No. 19-50231

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

NIKISHNA POLEQUAPTEWA,
Defendant-Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
DISTRICT COURT NO. SA CR 16-CR-36-CJC

GOVERNMENT'S ANSWERING BRIEF

NICOLA T. HANNA
United States Attorney

BRAM ALDEN
Assistant United States Attorney
Acting Chief, Criminal Appeals Section

VIBHAV MITTAL
Assistant United States Attorney
Deputy Chief, Santa Ana Branch Office

8000 United States Courthouse
411 West Fourth Street
Santa Ana, CA 92701
Telephone: (714) 338-3534
Email: vibhav.mittal@usdoj.gov

Attorneys for Plaintiff-Appellee
UNITED STATES OF AMERICA

TABLE OF CONTENTS

DESCRIPTION **PAGE**

TABLE OF CONTENTS (continued)

DESCRIPTION **PAGE**

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(S)**

TABLE OF AUTHORITIES (continued)

DESCRIPTION **PAGE(S)**

Federal Statutes

Federal Rules

No. 19-50231

IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA,
Plaintiff-Appellee,

v.

NIKISHNA POLEQUAPTEWA,
Defendant-Appellant.

APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE CENTRAL DISTRICT OF CALIFORNIA
DISTRICT COURT NO. SA CR 16-36-CJC

GOVERNMENT'S ANSWERING BRIEF

I

ISSUES PRESENTED

A. Whether the district court abused its discretion by denying without an evidentiary hearing defendant's motion to suppress the search of a laptop when it was uncontested in the moving papers as to the fact that defendant had previously stolen the laptop.

B. Whether it was plain error for the district court to give a sentencing-enhancement jury instruction when defendant did not object

to the instruction and it tracked the relevant language in 18 U.S.C. § 1030(c).

II

STATEMENT OF THE CASE

Nikishna Polequaptewa ("defendant") worked at Blue Stone Strategy Group ("Blue Stone"), a consulting firm, where he initially held information technology ("IT") responsibilities. He quit when Blue Stone assigned his IT responsibilities to someone else. Defendant made his resignation a criminal case by remotely "wiping" a Blue Stone computer and deleting various Blue Stone files held on its server and with third-party providers.

The evidence against defendant included his admission of guilt to one of the founders of Blue Stone, undisputed records from third-party entities such as Google, server logs and other records from Blue Stone, testimony from the new IT administrator at Blue Stone, testimony from other Blue Stone employees about defendant's statements and conduct before and after he resigned, and the contents of a laptop that was in defendant's possession at the time the wiping occurred. The jury

convicted defendant of a felony violation of 18 U.S.C. § 1030 because he caused over $5,000 worth of loss.

For the first time on appeal, defendant raises specific objections to two of the district court's rulings. First, the district court's denial of defendant's motion to suppress the contents of a laptop that was in defendant's possession at the time of the offense. The district court denied the motion without an evidentiary hearing because the facts established on the undisputed record before it that defendant had stolen the laptop and did not have a reasonable expectation of privacy in the contents of the stolen laptop. Second, defendant now objects to the sentencing-enhancement jury instruction that defined how the jury should calculate whether the loss caused by defendant was over $5,000. The parties jointly submitted this instruction to the district court to give to the jury and defendant's current objection rests on a novel interpretation 18 U.S.C. § 1030(c) that no court has adopted.

A. Jurisdiction, Timeliness, and Bail Status

The district court's jurisdiction rested on 18 U.S.C. § 3231. This Court's jurisdiction rests on 28 U.S.C. § 1291. The district court

entered judgment on July 10, 2019. (ER 1285-90.)[1] Defendant filed a timely notice of appeal on July 12, 2019. (ER 1291-97.) *See* Fed. R. App. P. 4(b)(1)(A)(i). Defendant is in custody.

B. Statement of Facts and Procedural History

1. The Offense

a. Defendant Joined Blue Stone in April 2014 and Initially Held Information Technology ("IT") and Marketing Responsibilities

In April 2014, defendant became a consultant for Blue Stone, a consulting firm that served Native American tribes. (ER 279-82, 314-15.) Until November 14, 2014, defendant's responsibilities included managing and setting up Blue Stone's IT system. (ER 590-604; GER 1-7, 128-42, 224.)

Blue Stone's IT system used multiple devices; some were local in its office in Irvine, California and many others were hosted by third-party providers. (ER 815-17, 1244-51; GER 106-113.) The following is a

[1] "CR" refers to the Clerk's Record in the district court and is followed by the docket number. "ER" refers to the Excerpts of Record filed by defendant. "AOB" refers to Appellant's Opening Brief, and "GER" refers to the Government's Excerpts of Record. These references are followed by applicable page numbers.

summary of the relevant devices and services that defendant and Blue Stone used and which were affected by defendant's crime:

- Defendant used an Apple Mac Pro, a desktop computer, in Blue Stone's Irvine office ("Blue Stone's desktop computer") to manage the IT infrastructure and store marketing materials, client project files, client relationship management ("CRM") data, and website files. (ER 816, 824, 1246.) Defendant had developed the CRM database system. (ER 592-93.)
- Blue Stone had a Synology DiskStation server in Irvine, California ("Blue Stone's server") that stored CRM data, website files, and other files. (ER 782-83, 816, 1245.)
- To market itself, Blue Stone used a service that MailChimp provided. (ER 281, 783-85.) From 2007 to 2014, Blue Stone collected information about potential clients and stored it on MailChimp's servers. (ER 281-82.) Blue Stone used MailChimp's service to send out marketing campaigns to new and old clients. (ER 679-81, 783; GER 66-76.) MailChimp also stored opt-out information so Blue Stone

knew who not to further solicit and to comply with anti-spamming laws. (ER 680-81, 783-85.)

- Blue Stone used Google Drive to store project information which included confidential tribal data and the deliverables that Blue Stone provided its clients. (ER 548-50, 821.) This included notes from interviews of clients, Blue Stone presentations, strategic plan documents, assessment documentation, and the budget and financial information of clients. (ER 548-50.)
- To backup its data, Blue Stone used Cox's backup service. (ER 818, 821.)

b. On November 14, 2014, Defendant Was Reassigned and Blue Stone Sought to Transition IT and Marketing Responsibilities to Outside Contractors

By October 2014, there were signs that defendant's workload needed to be adjusted. In an email to his supervisor, Bill Moon, defendant described the IT and marketing work he had done causing him to come into work late the next day. (GER 143-44.) In a memorandum, Moon documented how behind defendant was on his IT

and marketing work. (GER 228-29.) Blue Stone decided to transition defendant away from his IT and marketing work. (ER 605-06.)

On Friday, November 14, 2014, Blue Stone relieved defendant of his information technology and marketing responsibilities and put him on a consulting project in Florida. (ER 605-09, 812-13.) That day, defendant met with the outside contractor, Eldad Yacobi, who was going to take over the IT responsibilities. (ER 813-14). As part of that transition, Yacobi needed to get the various administrator passwords for the systems that Blue Stone used. (ER 813-14, 822.) Defendant was not happy to hear that he was no longer IT administrator and did not cooperate with Yacobi. (ER 814-15.) Defendant's lack of cooperation included not giving Yacobi all of the admin passwords and giving him incorrect passwords. (ER 815, 817-22; GER 223.)

The incomplete transition of administrator passwords to Yacobi meant that defendant retained significant abilities to control Blue Stone's IT system. For example, Yacobi became the administrator for Blue Stone's server but did not realize another Blue Stone employee, Janeen Goodman, had been given administrator privileges. (ER 819;

GER 223.)[2] Similarly, defendant retained administrator privileges over the Blue Stone desktop computer as well as Blue Stone's accounts with MailChimp and Cox. (ER 817-22; GER 223.) And while Yacobi became the administrator for the Google services that Blue Stone used, defendant still had access to Blue Stone's files with his own login. (ER 820-22, 836-37.)

