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.

On Appeal from the United States District Court
for the Central District of California
The Honorable Cormac J. Carney, Presiding
No. CR-16-00036-CJC

Appellant's Opening Brief

CUAUHTEMOC ORTEGA
Interim Federal Public Defender
JAMES H. LOCKLIN
Deputy Federal Public Defender
321 East 2nd Street
Los Angeles, California 90012
213-894-2929

Counsel for Defendant-Appellant

Table of Contents

Table of Authorities

Cases

U.S. Constitution

Statutes

Rules

Issues Presented

1. Erroneously determining that Nikishna Polequaptewa lacked Fourth Amendment standing, the district court (without holding any hearing) denied his motion to suppress the evidentiary fruits of sheriff deputies' unlawful entry into his hotel room to seize his laptop computer. Should the Court should reverse that ruling, reverse Polequaptewa's conviction, and remand for a new trial after a suppression hearing?
2. The charged crime was a misdemeanor unless the government proved that Polequaptewa intentionally caused loss of at least $5,000 through the offense and "a related course of conduct." The district court plainly erred in instructing the jury about this element. Should the Court reverse Polequaptewa's conviction and remand for a new trial?

Statement re Addendum

Pertinent authority is set forth in an attached addendum. *See* Circuit Rule 28-2.7.

Statement of Jurisdiction

A jury found Nikishna Polequaptewa guilty of one count of unlawfully damaging a computer in violation of 18 U.S.C. §1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I).[1] The district court, the Honorable Cormac J. Carney, Judge, presiding, had jurisdiction over this case under 18 U.S.C. §3231.

The district court entered its judgment on July 10, 2019.[2] Two days later, Polequaptewa filed a timely notice of appeal.[3] *See* Fed. R. App. P. 4(b).

This Court has jurisdiction to hear this appeal from the final judgment of a district court under 28 U.S.C. §1291.

Custody Status of Appellant

Nikishna Polequaptewa is in custody serving his 27-month sentence.[4] His projected-release date is August 2, 2021.

---

[1] ER 235-39, 1202-05, 1255-57. "ER" refers to the appellant's excerpts of record.

[2] ER 1285-90, 1312-13.

[3] ER 1291.

[4] ER 1285.

Statement of the Case

1. A jury found Nikishna Polequaptewa guilty of knowingly transmitting a command to intentionally cause damage to a computer with at least $5,000 in loss resulting from the offense and a related course of conduct.

In 2016, a grand jury indicted Polequaptewa on one count of violating 18 U.S.C. §1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I).[5] Section §1030(a)(5)(A) provides that whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer ... shall be punished as provided in subsection (c)[.]" Unless certain additional conditions are satisfied, subsection (c) makes this crime a misdemeanor punishable by no more than one year in custody. 18 U.S.C. §1030(c)(4)(G)(i). Polequaptewa was charged under a felony provision making the maximum sentence ten years "if the offense caused" specific kinds of harms. 18 U.S.C. §1030(c)(4)(B)(i). One such harm 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

---

[5] ER 27-29.

from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value[.]" 18 U.S.C. §1030(c)(4)(A)(i)(I).

The original indictment alleged that Polequaptewa had worked for Blue Stone Strategy Group, a company based in Irvine, California, but on November 18, 2014, he resigned and deleted various data files belonging to that company, including files on the company's internal server and a Mac Pro desktop computer, thereby causing at least $5,000 in loss to Blue Stone.[6] Polequaptewa's first trial on that charge ended in a mistrial when the jury couldn't reach a verdict.[7]

Before the retrial, the government obtained a superseding indictment charging the same offense but making two significant changes to the allegations.[8] First, the violation of §1030(a)(5)(A) was premised only on the Mac Pro desktop computer (not also Blue Stone's internal server, as in the original indictment).[9] **Let's call this the core misdemeanor crime.** Second, the new indictment alleged a "related course of conduct" resulting in at least $5,000 in loss to Blue Stone that encompassed not only deletion of files from the Mac Pro desktop and Blue Stone's

---

[6] ER 27-29.

[7] ER 206-34.

[8] ER 235-39.

