Second, Stein argued that the warrant was overbroad in its entirety because it authorized a search for computers. See 1R.34-40. More specifically, he argued that there was no probable cause to search his home for a computer at all and, therefore, including computers among the items to be seized rendered the warrant overbroad. See 3R.13-14 (arguing "[i]t is the fact that they had no evidence that there would be a computer, by adding the computer and other electronic devices * * * that was overbreadth").

On appeal, Stein now argues that the computer search was overbroad in three interrelated ways. Br. 18-25. He asserts that (1) the search warrant allowed for "a nearly limitless grant" of authority to search the electronic devices seized; (2) the search warrant's "expansive language" failed to appropriately limit the computer search under *United States* v. *Carey*, 172 F.3d 1268 (10th Cir. 1999); and (3) the "paragraphs of the warrant related to electronic media fail to include any narrowing language." See Br. 18-25.

Neither of Stein's particularity arguments in the district court, though, encompassed any of his particularity arguments on appeal. Stein's first argument below, which the district court considered and rejected (see 1R.407-409), concerned tangible "common household items," not digital evidence. His second

argument below, which the district court correctly concluded was simply a variant of his probable cause argument (see 1R.405-406),[4] concerned only the authority to seize computers, not their subsequent search once seized.

In fact, Stein affirmatively disavowed any challenge to the search of the computer. In the conspiracy case, his trial counsel stated: "[W]e have not argued the search of the computer. We have only argued the seizure of the computer and everything seized in the house * * * should be suppressed." 1R.260; see also 1R.145, 148-149. When the district court asked Stein's trial counsel at the suppression hearing in this case whether there were any additional matters to present beyond those raised in the conspiracy case, Stein's counsel again abandoned any challenge to the search of the devices. 3R.6 ("I did look at the issue of the search of the devices and determined that the strongest issues were presented to the Court at the prior hearing and that those were probably the only issues that were relevant.").

[4] The distinction, the court noted, was simply "one of remedy." 1R.406 n.11. If Stein had been successful in specifically challenging the paragraphs of the warrant concerning electronic devices for lacking probable cause, only the electronic evidence would have been suppressed. Instead, in the district court, Stein sought to suppress all physical evidence (digital and tangible) seized from his home by arguing that the warrant was insufficiently particular in its entirety for allowing officers to search for electronic devices without sufficient probable cause to support a search for digital evidence of the conspiracy.

In sum, Stein has moved from arguing *whether* electronic devices should have been included in the search warrant at all to arguing *how* the authority to search electronic devices for digital evidence should have been limited. But Stein chose not to raise this latter argument below, and cannot establish good cause for raising it belatedly on appeal. As a result, this Court should deem Stein's particularity challenge to the search of the electronic devices waived. See *Burke*, 633 F.3d at 991.

3. The Warrant's Grant Of Authority To Seize Electronic Devices To Conduct An Off-Site Search For Specific Digital Records Is Sufficiently Particular

Even if this Court reaches the merits of Stein's arguments, his challenge to the particularity of the computer search as authorized by the warrant is unpersuasive. "A description is sufficiently particular when it enables the searcher to reasonably ascertain and identify the things authorized to be seized." *United States* v. *Riccardi*, 405 F.3d 852, 862 (10th Cir.) (quoting *United States* v. *Leary*, 846 F.2d 592, 600 (10th Cir. 1988), cert. denied, 546 U.S. 919 (2005). As relates to computer searches, this Court has stated that officers "cannot simply conduct a sweeping, comprehensive search of a computer's hard drive." *United States* v. *Walser*, 275 F.3d 981, 986 (10th Cir. 2001) (summarizing *United States* v. *Carey*, 172 F.3d 1268 (10th Cir. 1999)), cert. denied, 535 U.S. 1069 (2002). Computer searches "may be as extensive as reasonably required to locate the items described

in the warrant," but "[o]fficers must be clear as to what it is they are seeking on the computer and conduct the search in a way that avoids searching files or types not identified in the warrant." *United States* v. *Potts*, 586 F.3d 823, 833 (10th Cir. 2009) (citations omitted; brackets in original).

For this reason, this Court has "invalid[ated] warrants purporting to authorize computer searches where [it] could discern no limiting principle," such as where the warrant "permitted a search of 'any and all' information, data, devices, programs, and other materials." *United States* v. *Christie*, 717 F.3d 1156, 1164-1165 (10th Cir. 2013) (internal quotation marks omitted) (quoting *United States* v. *Otero*, 563 F.3d 1127, 1132-1133 (10th Cir. 2009)). In contrast, this Court has approved of warrants "if they limit their scope either 'to evidence of specific federal crimes or [to] specific types of material.'" *Id.* at 1165 (brackets in original) (quoting *Riccardi*, 405 F.3d at 862).