On the evening of Saturday, November 15, 2014, Yacobi reset all the passwords for Blue Stone employees' email accounts; Google managed Blue Stone's email accounts. (ER 824, 1250.) On Sunday, November 16, 2014, Yacobi learned from defendant that Blue Stone employees were having issues logging into their emails, but defendant would not provide Yacobi the information necessary to assist. (ER 826-27.)

[2] Goodman was the witness's maiden name and name at the time of the crime at issue. (ER 541.) At the time of trial, her name had changed to "Janeen Gordon." Given that records from the relevant time period were in her maiden name, the brief refers to the witness as Goodman.

c. On November 18, 2014, Defendant Resigned During a Meeting with a Blue Stone Client

While on the consulting project in Florida, defendant told a co-worker that he was frustrated with Blue Stone's management. (ER 526.) On the first day of the trip (Monday, November 17, 2014), employees had trouble accessing the computer network. (*Id.*) Defendant became frustrated because he could help (with the access issues) but was not allowed to help anymore. (*Id.*) Defendant mentioned to a co-worker starting his own business similar to Blue Stone's business. (*Id.*)

On Tuesday, November 18, 2014, while in Florida, defendant and a co-worker traveled to a meeting with the Seminole Tribe, the client for the project. (ER 527.) After the dinner portion of the meeting, everyone, except defendant, went into an auditorium. (*Id.*) The purpose of the meeting was to explain the project and introduce Blue Stone employees to the Seminole Tribe. (ER 456-57, 527.) A co-worker of defendant's went to find him. (ER 527-28.) Defendant returned to the meeting. (ER 528.) First, Blue Stone employees described the project. (ER 457.) Then, Blue Stone employees introduced themselves. (*Id.*) When it came to defendant's turn to introduce himself, he stated

his name, stated that this was his last day and he would not be on the project, and that Blue Stone would continue to do a good job. (ER 458, 528.) Defendant's supervisor, Moon, in his 20 years in consulting, had never seen a consultant resign in front of a client. (ER 458-59.) Blue Stone employees were confused and surprised with defendant's abrupt and public resignation. (ER 459, 528-29.)

Moon later told John Mooers, a Blue Stone founder and the CEO, about defendant's resignation. (ER 460-61, 587, 682.) Mooers informed Moon that Blue Stone files were being deleted. (ER 461.) After his resignation, defendant was unresponsive to Moon's and others' phone calls. (ER 461-63.) Believing defendant had a Blue Stone laptop with him, Moon went to defendant's hotel room. (ER 463-65.) Because defendant was not responding and the door to his room was latched, Moon called the local sheriff's department. (ER 465-69.) With the assistance of the local sheriff's department, Moon obtained the laptop that was in defendant's hotel room. (ER 469-70.) Moon later shipped the laptop to Blue Stone's office in Irvine, California. (ER 470-71.) (The government refers to this laptop as the "UCI laptop," as defendant's

former employer, University of California, Irvine "UCI," was the lawful owner of it.)

Back in California, after learning of defendant's resignation, Mooers informed Yacobi around 5:30 p.m. on Tuesday, November 18, 2014, that defendant had resigned. (ER 827.)[3] Yacobi attempted to remove defendant's access to Blue Stone's system because Mooers said that he saw files being deleted from the server. (ER 828.) Server records and Yacobi's testimony established that Yacobi logged into the server at 5:17 p.m. and removed defendant's access later that evening. (ER 838-40; GER 209-10.)

d. Following his Resignation, Defendant Wiped Blue Stone's Desktop Computer

According to Apple records, on Tuesday, November 18, 2014, at 9:50 p.m., defendant executed an erase command on Blue Stone's desktop computer in Irvine, California, using Apple's Find My iPhone application and his personal Apple login (nikishna@yahoo.com) and from an IP address, 50.205.50.98. (GER 10, 114-27.) A Comcast record

[3] While some of the events took place in Florida and other events in California, for simplicity, this brief uses Pacific Standard Time throughout the brief.

showed that the IP address was assigned to defendant's hotel in Florida. (GER 9.) On Wednesday, November 19, 2014, Yacobi saw an erase command execute on Blue Stone's desktop computer. (ER 845-46.) Apple records corroborated Yacobi's testimony and showed that the wipe command was initiated on Wednesday, November 19, 2014, at 3:55 p.m. (GER 10.) The wipe command turned the device into a "brick" because not much could be done with it. (ER 845-46.) Based on a forensic examination of Blue Stone's desktop computer, the FBI found that the file system for Blue Stone's desktop computer was unrecognizable and it had no file structure. (ER 563, 568-70; GER 81-82.) Blue Stone's desktop computer would no longer boot, and a user would get an error message saying, "operating system not found," if the computer was turned on. (ER 570.) The FBI also found that, following the wipe command, Blue Stone's desktop computer had various Blue Stone-related documents in unallocated space, a portion of the computer's hard drive that could only be accessed with special computer forensic tools. (GER 8, 83-94; ER 570-71, 986-90.) The fact that Blue Stone's files were in unallocated space supported the inference that,

prior to the wipe command's execution, the desktop computer held Blue Stone's files in an accessible format.

e. Around the Time of His Resignation, Defendant Also Deleted Various Blue Stone Files, As Part of a Related Course of Conduct

Testimony at the re-trial[4], records from third-party providers, and logs from Blue Stone's server showed a related course of conduct where defendant deleted Blue Stone files across the firm's IT infrastructure on Monday, November 17, 2014, and Tuesday, November 18, 2014 without authorization. This included files held by Google, MailChimp, and Cox as well as files held on Blue Stone's server.

i. Defendant Deleted Files Held by Google

On Tuesday, November 18, 2014, Blue Stone employee Janeen Goodman attempted to get project information from defendant for a presentation she was working on. (ER 543-44.) But, defendant seemed unwilling to give it to Goodman. (*Id.)* Goodman learned that defendant had resigned at 5:15 p.m. (*Id.*) After learning of the resignation,

[4] Defendant was tried twice in 2018 as the first trial ended in a mistrial after the jury deadlocked 10-2 in favor of conviction. (CR 82; CR 129 at 2.) The trial testimony summarized in this brief is from the re-trial that took place in November 2018, where defendant was convicted.

Goodman saw defendant deleting items from Blue Stone's Google Drive. (ER 545-48; GER 77-80.) Yacobi was able to restore the deleted items and prevent defendant from deleting other Google Drive files. (ER 546.) Records from Blue Stone and Google also showed defendant deleting its files on Google Drive on Monday, November 17, 2014 from Florida. (GER 47-57, 145-208; ER 835-37.)

ii. Defendant Deleted Files Held by MailChimp and Attempted to Prevent Blue Stone from Accessing its Account

Defendant also deleted the data that Blue Stone stored with MailChimp. (ER 794-95, 840-41.) Defendant's actions with the MailChimp accounts were captured in logs that MailChimp provided the FBI. (GER 33-46.) For example, the MailChimp records showed that Blue Stone contact lists were exported on November 17, 2014, and Blue Stone contact lists and marketing campaigns were deleted on November 18, 2014. (GER 33-40.) The jury could infer that it was defendant who did these exports and deletions because the IP addresses came back to defendant's hotel in Florida and the IP address for the Seminole Tribe. (GER 9, 52-54.) The hotel IP address was the same IP

address defendant used to wipe Blue Stone's desktop computer. (GER 9-10.)