[9] ER 238.

internal server but also deletion of Blue Stone's files on remote servers hosted by Google Inc., Bluehost Inc., MailChimp, and Cox Communications.[10] **Let's call this the felony enhancement.**[11]

At Polequaptewa's retrial, the district court instructed the jury that it could find Polequaptewa guilty of violating §1030(a)(5)(A) as "charged in the single-count First Superseding Indictment"—the core misdemeanor crime—only if the government proved three elements beyond a reasonable doubt: (1) that he knowingly caused the transmission of a program, a code, a command, or information to the Mac Pro desktop computer; (2) that, as a result of the transmission, he intentionally impaired, without authorization, the integrity or availability of data, a program, a system, or information; and (3) that the Mac Pro desktop computer was used in or affected interstate or foreign commerce or

---

[10] ER 237-39. Although the original indictment mentioned the data deleted from these remote servers, it didn't allege a "related course of conduct" encompassing those acts. ER 28-29.

[11] Although the terms "core misdemeanor crime" and "felony enhancement" are useful given how the crime was charged and presented to the jury here, in truth the core crime and the fact triggering the heightened sentence together constitute a new, aggravated crime. *Infra* Argument, Part 2.A.1.

communication.[12] The district court also instructed the jury that if it found Polequaptewa guilty of that offense, it would then have to decide 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"—the felony enhancement.[13] The district court told the jury it would have a verdict form requiring it to find whether the government met that burden.[14] "Loss" was defined, but what constituted a "related course of conduct" was never explained.[15] And the jury was generally instructed that it was there only to determine whether Polequaptewa was guilty or not guilty of "the

---

[12] ER 18-19, 1225.

[13] ER 20, 1229. According to the transcript, the district court used the phrase "as a result of such conduct, in a related course of conduct" (ER 20) when orally instructing the jury instead of the written version's "as a result of such conduct and a related course of conduct" (ER 1229). The jury was given a copy of the written instructions. ER 11, 1210.

[14] ER 24-26, 1235.

[15] ER 10-26, 1209-36.

charge in the First Superseding Indictment" because he was "not on trial for any conduct or offense not charged" therein.[16]

The jury found Polequaptewa guilty of the core misdemeanor crime and made the felony-enhancement finding.[17] The district court subsequently imposed a 27-month sentence,[18] and Polequaptewa appealed.[19] In this appeal, Polequaptewa raises two issues challenging his conviction: (1) that the district court erroneously denied his motion to suppress the evidentiary fruits of an illegal entry into his hotel room to seize his MacBook Pro laptop computer;[20] and (2) that the district court erred in failing to properly instruct the jury on the related-course-of-conduct element that increased the charged crime from a misdemeanor to a felony.[21] The remainder of this statement of the case will discuss the facts relevant to those issues.

---

[16] ER 17, 1223.

[17] ER 1202-05, 1255-57.

[18] ER 1285-90.

[19] ER 1291.

[20] *Infra* Argument, Part 1. Note that this is different from the Mac Pro *desktop* computer referenced in the indictments.

[21] *Infra* Argument, Part 2.

2. Without any hearing on the matter, the district court denied Polequaptewa's motion to suppress the evidentiary fruits of an unlawful entry into his hotel room to seize his laptop computer.

A significant amount of evidence at Polequaptewa's trial was obtained from his laptop computer, purportedly the tool he used to remotely delete most of the data at issue.[22] Although there were material factual disputes about how police seized that laptop, the district court sidestepped those issues by concluding that Polequaptewa lacked standing to bring a suppression motion because he purportedly "stole" the laptop when he didn't return it to a former employer upon being fired.[23]

A. *The Evidence Pertaining to the Seizure*. It's undisputed that the laptop was taken from Polequaptewa inside his hotel room at a Residence Inn in Florida by Broward County Deputy Sheriff Laughten Hall and other deputies without a warrant at the prompting of Blue Stone employee William Moon.[24] Polequaptewa and Hall told very different stories about how that happened in the declarations they submitted in support of and in opposition to Polequaptewa's suppression

---

[22] *Infra* Part 3.

[23] ER 1-8.

[24] ER 103-06, 184-90.

motion.[25] Because the district court didn't hold an evidentiary hearing on that motion, however, they weren't cross-examined and the court made no findings about what happened.[26] At Polequaptewa's retrial however, both Moon and Polequaptewa's wife testified about the circumstances surrounding the seizure, and their accounts are inconsistent with Hall's version in significant ways.[27] Each of the four accounts is summarized here:

1. *Polequaptewa's Declaration*. On November 18, 2014, Polequaptewa and other Blue Stone employees were in Florida for business meetings.[28] His wife and children accompanied him to Florida and stayed with him in his hotel room.[29] At about 7:25 p.m. EST,[30] Polequaptewa announced at a meeting that he was

---

[25] ER 103-06, 184-90.