Stein argues that the warrant here "lacks the requisite particularity" as relates to the computer search. See Br. 18; see generally Br. 18-25. He cherry-picks four paragraphs (paragraphs K, L, N, and O) which he says include "problematic 'catch-all' phrases," and, taken out of context, do not limit the search to the crime at issue. Br. 19, 23. He also suggests that the warrant somehow violates *Carey*'s requirement that a computer search be appropriately limited. See Br. 20-22.

The text of the warrant, however, must be understood as a whole "with due regard to context, coupled with the specifics of the supporting affidavit." See *United States* v. *Burgess*, 576 F.3d 1078, 1092 (10th Cir.), cert. denied, 558 U.S. 1097 (2009); see also *Brooks*, 427 F.3d at 1252 (analyzing the language of the warrant "as a whole"). Read in full, the warrant authorizes the seizure of electronic devices, storage media, and software to search for specified digital evidence, insofar as they are tied either to the crime alleged or to the type of material. The off-site search then enabled officers to conduct a careful review of the items seized for digital evidence of the alleged conspiracy. The agent conducting the search acted pursuant to the warrant's limits.

a. First, the warrant authorized the search for clearly defined digital evidence tied to the alleged crime of conspiring to use a weapon of mass destruction. Paragraph G, for example, seeks "computer-generated or stored information * * * that relate to manufacture, construction and/or assembly of improvised explosive devices, or any of the components thereof." 1R.73. Likewise, Paragraph H concerns the "purchase or procurement of any and all materials and tools that have been used, can be used, or intended to be used in the design, manufacture and construction of improvised explosive devices." 1R.73. Paragraph I includes "computer files * * * that may relate to terrorist individuals, explosives, bombs, terrorism, or terrorist attacks." 1R.74. Paragraph

M is limited to individuals who contacted defendants "for the purpose of conspiring to commit an act of terrorism." 1R.74. Stein does not challenge any of these provisions in the warrant and, in fact, uses Paragraph I as an example of an appropriately constrained search target. Br. 22-23.[5]

b. Second, the warrant authorized the search for clearly defined digital evidence limited to the type of material at issue. Paragraph N includes "[a]ny and all records * * * *that concern online storage or other remote computer storage*, including, but not limited to," evidence such as software or user logs that show access to such online storage. 1R.74 (emphasis added). Paragraph O includes "[a]ny and all records * * * *pertaining to occupancy or ownership of the premises* * * * including, but not limited to," evidence such as "mortgage documents" or bills. 1R.74 (emphasis added).

[5] To the extent that the Court disagrees that Stein's particularity argument is waived, that the paragraphs he challenges are sufficiently particular, and that the good-faith exception nevertheless applies, see pp. 28-39, 43-44, *infra*, it must engage in a severability analysis of the contested paragraphs. Under this analysis, "valid portions of a warrant are severed from the invalid portions and only materials seized under the authority of the valid portions, or lawfully seized while executing the valid portions, are admissible." *United States* v. *Sells*, 463 F.3d 1148, 1155 (10th Cir. 2006), cert. denied, 549 U.S. 1229 (2007). Here, Stein's particularity challenge on appeal goes only to paragraphs K, L, N, and O. Br. 19, 23. Even if the Court determines that these paragraphs are insufficiently particularized and must be stricken, officers still would have searched the computer pursuant to the uncontested paragraphs G, H, I, and M, and still would have had a basis to seek the second warrant for a further search specific to child pornography.

Stein ignores the italicized language, focusing instead on the "any and all" and "not limited to" phrases. But these phrases do not, by their mere presence, automatically invalidate a warrant. See, *e.g.*, *United States* v. *Pulliam*, 748 F.3d 967, 972 (10th Cir. 2014) (rejecting a particularity challenge to a search warrant that included "[a]ny and all firearms" and "[a]ll items of indicia for proof of ownership and occupancy"). For example, this Court has held that "the 'not limited to' language does not taint a warrant when the language serves only to modify one or more categories in the list." *United States* v. *Dunn*, 719 F. App'x 746, 749 (10th Cir. 2017) (unpublished). Here, too, the phrases "any and all" and "not limited to" modify specific categories of documents that are explicitly limited to a type of material, *i.e.*, online storage or occupancy.

c. Third, the warrant authorized the seizure of electronic devices, storage media, and software. Paragraph J listed a defined universe of electronic devices: "[c]omputer(s), computer hardware, smart TVs, tablets, gaming consoles, computer software, computer related documentation, computer passwords, and data security devices." 1R.74. Paragraphs K and L, in turn, included "[a]ny and all computer storage media" and "[a]ny and all computer software. 1R.74.