In addition to the exports and deletions, MailChimp records showed that defendant also blocked Blue Stone's access to its files when he revoked Goodman's admin access to Blue Stone's MailChimp account. (GER 222; ER 400-03.) Goodman had not authorized defendant to revoke her admin access to the MailChimp account. (ER 543.)

iii. Defendant Deleted Files Held by Cox

An email with Robert Mooers (the contractor who took over marketing responsibilities) showed that defendant still had access to Blue Stone's Cox account after the Friday, November 14, 2014 transition meeting. (GER 95-102.) Records obtained from Cox and its subcontractor, Mozy, showed that defendant deleted Blue Stone files backed up with Cox on Tuesday, November 18, 2014, and changed the login for this service to a personal email address, nikishna@gmail.com. (ER 995-96; GER 230-33.) Yacobi's testimony corroborated the records where Yacobi testified that defendant changed the login for Blue Stone's Cox account to his personal email address. (ER 841.)

After defendant deleted the backups on November 18, 2014, Blue Stone was unable to get the backups from Cox restored. (ER 841-42, 896-97.) Yacobi's testimony about attempting to restore the Cox backup was corroborated by records the FBI obtained from Cox and Mozy. (ER 993-96; GER 102-05, 225-27, 230-33.)

iv. Defendant Deleted Files Held on Blue Stone's server, including Blue Stone's website

Robert Mooers saw Blue Stone's website on Friday, November 14, 2014. (ER 788-90.) But, by the evening of Tuesday, November 18, 2014, Mooers saw that the website was no longer accessible. (ER 791.) Yacobi also learned Blue Stone's website files stored on its server had been deleted. (ER 828-29.) According to the server's logs, on November 18, 2014, at 11:58 a.m., defendant logged into the server using his credential and accessed the folder that stored the website files; Yacobi later found the folder to be empty. (ER 833; GER 58.) Because the website files were not able to be restored, Robert Mooers worked to recreate the website from an old version which did not include months of development. (ER 791-94.)

In addition, records showed that Bill Moon's folder on the server was accessed on November 18, 2014, at 4:12 a.m.; that folder was also

later found to be empty. (ER 471, 833-34; GER 59-60.) Testimony from Moon showed that he did not access the folder at that time. (ER 471.) The jury could infer that defendant deleted Moon's folder using Moon's login, given defendant's knowledge of Blue Stone's IT system.

f. Defendant Attempted to Create a "Backdoor" to Blue Stone's Server

As part of his investigation into defendant's deletions, Yacobi pulled log files from Blue Stone's server. (ER 832-35, 837-40; GER 58-63, 209-10.) Yacobi discovered how defendant had attempted to create a backdoor to the server. (ER 837-38.) Just before the meeting on Friday, November 14, 2014, a log showed that defendant had made Goodman an administrator of Blue Stone's server. (ER 837-38; GER 209-10.) Goodman was not aware that her account was given administrator privileges. (ER 542.)

On Saturday, November 15, 2014, when Yacobi was resetting passwords, Yacobi found Goodman was an "admin," and disabled her admin access. (ER 838-39; GER 210.) Server logs showed that on Monday, November 17, 2014, defendant logged in as "Goodman" from Florida, where he was on assignment with the Seminole Tribe. (ER 834; GER 52-53, 61.) Goodman was in California at the time and never

authorized anyone in Florida to use her login. (ER 542-43.) Just before the Goodman login, records showed that an admin login failed and defendant had logged in. (*Id.*) The jury could infer that defendant learned on Monday, November 17, 2014, that he no longer had admin access to Blue Stone's server. His backdoor via Goodman's login had been closed, adding to his frustration of over the reassignment.

g. Defendant Admitted to Deleting Blue Stone Files

On Wednesday, November 19, 2014, defendant returned to the Blue Stone office with an aggressive demeanor. (ER 296-306, 1238-41.) Defendant had returned to get his personal belongings. (ER 1238.) After defendant said, "let me get my stuff," a Blue Stone founder, Jamie Fullmer, said Blue Stone wanted to make sure that it got all of its "stuff" back, referring to all the items that had been deleted the day before. (ER 304, 1241.) Defendant responded, "What stuff? I deleted it. That's the point." (ER 1241.) Defendant's admission was recorded in a video taken using a phone. (ER 1238-41.)

After the recording ended, Fullmer continued to talk to defendant. Fullmer was upset with defendant's response. (ER 305.) Fullmer asked defendant why he had done it. (*Id.*) With a remorseless, matter of fact

demeanor and as if defendant felt justified in doing the deletions, defendant said to Fullmer that he (defendant) had done it and it was done. (ER 305-06.)

h. Blue Stone's Loss from Defendant's Deletions

The government presented evidence at trial to establish that the amount of Blue Stone's loss from defendant's criminal conduct was at least $5,000. The amount of loss was an issue for the jury because the relevant felony provision in 18 U.S.C. § 1030(c) depended on the amount of loss. The following is a summary of the "loss" proven at trial:

- John Mooers and other Blue Stone employees spent hours responding to defendant's offense, including assessing the damage done and trying to restore systems. (ER 322-25, 626-32, 678, 1242-43.) This cost Blue Stone approximately $48,550.60. (*Id.*)
- Jamie Fullmer flew to the Irvine, California office on November 19, 2014, and incurred expenses in responding to the offense. (GER 211-21; ER 297-98, 306.) Those flights and other expenses totaled $629.43. (*Id.*)

- Yacobi, the IT consultant, charged $2,300 for his company's efforts to respond to defendant's offense, including efforts to restore backups. (GER 64; ER 847-49.)
- Robert Mooers, the marketing consultant, charged Blue Stone $1,825 to rebuild its website after defendant deleted it. (ER 795-97; GER 65.)

i. Evidence Admitted at Re-trial from the Laptop Subject to Motion Suppress

During the re-trial, the government introduced evidence from the laptop that Moon obtained in Florida, UCI laptop. This evidence provided corroboration for the other evidence of defendant's guilt summarized earlier.[5] The following are examples of what the laptop evidence showed:

[5] Following the mistrial, the government searched the laptop again pursuant to UCI's consent, as the district court had already ruled that defendant had stolen the laptop from UCI. (ER 926-27, 972-73, 977.) However, the items introduced at trial from that consent search are not summarized here, as that consent search was not contested below or raised in the opening brief. Regardless, those additional items would not have a bearing on the harmless error argument made in this brief, which relies on the Court finding that the laptop evidence was merely cumulative to the evidence obtained from sources other than the laptop.

- Defendant accessed Goodman's password on November 17, 2014, which was consistent with the log files that Yacobi had introduced showing defendant attempting to access Blue Stone's server via Goodman's login (GER 13-14);
- Emails from the laptop showed defendant's frustration at being re-assigned away from IT and marketing (GER 23-30);
- An email from MailChimp on November 17, 2014, showed that defendant was exporting Blue Stone lists and advised that exports are not available after lists were deleted (GER 15);
- Defendant's web searches were consistent with the charged acts of deletion (GER 11-12); and
- Evidence of defendant deleting Blue Stone's website and accessing third-party providers were also on the laptop (GER 16-22, 31-32).

2. First Superseding Indictment

Following a mistrial, defendant was charged in the first superseding indictment with a violation of § 1030(a)(5)(A) for sending the "wipe" command to Blue Stone's desktop computer. (ER 237-38.)

As part of a "related course of conduct", defendant was also charged with the deletions he executed on Blue Stone's internal server and other remote servers operated by Google, Bluehost, MailChimp, and Cox. (ER 236, 237, 239.) The loss from the "wipe" command and the "related course of conduct" was alleged as part of the sentencing enhancement stated in 18 U.S.C. §§ 1030(c)(4)(B)(i), (c)(4)(A)(i)(I), because the loss was greater than $5,000. (ER 238-39.)