[26] ER 1-8.

[27] ER 461-70, 494-513, 517-18, 1067-90.

[28] ER 103.

[29] ER 104.

[30] Some events on November 18 happened on the East Coast and others happened on the West Coast, so the brief will distinguish between Eastern Standard Time (EST) and Pacific Standard Time (PST).

resigning from Blue Stone.[31] He then went to dinner with his family before returning to his hotel room a few hours later.[32]

Polequaptewa heard a loud pounding on his hotel-room door shortly before 11:00 p.m. EST.[33] Unsure about who it was and whether it was safe to answer, he called 911 to request police assistance.[34] Shortly thereafter, he again heard loud knocking on the door, which was eventually opened from the outside until stopped by the security latch.[35] Through the cracked-opened door, Polequaptewa saw two groups of sheriff deputies (totaling about five or six officers) and Moon.[36] Apparently, one group of deputies responded to Moon's call and the other responded to Polequaptewa's.[37] A deputy said he was checking on Polequaptewa in response to a wellness call.[38] Polequaptewa replied that he was not harming himself and that he was in the room with his wife and his three small children, who

---

[31] ER 104.

[32] ER 104.

[33] ER 104.

[34] ER 104.

[35] ER 104.

[36] ER 104.

[37] ER 104.

[38] ER 104.

were sleeping.[39] The deputy then told Polequaptewa that the officers needed to come inside his room due to allegations that he was committing fraud on a laptop computer belonging to Blue Stone.[40] Polequaptewa told the deputy the computer was not Blue Stone's property and that the officers didn't have permission to enter his room.[41] In response, the deputy told Moon that the dispute was a civil matter and there was nothing more the officers could do, but Moon insisted that the computer belonged to Blue Stone.[42]

At that point, Polequaptewa asked everyone to leave and started to close the still security-latched door.[43] But the deputy put his hand inside the room to block the door and demanded that Polequaptewa open the door or else he would break it down and arrest him.[44] Polequaptewa said he wanted to exercise his Fourth

---

[39] ER 104.

[40] ER 104.

[41] ER 104.

[42] ER 104.

[43] ER 105.

[44] ER 105.

Amendment rights and deny the officers entry into his room.[45] The deputies mocked that assertion of his constitutional rights.[46]

When Polequaptewa heard the deputy instruct his partner to "get the tools" to break down the door, Polequaptewa unlatched the door to protect his children.[47] As soon as Polequaptewa did so, two deputies pushed their way into his room despite him again telling them he did not want them there.[48] The deputies insisted they would not leave without the laptop unless Polequaptewa could present proof of ownership, which he couldn't find.[49] The deputies therefore told Polequaptewa that they would take him to jail if he didn't hand over the laptop.[50] Because Polequaptewa felt threatened, he gave them the laptop to avoid a physical confrontation that might harm him or his family.[51]

---

[45] ER 105.

[46] ER 105.

[47] ER 105.

[48] ER 105.

[49] ER 105.

[50] ER 105.

[51] ER 105.

As soon as the deputies left Polequaptewa's room, they handed the laptop to Moon.[52] When Polequaptewa questioned that, the deputies told him to go into his room or things would go in a different direction.[53]

2. *Deputy Hall's Report and Declaration*. Deputy Hall wrote a short report near the time of the incident in November 2014, and then affirmed the accuracy of that report and asserted additional facts in a 2018 declaration.[54]

According to his report, Hall responded to a disturbance call and arrived at the Residence Inn shortly before 11:00 p.m. EST.[55] He met with the caller (Moon), who said Polequaptewa was an ex-employee not responding to calls or knocks at his hotel room.[56] Moon also told Hall that Polequaptewa had had used a company computer—still in his possession inside his hotel room—to delete files "in reference to an alleged identity fraud cases [sic]" such that "approximately (200) identities were compromised by" Polequaptewa.[57] Hall supposedly told Moon that

---

[52] ER 105.

[53] ER 105.

[54] ER 184-90.

[55] ER 190.

[56] ER 190.