Stein objects to the last two paragraphs (K and L) because they use the "any and all" phrase (Br. 19-20), but the wholesale seizure of such digital media is necessary to conduct a limited off-site review. In a section titled, "[n]ecessity of

seizing or copying entire computers or storage media," the affidavit explained that reviewing a hard drive "for things described in the warrant" can take time and "sometimes requires tools or knowledge that might not be present on the search site." 1R.58. As a result, "[i]n most cases, a thorough search of a premises for information that might be stored on a storage media often requires the seizure of the physical storage media and later off-site review consistent with the warrant." 1R.58.

The procedure used here to seize all electronic media for a later, targeted review of its contents is specifically authorized by Federal Rule of Criminal Procedure 41(e)(2)(B), and has been approved by courts. See *United States* v. *Schesso*, 730 F.3d 1040, 1046 & n.3 (9th Cir. 2013) (noting this procedure "is not out of the ordinary"). This Court has rejected a particularity challenge in a case where the affidavit "made clear that the search of the computer would be off-site in a laboratory setting." See *United States* v. *Grimmett*, 439 F.3d 1263, 1269 (10th Cir. 2006). As a sister circuit summarized, "[t]he federal courts are in agreement that a warrant authorizing the seizure of a defendant's home computer equipment and digital media for a subsequent off-site electronic search is not unreasonable or overbroad, as long as the probable-cause showing in the warrant application and affidavit demonstrate a sufficient chance of finding some needles in the computer

haystack." *United States* v. *Evers*, 669 F.3d 645, 652 (6th Cir. 2012) (internal quotation marks and citation omitted).

d. Finally, as to the conduct of the search, Stein cannot seriously argue that that officers exceeded the scope of the warrant. See Br. 20-22. In *Carey*, this Court found an "unconstitutional general search" of a defendant's computer when the officer exceeded the scope of the warrant. 172 F.3d at 1276. Subsequently, in *Walser*, this Court explained that the problem in *Carey* was that, after inadvertently discovering evidence of child pornography, the officer "proceeded to rummage through the hard drive for more images of child pornography despite the fact that he did not possess a warrant to conduct such a search." 275 F.3d at 987. The officer in *Walser*, in contrast, "showed restraint by returning to the magistrate for a new warrant before commencing a new search for evidence of child pornography." *Ibid.*

In his brief, Stein cites both *Carey* and *Walser* and argues incorrectly that "[n]o such caution was employed here." Br. 21-22. To the contrary, the agent in this case proceeded along the same lines, approved by this Court, as the officer in *Walser*. When the agent came across evidence of child pornography in her search for image evidence of the conspiracy to use a weapon of mass destruction, she stopped her review, returned to the magistrate, and obtained an additional warrant

that would authorize a search specific to child pornography. 2R.8. The conduct of this search was reasonable and within the confines of the warrant as written.

In sum, contrary to Stein's assertion (see Br. 20), the warrant's authorization for a computer search was sufficiently particularized given its practical operation. As this Court has recognized, "in the age of modern technology[,] * * * the warrant could not be expected to describe with exactitude the precise form the records would take." *United States* v. *Reyes*, 798 F.2d 380, 383 (10th Cir. 1986); see also *United States* v. *Tsarnaev*, 53 F. Supp. 3d 450, 457 (D. Mass. 2014) (noting that "[s]ometimes only generic description is possible"). The warrant was written with sufficient particularity and the search was carried out within its limits.

C. The Good-Faith Exception To The Exclusionary Rule Provides An Independent Reason To Deny Stein's Motion To Suppress

1. Standard Of Review

Whether the good-faith exception to the exclusionary rule applies is a question of law that this Court reviews de novo. *United States* v. *Gonzales*, 399 F.3d 1225, 1228 (10th Cir. 2005).

2. The Good-Faith Exception To The Exclusionary Rule Applies Because Officers Reasonably Relied On The Warrant Issued By The Magistrate Judge

The allegations included in the affidavit accompanying the search warrant established probable cause to search for digital evidence on electronic devices found in Stein's home and the warrant's authorization for this search was

sufficiently particular. But, even if the warrant fell short in some respect on either probable cause or particularity, the good-faith exception to the exclusionary rule applies because officers reasonably relied on the magistrate judge's issuance of the warrant.