3. Motion to Suppress

a. Procedural History of Motion to Suppress

The FBI opened an investigation into defendant's conduct after November 20, 2014; John Mooers, the Bluestone CEO, had reported defendant's actions to the FBI on a public access line on November 20, 2014. (ER 122, 123, 145.) The FBI then sought and obtained a search warrant issued by the Honorable Jay C. Gandhi, United States Magistrate Judge. (ER 50-102.) The FBI searched the laptop pursuant to the terms of the warrant and some of the digital data on the laptop was admitted into evidence at the second trial, as discussed above.

Prior to the first trial, defendant moved to suppress the contents of the UCI laptop that the government obtained through the FBI's search.

The record before the district court on the motion to suppress consisted of the evidence and argument contained in four pleadings filed by the parties. First, there was defendant's motion to suppress, which was factually supported with a declaration from defendant, the search warrant application including the case agent's affidavit, and the search warrant. (ER 30-108.) Defendant essentially raised two objections to the search of the laptop: (1) Blue Stone obtained the UCI laptop from defendant in the Florida hotel room through a warrantless search for which no exception to the warrant requirement applied; and (2) the was not sufficient probable cause for the warrant. (ER 32.) Defendant's only attack on the probable cause in the warrant was that there was a break in the chain of custody because Blue Stone had possession of the laptop for most of the time from when defendant possessed it to the time that the FBI conducted the search. (ER 45-46.) Defendant's declaration exclusively addressed the events in the hotel room in Florida on November 18, 2014. (ER 103-06.)

The government filed an opposition to defendant's motion in which it argued that events at the Florida hotel room were irrelevant to the validity of the warrant, exceptions to the warrant requirement applied to the Florida events because defendant's account of the evening was inaccurate, and the supporting affidavit for the warrant contained sufficient probable cause for the search of the UCI laptop. (ER 115-37.) More specifically, the government argued: (1) defendant lacked a reasonable expectation of privacy in the laptop because he stole it from his former employer, UCI (ER 123-27); (2) the laptop was lawfully seized in Florida because there was consent and local law enforcement thought defendant and his family needed emergency aid (ER 128-31); (3) any illegal action by Blue Stone employees with respect to obtaining the laptop had no bearing on the validity of the federal warrant because those employees were not government agents (ER 131-32); (4) the probable cause for the search warrant was not derived from the events in Florida and the independent source doctrine, inevitable discovery exception, and good faith exception all applied (ER 132-36); and (5) there was sufficient probable cause for the warrant (ER 136-37). Two of the three government's declarations concerned defendant's theft of the

laptop from UCI and the third was from a Florida deputy sheriff who contradicted key parts of defendant's declaration concerning the events in the hotel room. (ER 146-90.) In addition to the three declarations, the government attached three exhibits to its opposition: the consent UCI gave to search the laptop in June 2015 (ER 138-40), Blue Stone's loss estimate (ER 141-43), and a portion of a FBI document showing that Mooers had called the FBI to report defendant's criminal conduct on November 20, 2014 (ER 144-45).

Defendant filed a reply that did not contain any more case cites, declarations, or exhibits. (ER 191-96.) It did not address the government's arguments concerning independent source, inevitable discovery, good faith, or the absence of involvement by government agents in the events at the Florida hotel room. It did not dispute the accuracy of any of the facts asserted in the two declarations of the UCI employees in the government's opposition. It did not dispute that the FBI's investigation began after Mooers called the FBI on November 20, 2014. It did contain the argument that during the events at the Florida hotel room no one asserted that the laptop was owned by UCI and that

defendant had consistently argued that night and in subsequent civil litigation that the laptop did not belong to Blue Stone. (ER 193.)

After defendant filed his reply, the government filed an *ex parte* application for an order precluding the need for an appearance by the government's three declarants; *i.e.*, eliminating the need for an evidentiary hearing. (ER 197-200.) The basis for this request was defendant's failure to dispute the facts that established that he had stolen the UCI laptop. (ER 200.) While defendant opposed the government's application and wanted to cross-examine its three witnesses, defendant did not contest any of the specific facts in the declarations by the two UCI declarants or make an additional proffer regarding this topic. (Id.)

The parties therefore did not dispute the following facts:

- On November 18, 2014, James Moon, defendant's supervisor at Blue Stone, went to defendant's hotel room in Florida after defendant had resigned. (*Compare* ER 103-06, 192-94 with ER 50-102, 184-90.)
- That night, Moon called the local sheriff's office. (*Id.*)
- Eventually, Moon obtained the UCI laptop from defendant with the assistance of the local sheriff's office. (*Id.*)

- Blue Stone held the UCI laptop from November 18, 2014, until December 9, 2014, when the Irvine Police Department ("IPD") took custody of the UCI laptop. (ER 60-61, 65, 70-71.)

- The FBI did not open its investigation until at least November 20, 2014 when Blue Stone contacted the FBI. (ER 145.)

- The FBI took investigative steps between December 1, 2014, and December 10, 2014, including interviews of witnesses. (ER 53-81.)

- On December 11, 2014, the FBI obtained a search warrant to search the UCI laptop, which was in the custody of the IPD at that time, for evidence of violations of 18 U.S.C. §§ 1030(a)(1), (a)(5). (ER 50-102.)

The parties did contest the lawfulness of the entry by deputy sheriffs into defendant's hotel room in Florida and the circumstances by which Moon came into possession of the UCI laptop. (*Compare* ER 103-06, 192-94 with ER 50-102, 184-90.)

b. The undisputed facts regarding the stolen UCI laptop and the district court's denial of defendant's motion to suppress without an evidentiary hearing.

The following facts concerning UCI's ownership of the laptop and defendant's theft were in the record before the district court when it

determined that it did not need an evidentiary hearing or cross-examination of the government's witnesses to rule on defendant's motion to suppress.

Before joining Blue Stone, defendant worked for UCI. (ER 146.) In that job, defendant purchased two laptops; the second laptop is the UCI laptop and was the laptop that Moon obtained in Florida. (ER 146, 176.) Both laptops were purchased using UCI funds and were to be used for a National Science Foundation-funded project. (ER 176-77.) According to UCI policy, "[t]he Board of Regents, with few exceptions, [held] title to all property acquired with University funds – including funds from extramural sources - contracts, grants, gifts, etc." (ER 153.)

On March 3, 2014, UCI terminated defendant, and he was required to "return all UC equipment, including . . . laptops . . . in [his] possession." (ER 157.) In August 2014, defendant's wife returned the first laptop. (ER 172.) In January 2015, UCI sent defendant and his wife letters reminding them that the UCI laptop "must be returned." (ER 171-75.) Without a response, UCI turned to its police department for assistance to recover the UCI laptop. (ER 147.) UCI maintained

that defendant stole the UCI laptop when he failed to return it following his termination. (ER 147.)

Based on the record before it, the district court ruled that an evidentiary hearing was not necessary and then denied defendant's motion to suppress on the ground that defendant had not established a reasonable expectation of privacy in the UCI laptop. (ER 1-8.) The district court found: "Defendant does not contest that UCI is the rightful owner of the July laptop or that he failed to return UCI's property despite UCI's efforts to obtain it from him." (ER 8.) Defendant did not have "standing" (in the Fourth Amendment meaning of that term) to suppress the contents of the laptop because a defendant cannot have a reasonable expectation of privacy in stolen property. (ER 6.)

4. Jury Instructions

The district court instructed the jury on the three elements for a violation of § 1030(a)(5)(A). (ER 1225.) As to the sentencing enhancement for loss, the district court followed the jointly submitted jury instruction and instructed as follows:

> If you find the defendant guilty of the charge in Count One of the first superseding indictment, you are then to determine whether the government proved beyond a reasonable doubt that as a result of such conduct and a

> related course of conduct affecting one or more other computers used in or affecting interstate or foreign commerce or communication, the defendant caused loss to Blue Stone Strategy Group during any one-year period of an aggregate value of $5,000 or more.

(ER 1229.) The district court provided a verdict form, without any relevant objection, requiring the jury to unanimously find that the government had proven the loss was $5,000 or greater. (ER 1257.)

5. Conviction and Sentencing

In the re-trial, the jury found defendant guilty of the charged conduct, including the sentencing enhancement. (ER 1256-57.) Defendant was sentenced to 27 months of imprisonment. (ER 1285-90.)

III

SUMMARY OF ARGUMENT

Defendant failed to establish his reasonable expectation of privacy in the laptop when he failed to contest in the district court that he had stolen it from UCI. That failure disposed of all the issues in the motion to suppress. Accordingly, the district court did not abuse its discretion in denying the motion to suppress without an evidentiary hearing. Defendant's new arguments on appeal should not be considered by this Court because there is not good cause for presenting them now. They

are also wrong on the merits. Similarly, the government's arguments for application of the independent-source doctrine was sufficiently factually supported, so the Court should affirm on that ground. Regardless, any error was harmless, given that the evidence from the laptop was merely cumulative of defendant's guilt. Finally, if there was error, judicial economy favors only a limited remand for the district court to consider the remaining arguments presented in defendant's previously filed motion to suppress, not for a new trial.

The jury instruction as to the § 1030 sentencing enhancement was not plainly erroneous and does not warrant the reversal of the sentencing enhancement.

Defendant's conviction should be affirmed.

IV

ARGUMENT

A. The District Court Did Not Abuse Its Discretion or Err in Denying the Motion to Suppress Without an Evidentiary Hearing

1. Standard of review

Different levels of review apply to the denial of a motion to suppress depending on the issues raised by the denial. The general

standard of review for reviewing the denial of a motion to suppress is *de novo*. *United States v. Magdrila*, 962 F.3d 1152, 1156 (9th Cir. 2020). The district court's underlying factual findings are reviewed for clear error. *United States v. Barnes*, 895 F.3d 1194, 1199 (9th Cir. 2018). Where the district court does not make a finding on a precise factual issue relevant to the Fourth Amendment analysis, this court will "'uphold a trial court's denial of a motion to suppress if there was a reasonable view to support it.'" *Magdrila,* 962 F.3d at 1156 (quoting *United States v. Gooch*, 506 F.3d 1156, 1158 (9th Cir. 2007)).

The Ninth Circuit uses the "good cause" standard under Federal Rule of Criminal Procedure 12(c)(3) to determine whether new argument and evidence on a motion to suppress can be raised for the first time on appeal (although not all courts agree that this is the correct standard). *United States v. Guerrero*, 921 F.3d 895, 897-98 (9th Cir. 2019).

The Court reviews for an abuse of discretion a district court's decision whether to conduct an evidentiary hearing on a motion to suppress. *United States v. Howell*, 231 F.3d 615, 620 (9th Cir. 2000) (citations omitted). An evidentiary hearing on a motion to suppress

must be held only when the moving papers allege facts with sufficient definiteness, clarity, and specificity to enable the trial court to conclude that contested issues of fact exist. *Id.*

2. Defendant Failed to Establish a Reasonable Expectation of Privacy in the UCI Laptop Before the District Court

Defendant could challenge the legality of the search on Fourth Amendment grounds only if he had a "legitimate expectation of privacy" in the laptop searched. *United States v. Zermeno*, 66 F.3d 1058, 1061 (9th Cir. 1995) (citation omitted). Defendant had the burden of establishing his legitimate expectation of privacy in the laptop that the FBI searched. *Id.* (citation omitted). The government submitted evidence that UCI was the proper owner and possessor of the laptop. As the government discusses below, defendant failed to argue in the district court that the UCI declarations and exhibits were inaccurate. Accordingly, the district court did not err, let alone commit clear error, when it found that UCI was the owner of the laptop, that defendant had stolen the laptop, and he did not have a legitimate possessory interest in the laptop. (ER 7.)

These findings are fatal to defendant's motion. The district court properly denied defendant's motion to suppress because defendant failed to establish that he had a reasonable expectation of privacy in the contents of the laptop. *See United States v. Wong*, 334 F.3d 831, 839 (9th Cir. 2003); *United States v. Caymen*, 404 F.3d 1196, 1200–01 (9th Cir. 2005).

Defendant points to facts that show his subjective belief in his expectation of privacy in the laptop. (AOB at 49-52.) Whether or not defendant believed the laptop was his, "[t]he Fourth Amendment does not protect a defendant from a warrantless search of property that he stole, because regardless of whether he expects to maintain privacy in the contents of the stolen property, such an expectation is not one that 'society is prepared to accept as reasonable.'" *Caymen*, 404 F.3d at 1200 (quoting *Smith v. Maryland*, 442 U.S. 735, 740 (1979)).

3. The District Court Did Not Abuse its Discretion or Otherwise Err In Not Holding an Evidentiary Hearing

Defendant argues that he was entitled to evidentiary hearing because the government put forth declarations from UCI employees. (AOB at 52-57.) As defendant himself admits, the contours of defendants' constitutional rights to cross-examine government

declarants at a suppression hearing are not fully established. (AOB at 54 (citing *United States v. Campbell*, 743 F.3d 802, 808-09 (11th Cir. 2014)). Despite this uncertainty, the government agrees that, where resolution of contested issues of fact could result in a grant of the motion to suppress, it would be error or an abuse of discretion for a district court not to allow cross-examination of the government's declarants at an evidentiary hearing. *See United States v. Mejia*, 69 F.3d 309, 318 (9th Cir. 1995) (citation omitted).

Nonetheless, defendant does not cite any cases that state that defendants cannot waive, forfeit, or otherwise lose any rights they may have to cross-examine witnesses through their considered, tactical decisions not to raise some kind of question about the accuracy of the government's evidence. Thus, courts—including this Court—have ruled before and after *Crawford v. Washington,* 541 U.S. 36 (2004) that the district court must hold an evidentiary hearing on a motion to suppress if the resolution of the contested issue of fact could result in relief being granted.

This Court also has been clear that, for motions to suppress, "[e]videntiary hearings need be held only when the moving papers

allege facts with sufficient definiteness, clarity, and specificity to enable the trial court to conclude that relief must be granted if the facts alleged are proved." *United States v. Carrion,* 463 F.2d 704, 706 (9th Cir. 1972); *see also United States v. Walczak*, 783 F.2d 852, 857 (9th Cir. 1986) ("[T]he record contains no controverted fact sufficient to require an evidentiary hearing, and the district court properly denied the motion for an evidentiary hearing."); *Mejia*, 69 F.3d at 318 ("Our cases *require* the district court to conduct an evidentiary hearing when the moving papers filed in connection with a pre-trial suppression motion show that there are contested issues of fact relating to the lawfulness of a search." (emphasis original)); *Howell,* 231 F.3d at 620 ("An evidentiary hearing on a motion to suppress need be held only when the moving papers allege facts with sufficient definiteness, clarity, and specificity to enable the trial court to conclude that contested issues of fact exist."); *United States v. Kyle*, 565 F. App'x 672, 673 (9th Cir. 2014) (citing *Howell* and stating, "Although Kyle requested an evidentiary hearing, he never questioned or objected to the accuracy of the government's version at all, much less with the 'sufficient definiteness, clarity, and specificity to enable the trial court to conclude that

contested issues of fact exist.'"); *United States v. Nuñez,* 753 F. Appx. 450, 451, (9th Cir. 2019) (citing *Howell* and stating, "Because Nuñez failed to identify a factual dispute as to the canine's reliability in his moving papers, the district court did not abuse its discretion in denying him an evidentiary hearing on the reliability of the canine's alert.").