In *United States* v. *Leon*, 468 U.S. 897 (1984), the Supreme Court held that suppression of evidence obtained with a warrant is only proper "in those unusual cases in which exclusion will further the purposes of the exclusionary rule," which is to deter police misconduct. *Id.* at 918; see also *United States* v. *Russian*, 848 F.3d 1239, 1246 (10th Cir. 2017). The good-faith exception "provides that evidence seized pursuant to the warrant need not be suppressed if the executing officer acted with an objective good-faith belief that the warrant was properly issued by a neutral magistrate." *United States* v. *Barajas*, 710 F.3d 1102, 1110 (10th Cir.) (internal quotation marks and citation omitted), cert. denied, 571 U.S. 896 (2013). Thus, this Court "presume[s] good-faith when an officer acts pursuant to a warrant unless one of 'four contexts' apply." *Ibid.* (citation omitted).

Stein attempts to invoke two such circumstances here.[6] He argues that the affidavit is "so lacking in indicia of probable cause to search for computers and

[6] The good-faith exception also is inapplicable if, under *Franks*, the affidavit supporting a search warrant contained an intentional or reckless misstatement or omission that is material. See *United States* v. *Leon*, 468 U.S.

(continued…)

other electronic storage devices as to render official belief in its existence entirely unreasonable", and that the warrant is "so facially deficient—i.e., in failing to particularize the things to be seized—that the executing officers could not reasonably presume it to be valid." Br. 27. Neither argument is persuasive.

a. Even if the affidavit failed to establish probable cause to search for digital evidence on electronic devices found at Stein's home, which it did not, officers were entitled to rely on the magistrate judge's probable cause determination such that the good-faith exception to the exclusionary rule applies. The affidavit was not so "bare bones" as to render officers' reliance on it unreasonable. See, *e.g.*, *United States* v. *Ingram*, 720 F. App'x 461, 468-469 (10th Cir. 2017) (unpublished), cert. denied, 138 S. Ct. 1179 (2018).

As the Supreme Court recently reaffirmed, "[i]n the ordinary case, an officer cannot be expected to question the magistrate's probable-cause determination because [i]t is the magistrate's responsibility to determine whether the officer's allegations establish probable cause and, if so, to issue a warrant comporting in form with the requirements of the Fourth Amendment." *Messerschmidt* v. *Millender*, 565 U.S. 535, 547 (2012) (internal quotation marks and citation

---

(…continued)
897, 923 (1984) (citing *Franks*); see also *United States* v. *Gonzales*, 399 F.3d 1225, 1229 (10th Cir. 2005). As previously explained, pp. 25-28, *supra*, there is no *Franks* violation and therefore the good-faith exception can apply.

omitted; brackets in original). As a "corollary," this Court has noted that "police officers should be entitled to rely upon the probable-cause determination of a neutral magistrate when defending an attack on their good faith for either seeking or executing a warrant particularly where, with the benefit of hindsight and thoughtful reflection, reviewing judges still cannot agree on the sufficiency of the affidavit." *United States* v. *McKneely*, 6 F.3d 1447, 1454 (10th Cir. 1993) (internal quotation marks and citation omitted).

For an affidavit to be "so lacking in indicia of probable cause" to render the good-faith exception inapplicable, *Leon*, 468 U.S. at 923, the affidavit must be "*devoid* of factual support," meaning that it fails to establish even a minimal nexus between the illegal activity and the place to be searched, see *United States* v. *Campbell*, 603 F.3d 1218, 1231 (10th Cir.) (citation omitted), cert. denied, 562 U.S. 939 (2010). The "minimal nexus" required for good-faith determinations is "a lower standard" than the "substantial nexus" required for probable-cause determinations. *Barajas*, 710 F.3d at 1110-1111 (citation omitted). "Thus, [i]t is only when [an officer's] reliance was *wholly unwarranted* that good faith is absent." *McKneely*, 6 F.3d at 1454 (citation omitted; brackets in original).

Here, the affidavit does not "sink[] to such a low level" that the good-faith exception does not apply. See *United States* v. *Harris*, 735 F.3d 1187, 1193 n.2 (10th Cir. 2013). The nature of digital evidence, the specifics of this crime, and

reasonable inferences established the requisite nexus between digital evidence on electronic devices in Stein's home and the planned attack. See pp. 18-25, *supra*. As the district court aptly recognized, "it was not unreasonable for an objective officer acting in good faith to execute the search under the belief the warrant was valid." 1R.417.

b. The warrant also was sufficiently particular in setting out the authorized scope of the computer search but, even if it was not, the good-faith exception to the exclusionary rule would apply. The good-faith exception does not apply if the warrant is "so facially deficient" in terms of particularity that officers could not reasonably rely on it. *Leon*, 468 U.S. at 923.