The district court did not abuse its discretion or otherwise err in declining to hold an evidentiary hearing on the issue of defendant's theft of the laptop. Defendant did not even come close to alleging facts with "sufficient definiteness, clarity, and specificity" that disputed the government's showing on this point. If defendant did not establish a reasonable expectation of privacy in the laptop, then the analysis on the motion was done. And, as one of the UCI declarants flatly stated: "UCI has viewed since July 9, 2012, and continues to view the laptop as its property. Mr. Polequaptewa has not returned the laptop to UCI since he was terminated on March 3, 2014. UCI does not believe that Mr. Polequaptewa has any right to the laptop and considers it to be stolen property." (ER 147.)

As the district court found, defendant did not address in his motion his ownership interest in the UCI laptop. (ER 8.) Nor did he

contest in his reply any of the UCI declarations and exhibits that were in the government's opposition. Rather, defendant in his reply re-visited his arguments regarding the events at the Florida hotel room and noted that he had consistently argued that *Blue Stone* did not own the laptop. (ER 191-94.) The government put defendant on explicit notice that his showing on his reasonable expectation of privacy was insufficient when it requested the district court to excuse the government's witnesses from appearing at an evidentiary hearing. (ER 197-202.) Yet even then, defendant merely raised a general objection to the government's request rather than identifying potential inaccuracies in the government's showing or specific need for cross-examination. (ER 200.)

Defendant's consistent failure in the district court to confront, question, or dispute the accuracy of the UCI evidence certainly did not raise any definite, clear, or specific objection that needed to be resolved in an evidentiary hearing. In sum, there was no contested issue of fact presented below that defendant had stolen the laptop from UCI following his termination. Without demonstrating a reasonable expectation of privacy in the UCI laptop, defendant's motion to suppress

could not succeed. Accordingly, the district court did not abuse its discretion or otherwise err in ruling on the motion to suppress without holding an evidentiary hearing.

4. Defendant's New Arguments in his Opening Brief are Too Late (and Too Little)

For the first time on appeal, defendant argues that he still has a legitimate expectation of privacy in his laptop even if it was stolen because Moon took it from his Florida hotel room, a place in which he did have a legitimate expectation of privacy. (AOB 43-48.) Also for the first time on appeal, defendant now argues that the government's evidence of UCI's interest over the laptop was insufficient. (AOB at 48-53, 55-56.) Defendant supports this argument with testimony from his wife at his trial. (AOB 56.)

i. There is no good cause for defendant waiting for his appeal to advance the new arguments.

Defendant's belated efforts to redress the flaws in his district-court arguments are improper and lacking on the merits. Defendants ordinarily may not raise new grounds for suppression on appeal. *See United States v. Keesee*, 358 F.3d 1217, 1220 (9th Cir. 2004). A defendant must show "good cause" under Federal Rule of Criminal

Procedure 12(c) to make new arguments on appeal. *Guerrero*, 921 F.3d at 897-98. Without good cause, a defendant therefore may not: "(1) assert facts contradicting the facts he or she asserted before the district court; (2) rely on facts that were not raised before or relied upon by the district court; or (3) make a new legal argument in support of suppression, unless the issue does not affect or rely on the factual record developed by the parties." *Magdrila,* 962 F.3d at 1156-57 (citations omitted).

Defendant in his opening brief neither mentions nor meets the "good cause" standard. His new arguments all could have been made to the district court. In regard to UCI's ownership of the laptop, defendant now suggests the policy that governed UCI's interest in the laptop was inadequately cited by the government (ER 153), argues the March 2014 letter demanding return of UCI property was too "general," argues that the January 2015 letter sent specifically for the laptop was too late in time because the FBI had already seized the laptop by that time, and contends (without any factual support) that UCI's view that the laptop was "stolen property" was "manufactured at the government's behest." (AOB at 50-51.)

Defendant also cites to his wife's trial testimony, claiming that UCI signed off on a list of items he returned and the list did not include the laptop. (AOB at 55-56 (citing ER 1116).) He presents this testimony in support of an argument that UCI had abandoned the laptop or had not done enough to take ownership of the laptop. (AOB at 16-22, 55-56.)

Had defendant contested the sufficiency of the UCI declarants in his reply brief or when the government applied for a ruling without an evidentiary hearing, the government could have supplemented the record. However, no such position was taken below and there is no good cause for these arguments to be advanced now. Similarly, defendant does not provide good cause for why he could not have submitted a declaration from his *wife* to the district court at the time he filed his suppression motion. This new argument and evidence therefore now is improper and cannot be used to undermine the district court's ruling.[6]

[6] Moreover, even if the Court did consider testimony from the re-trial, these "facts" do not show that defendant had a reasonable expectation of privacy in the laptop. The evidence showed that UCI owned the laptop, and UCI repeatedly asked for the return of the laptop, ultimately turning to the police. (ER 146-83.) Defendant's wife's testimony was not corroborated with the signed list or any

For similar reasons, defendant has not shown good cause for waiting for his appeal to argue that his expectation of privacy in his hotel room can support his motion to suppress the search that took place pursuant to the warrant for the laptop. (AOB at 45-48.) To reach this conclusion, defendant attempts to distinguish *Caymen* and *Wong*. (AOB at 46-47.) But obviously these are distinctions that could have been presented to the district court. Among other new case citations, defendant cites to case law involving the illegal stops of cars where the defendant had no reasonable expectation of privacy in the car. (AOB at 47-48.) This line of authority was not cited to the district court. Defendant has not shown good cause for his delay so this argument is improper now.

ii. The new argument regarding defendant's expectation of privacy in the Florida hotel room also fails on the merits.

Even if this Court were to consider defendant's belated attempts to distinguish *Caymen* and *Wong,* this new argument fails. Contrary to

---

evidence about when the list was signed. Even with this new evidence, defendant did not establish a reasonable expectation of privacy in the UCI laptop.

defendant's suggestion, both decisions rejected "fruit of the poisonous tree" arguments quite similar to the one now advanced by defendant. In *Wong*, the defendant asserted that the warrant at issue (a February 2, 2000 warrant) was the fruit of the poisonous tree because of deficiencies in prior warrants (warrants from January 26 and 28, 2000). The Court rejected that argument for two reasons. First, it found that the prior warrants were valid. Second, and more importantly here, it alternatively found that the defendant could not challenge the search of the laptop because it belonged to his former employer. *Wong*, 334 F.3d at 839. That alternative ground is precisely the fact pattern here. Defendant seems to read that holding out as *dicta* even though this Court in *Wong* used the defendant's failure to establish a reasonable expectation of privacy in the laptop as one basis to affirm the denial of the motion to suppress.

In *Caymen,* the defendant committed credit card fraud and purchased a laptop using another's credit card number. 404 F.3d at 1197. As part of that investigation, police seized the fraudulently obtained laptop pursuant to a warrant. *Id.* at 1198. Then, the police searched it based on the consent of the business that sold the laptop.

Id. While looking for evidence of credit card fraud, the police found evidence of child pornography. *Id.* Based on that initial search, the police obtained a warrant to search the laptop and other devices for child pornography. *Id.*

The defendant in *Caymen* contested the police's initial search of the laptop, arguing that the subsequent search pursuant to a warrant was the "fruit of the poisonous tree." *Id.* at 1198-99. There, the district court (like here) found that defendant lacked a reasonable expectation of privacy and denied the motion. *Id.* at 1200. This Court affirmed the district court's ruling because defendant lacked a reasonable expectation of privacy in the laptop and the business (the rightful owner) had consented to the search. *Id.* at 1199-1201.

Here, the FBI also conducted the search of the laptop pursuant to a warrant, and defendant also is arguing that the warrant is derived from illegal evidence (namely, the entry into defendant's Florida hotel room and seizure of the UCI laptop in Florida). But unlike many of the cases he now cites (AOB at 47-48), defendant does not establish that the probable cause showing in the warrant actually relies on the events in Florida. The probable cause for the warrant here was based on the

investigation that the FBI did between December 1, 2014 and December 10, 2014, as to defendant's deletions (ER 53-81). In the affidavit submitted in the application, there were only passing references to the events at the hotel room, and defendant does not dispute the basic timeline of events as they are described in the affidavit. (ER 57, 59-64, 192-93 (defendant in his reply brief acknowledging that "neither Defendant nor the Government dispute the fact that Mr. Moon of Bluestone was physically present when deputies arrived at Defendant's hotel room and that the laptop was handed over to Mr. Moon at the hotel").) The probable cause in the application for the warrant does not rest on the events in Florida and is therefore not derived from those events. At most, the events in Florida were described in the affidavit to explain why the UCI laptop was in IPD's custody at the time of the application.

Second, this case is unlike the traffic-stop cases cited by defendant in which the same law enforcement agency illegally stops a car and then later searches the car as part of a coordinated course of conduct. *See United States v. Gorman*, 859 F.3d 706 (9th Cir. 2017). Here, it is undisputed that the FBI searched a laptop after receiving a complaint

from the victim company; by the time that the FBI obtained the warrant, another agency (IPD) had taken custody of the UCI laptop from Blue Stone. Defendant never contested that the FBI first learned of the crime when Blue Stone submitted a complaint on November 20, 2014 (ER 122-23, 145). Even defendant does not suggest that the FBI's decision to seek the warrant rested on the disputed events in the hotel room.

Alternatively, the argument and undisputed facts for why the probable cause for the warrant is not derived from the events at the hotel room are almost identical to those the government presented to the district court for why the independent-source doctrine applies in this case. (ER 122, 132-36.)[7] The probable cause showing in the warrant adequately rests on grounds that are not tainted by any so-called illegality in Florida. *See United States v. Reed*, 15 F.3d 928, 933

[7] Defendant did not raise any argument or objection to the independent-source doctrine in his reply in the district court (ER 191-97.) In his opening brief, defendant summarily claims, for the first time on appeal, that the factual record for the independent-source doctrine and other arguments is insufficient. (AOB at 61.) But defendant has shown no good cause why he raises this his argument only now on appeal. These new arguments therefore are defective for the reasons previously discussed.

(9th Cir. 1994) ("information which is received through an illegal source is considered to be cleanly obtained when it arrives through an independent source." (citing *Murray v. United States*, 487 U.S. 533, 538-39 (1987))); *United States v. Oliver*, 630 F.3d 397, 409 (5th Cir. 2011) ("Even without mentioning the original seizure of the laptop, the affidavit contains sufficient information to make the resulting warrant a distinct, untainted source, permitting agents to reseize and search the laptop."). This is particularly true here, where a victim company (Blue Stone) and not a government actor held the UCI laptop from November 18, 2014, until December 9, 2014. (ER 60-61, 65, 70-71.) Again, the probable cause was based on the FBI's investigation in December 2014, not any actions of law enforcement in Florida on November 18, 2014.

The district court did not reach the government's independent-source arguments when ruling on the motion to suppress because the theft issue was dispositive. (ER 8.) Nonetheless, this Court should affirm the district court on this ground as well because the government's argument rests on undisputed facts and defendant did not challenge this argument in his reply in the district court. *See*, *e.g.*, *Magdrila,* 962 F.3d at 1156; *United States v. Pope*, 686 F.3d 1078, 1080

(9th Cir. 2012) (stating that the Court may affirm on any basis supported by the record even if the district court did not rely on that basis) .[8]

5. Any Error in Denying the Motion to Suppress Was Harmless

The evidence from the UCI laptop did corroborate other parts of the government's case at the re-trial. Nonetheless, any error by the admission of the UCI laptop evidence was harmless beyond a reasonable doubt because the evidence was merely cumulative. *United States v. Studley*, 783 F.2d 934, 941 (9th Cir. 1986) (citation omitted). The other evidence demonstrating defendant's guilt included: defendant's recorded admission on November 19, 2014, records from third-party providers and Blue Stone's server showing the deletions, forensic evidence from the wiped desktop computer, testimony describing defendant's abrupt resignation in front of a client, and

[8] The government agrees with defendant that the lawfulness of any seizure of the laptop in Florida by deputy sheriffs cannot be reviewed on appeal because the district court did not reach that issue. Thus, the issues of consent and emergency aid could only be determined on remand because an evidentiary hearing would be required to address these grounds to deny the motion. (AOB at 57-61.)

testimony from witnesses showing defendant was motivated by revenge and frustration to do the deletions. (ER 296-306, 400-03, 458-71, 526-29, 542-48, 563, 568-71, 587, 590-604, 682, 788-95, 813-22, 826-29, 832-42, 845-46, 896-97, 986-90, 993-96, 1238-41; GER 1-10, 33-63, 77-105, 114-210, 222-33.) For example, the government introduced records like Government Trial Exhibit 23 from Apple that objectively showed defendant wiping the Blue Stone desktop computer using the Find My iPhone Application. (GER 10.) That type of evidence showed defendant made the deletions. Because the laptop evidence was only cumulative, any error was harmless.

6. If the Court Was to Find the Denial of the Motion to Suppress Was Harmful Error, Only a Limited Remand Would be Necessary

Defendant's contention that *United States v. Christian*, 749 F.3d 806, 810-13 (9th Cir. 2014) requires remand and a new trial is incorrect. (AOB at 72-73.) This Court has overruled *Christian* and related cases because, even in the context of determining the admissibility of expert testimony, it typically will make no sense to require a new trial on remand if the district court's admissibility ruling would be correct on an alternative basis that was not before the Court. *United States v. Ray*,

__F.3d__, 2020 WL 6498258 (9th Cir. Nov. 5, 2020). The Supreme Court previously reached the same conclusion in the context of suppression issues similar to those raised in this case. When an appellate court identifies a flaw in the process by which evidence was assessed but the trial court reaches the same admissibility ruling on remand, "a new trial presumably would be a windfall for the defendant, and not in the public interest." *Waller v. Georgia*, 467 U.S. 39, 50 (1984). Thus, "a new trial need be held only if a new … suppression hearing results in the suppression of material evidence not suppressed at the first trial, or in some other material change in the positions of the parties." *Id.* Because the district court could ultimately deny the motion to suppress again on the grounds not reached, requiring a new trial would be a windfall for defendant and not in the public interest, particularly since there have already been two jury trials in this matter. If the Court finds that there was harmful error, the remand should be limited; if the district court denies the motion to suppress on remand on a ground not previously reached, then no new trial should result.