In this inquiry, courts must review not only "the text of the warrant" but also "the circumstances of the search" to determine "whether a reasonably well trained officer would have known that the search was illegal despite the magistrate's authorization." See *United States* v. *Riccardi*, 405 F.3d 852, 863 (10th Cir.) (citations omitted), cert. denied, 546 U.S. 919 (2005). For example, in *Russian*, this Court applied the good-faith exception, in part, because the officer "confined his search to the evidence specified in the warrant application and affidavit," which "further indicat[ed] he acted in good faith and in objectively reasonable reliance on what he believed was a valid warrant." 848 F.3d at 1247; see also *United States* v. *Otero*, 563 F.3d 1127, 1135-1136 (10th Cir.) (applying the good-faith exception

with similar consideration of the circumstances of the search), cert. denied, 558 U.S. 924 (2009).

Here, the warrant is simply not "so facially deficient" that the court cannot presume good faith, and the officers' conduct confirms as much. The warrant and accompanying affidavit provided the officers with sufficient direction once they seized the electronic devices to conduct an appropriately limited search of those devices for evidence of the conspiracy, as evidenced by the conduct of the agent performing the search. Critically, the agent stopped her search when she came across evidence of child pornography in her search for image evidence of the conspiracy to use a weapon of mass destruction (2R.8), understanding this to exceed the scope of the original warrant. The seizure of electronic devices, storage media, and software for a careful off-site search for specific digital records does not offend the particularity requirement let alone the good-faith exception.

All told, this is simply not one of the "unusual cases" in which suppression will further the purposes of the exclusionary rule. See *Leon*, 468 U.S. at 918. Officers attempted to comply with the Fourth Amendment by seeking the original and subsequent warrants. They were entitled to rely on the magistrate judge's determination that probable cause existed and that the warrant was sufficiently particular. Accordingly, the good-faith exception to the exclusionary rule applies.

CONCLUSION

For the foregoing reasons, this Court should affirm the district court's denial of Stein's motion to suppress.

Respectfully submitted,

ERIC S. DREIBAND
Assistant Attorney General

s/ Alisa C. Philo
THOMAS E. CHANDLER
ERIN H. FLYNN
ALISA C. PHILO
Attorneys
Department of Justice
Civil Rights Division
Appellate Section
Ben Franklin Station
P.O. Box 14403
Washington, D.C. 20044-4403
(202) 616-2424
Alisa.Philo@usdoj.gov

STATEMENT REGARDING ORAL ARGUMENT

The United States does not oppose Stein's request for oral argument if it would be helpful to the Court in resolving this appeal.

CERTIFICATE OF COMPLIANCE

I certify, pursuant to Federal Rule of Appellate Procedure 32(g):

1. This brief complies with the type-volume limitations of Federal Rule of Appellate Procedure 32(a)(7)(B) because, excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(f), this brief contains 10,493 words according to the word processing program used to prepare the brief.

2. This brief complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5), and the type style requirements of Federal Rule of Appellate Procedure 32(a)(6), because it has been prepared in a proportionally spaced typeface using Microsoft Office Word 2016 in Times New Roman 14-point font.

s/ Alisa C. Philo
ALISA C. PHILO
Attorney

Dated: December 12, 2019

CERTIFICATE OF DIGITAL SUBMISSION

I certify that the electronic version of the foregoing BRIEF FOR THE UNITED STATES AS APPELLEE, prepared for submission via ECF, complies with the following requirements.

1. All required privacy redactions have been made under Federal Rule of Appellate Procedure 25(a)(5) and Tenth Circuit Rule 25.5;
2. With the exception of any redactions, every document submitted in digital form or scanned PDF format is an exact copy of the written document filed with the clerk; and
3. The ECF submission has been scanned for viruses with the most recent version of Windows Defender (Version1.2.3412.0) and is virus-free according to that program.

s/ Alisa C. Philo
ALISA C. PHILO
Attorney

Dated: December 12, 2019

CERTIFICATE OF SERVICE

I hereby certify that on December 12, 2019, I electronically filed the foregoing BRIEF OF THE UNITED STATES AS APPELLEE with the United States Court of Appeals for the Tenth Circuit via this Court's CM/ECF system, which will send notice to all counsel of record by electronic mail. All participants in this case are registered CM/ECF users.

I further certify that seven paper copies of the foregoing brief will be sent to the Clerk of the Court by overnight mail within two business days.

s/ Alisa C. Philo
ALISA C. PHILO
Attorney