B. The Jury Instruction as to the Section 1030 Sentencing Enhancement Was Not Plainly Erroneous

1. Standard of review

When a defendant does not object to a jury instruction at trial, as here, the Court reviews that instruction for plain error. *United States v. Sanders*, 421 F.3d 1044, 1050 (9th Cir. 2005). When a defendant fails to object to a jury instruction in the district court, the standard of review is plain error. This Court "may only correct a plain error where the appellant demonstrates that: (1) there is an error; (2) the error is clear or obvious, rather than subject to reasonable dispute; (3) the error affected the appellant's substantial rights, which in the ordinary case means it affected the outcome of the district court proceedings; and (4) the error seriously affects the fairness, integrity or public reputation of judicial proceedings." *Id.*

2. The District Court's Instruction Tracked the Language of the Statute and the Evidence Squarely Fits that Language

Defendant contends that the district court's instruction as to the sentencing enhancement in this matter was plainly erroneous. (AOB at 65-74.) The district court used the instruction (ER 1229) which the parties jointly submitted. Defendant argues that the district court's

instruction was faulty as to defining "related course of conduct" for three reasons. (AOB at 68-69.) None of these reasons demonstrates error—let alone plain error. Defendant's three arguments for error are framed as "plain meaning" arguments, but they ignore the fact that the jury instructions were written and agreed-upon using the statutory language, 18 U.S.C. §§ 1030(c)(4)(B)(i), (c)(4)(A)(i)(I).

First, defendant contends that the "related course of conduct" must be equivalent to the § 1030(a)(5)(A) offense. (AOB at 69.) This is not what § 1030 says. To satisfy the $5,000 loss threshold, the government may use loss from the charged § 1030(a)(5)(A) offense and "loss resulting from a related course of conduct affecting 1 or more other protected computers." § 1030(c)(4)(A)(i)(I). "Loss" is defined at § 1030(e)(11). Section 1030(c)(4)(A)(i)(I) does not require that the "loss resulting from a related course of affecting 1 or more other protected computers" be equivalent to a § 1030(a)(5)(A) offense. Defendant is seeking to expand the plain language of § 1030(c)(4)(A)(i)(I).

Second, defendant argues that the district court needed to instruct the jury that "related" means the transmissions were "so connected that each individual act was part of a single episode with a common

purpose." (AOB at 69.) Defendant comes up with this definition of "related" without any legal support. The general rule is that "the district court need not define common terms that are readily understandable by the jury." *United States v. Hicks*, 217 F.3d 1038, 1045 (9th Cir. 2000). Given how the jury was instructed on the elements of § 1030(a)(5)(A) and "loss" (ER 1225-29) and the jury did not state it was confused as to the instructions, no further instruction as to "related" was needed.

Third, defendant argues that the jury was required to find that defendant intentionally caused a loss of $5,000 or more. (AOB at 69.) Section 1030(a)(5)(A) requires that defendant "intentionally cause[d] damage." But, that "intentionally" language is not present in the sentencing enhancement. The sentencing enhancement states that a violation of § 1030(a)(5)(A) carries a 10-year statutory maximum penalty if "the offense caused . . . a harm provided in [§ 1030(c)(4)(A)(i)(I)]." 18 U.S.C. § 1030(c)(4)(B)(i) (modified for the "harm" charged). The harm in § 1030(c)(4)(A)(i)(I) is, "loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss

resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value." Accordingly, the language in the sentencing enhancement does not require that defendant to intend to cause the amount of loss described in § 1030(c)(4)(A)(i)(I). The government is not aware of any authority finding that that the intent requirement applies to the loss. *See*, *e.g.*, *United States v. Goodyear*, 795 F. App'x 555, 559 (10th Cir. 2019) (describing elements of § 1030(a)(5)(A) and no mention of an intent requirement for the loss amount). The district court correctly did not include an intent requirement for the loss amount.

Even if the Court were to find error, any error was not plain. Defendant argues that, because of the alleged error, the jury could not have found that someone else issued the commands or that defendant accidently did it. (AOB at 72.) This ignores that the issue at trial was whether defendant sent the commands and whether he did it intentionally. The argument was that defendant—not someone—engaged in a "related course of conduct." Also, those arguments about identity and intent were able to be made with the instructions given, because they required the jury to find that *defendant's* offense "caused"

the loss. (ER 1173-74, 1181-82, 1186 (defense counsel arguing that someone else could have done the deletions).)

Defendant asserts that if the jury was instructed that the commands were related only if they were all part of a single episode with a common purpose, then the jury might have concluded that the "wipe" command to the desktop computer was distinct from the other commands in time and/or in nature to render them unrelated. (AOB at 72.) This argument ignores the evidence at trial which showed the deletions all occurred within a short period of time (between November 17 and 18, 2014). Moreover, the use of the phrase "related" required the jury to find the connection defendant now demands and permitted defendant to argue to the jury that the other deletions were unrelated. There was no prejudice to defendant with the jury instructions because defendant was able to make the argument that he now claims he could not make. However, all the evidence at trial showed that the deletions were "related" so such a defense would have been frivolous.

Indeed, as defendant points out, the loss evidence did not show the loss caused by each deletion but instead it was aggregated for all the deletions. (AOB at 72-73.) The government admitted proof that the

loss was greater than $50,000 with the bulk coming from Blue Stone employees' time ($48,550.60). (ER 297-98, 306, 322-25, 626-32, 678, 795-97, 847-49, 1242-43; GER 64-65, 211-21.) But, defendant is incorrect that the jury, with the instructions given, could not have found that any of the commands were "unrelated" and still made a loss determination in defendant's favor. (AOB at 73.) Rather, with the instructions given, if the jury found that any of the deletions were "unrelated" to the "wipe" command sent to the desktop computer, then it could have found defendant did not cause a loss of greater than $5,000 because the loss evidence was aggregated. The jury was required to find defendant's wiping of the Blue Stone desktop computer and *defendant's* related course of conduct "caused" the loss. The jury could have broken up the evidence however it saw fit with the instructions given.

Defendant argues that he was prejudiced by the sentencing enhancement jury instruction because the government did not prove that he intended to cause at least $5,000 in loss. (AOB at 73.) Section 1030 did not require such proof. But, defendant again ignores the evidence at trial, where defendant admitted multiple times that he

intentionally deleted Blue Stone's files. The evidence at trial did show that defendant intended to cause a loss of $5,000 or more to Blue Stone. Any suggestion that all the deletions were accidently was not supported by the evidence, including records from various third-party providers. This was a calculated computer attack on Blue Stone.

Defendant contends that the rule of lenity and constitutional avoidance supported defendant's claims of plain error. (AOB at 69-71.) The rule of lenity and constitutional avoidance do not apply here because § 1030 is not vague. These arguments can be summarily rejected.

Finally, defendant does not establish that any error in these circumstances seriously affects the "fairness, integrity or public reputation of judicial proceedings." The jury determined the loss amount under an agreed-upon instruction that tracked the statutory language in a case centered on whether defendant conducted coordinated attacks on a former employer. There was nothing fundamentally unfair in using this instruction once the jury found that defendant was guilty of the underlying offense.

V

CONCLUSION

For the reasons set forth above, defendant's conviction should be affirmed.

DATED: November 18, 2020

Respectfully submitted,

NICOLA T. HANNA
United States Attorney

BRANDON D. FOX
Assistant United States Attorney
Chief, Criminal Division

BRAM ALDEN
Assistant United States Attorney
Acting Chief, Criminal Appeals Section

/s/ Vibhav Mittal

VIBHAV MITTAL
Assistant United States Attorney
Deputy Chief, Santa Ana Branch Office

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 complies with the length limits permitted by Ninth Circuit Rule 32-1 because the brief contains 10,916 words, excluding the portions exempted by Fed. R. App. P. 32(f), if applicable.

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 2016.

DATED: November 18, 2020 */s/ Vibhav Mittal*

VIBHAV MITTAL
Attorney for Plaintiff-Appellee
UNITED STATES OF AMERICA