[57] ER 190.

unless he had proof of ownership, the computer could not be taken without the Polequaptewa's consent.[58]

In his report, Hall asserted that "[c]ontact was made with Mr. Polequaptewa to insure he was alive" and to evaluate whether he "was distraught over the loss of his job."[59] His declaration four years later embellished on that bald assertion, claiming that he wanted to keep Polequaptewa calm and ascertain his mental state to confirm that he would not harm himself or his family.[60] When Hall entered the hotel room, he supposedly "knew, among other things, that Mr. Polequaptewa was in a new state, no longer had a job, and his former employer was accusing him of engaging in fraud."[61] Notably, neither Hall's report nor his declaration recounted how he entered Polequaptewa's hotel room.[62]

Hall's police report described the encounter he had with Polequaptewa, apparently after he entered the hotel room with Moon.[63] Hall noted that Polequaptewa's child was asleep in the room where they spoke, with his wife and

---

[58] ER 190.

[59] ER 190.

[60] ER 184.

[61] ER 184-85.

[62] ER 184-90.

[63] ER 190.

other children in another room in the suite.[64] According to Hall, Polequaptewa (fully dressed in a suit) appeared nervous, with shaking hands.[65] At one point, Polequaptewa and Moon "had a yelling match" over ownership of the laptop but neither could present proof of ownership.[66] Hall supposedly told Polequaptewa that "this was a civil matter and [his] presence was just to insure a peaceful interaction between the two parties."[67] But the report also stated that Hall told Polequaptewa "that if he had nothing to hide giving the computer to Mr. Moon would show that he was innocent and had nothing to hide."[68] Hall also supposedly advised Polequaptewa "to take pictures of the laptop and lock the device before giving it to Mr. Moon."[69] Although the report didn't memorialize Polequaptewa's response, Hall claimed in his declaration that his "memory is that Mr. Polequaptewa consented to turn over a laptop in his room to William Moon."[70]

---

64 ER 190.

65 ER 190.

66 ER 190.

67 ER 190.

68 ER 190.

69 ER 190.

70 ER 186.

In his declaration, Hall disputed claims made in Polequaptewa's declaration, asserting that he did not recall any of the following: Polequaptewa claiming that the laptop didn't belong to Blue Stone;[71] Polequaptewa saying he didn't want the deputies to enter his hotel room; any deputy putting a hand inside Polequaptewa's room to block the door, demanding that he open the door, or threatening to break down the door and arrest him if he didn't do so; any deputies telling Polequaptewa that they needed to enter the room in response to Moon's fraud allegation; Polequaptewa asserting his Fourth Amendment rights; any deputy making derogatory statements in response; any deputy telling Polequaptewa they would not leave without the laptop unless he could present proof of ownership or that they would take him to jail if he did not hand over the laptop; or any deputy having the conversation described by Polequaptewa after they left his room.[72]

3. *William Moon's Trial Testimony*. Moon testified that John Mooers (Blue Stone's co-founder) called from Irvine to tell him that files were being deleted from somewhere in the Florida hotel.[73] Although Moon testified that Mooers

---

[71] Notably, this was inconsistent with his report's assertion that Polequaptewa and Moon "had a yelling match" over ownership of the laptop. ER 190.

[72] ER 185.

[73] ER 461, 494; *see also* ER 587. Moon told an FBI agent he got this call at about 10:00 p.m. EST. ER 59.

instructed him to get Polequaptewa's computer, which they believed to be Blue Stone's property,[74] Mooers denied doing so, testifying that he only told Moon to find Polequaptewa and then to call the police.[75] It was undisputed that Moon and Mooers were mistaken in that the laptop at issue did not, in fact, belong to Blue Stone.[76]

Moon testified that he and others tried calling Polequaptewa several times from 9:00 to 9:30 p.m. EST but couldn't reach him.[77] Moon therefore went to Polequaptewa's hotel room with hotel staff, but no one answered their knocks on the door.[78] Moon's testimony was unequivocal—he had no concerns about Polequaptewa's well-being; his intent was to get Polequaptewa's laptop computer.[79] After Mooers informed Moon that files were still being deleted, Moon got the hotel staff to unlock the door to Polequaptewa's room, but it opened only a couple inches because it was latched from the inside.[80] Then the staff, at Moon's

---

[74] ER 463-64, 494, 518.

[75] ER 616-17, 709-10.

[76] ER 617, 518.

[77] ER 461-62, 496.

[78] ER 462-64, 499.

[79] ER 465, 496, 500-03, 514.

[80] ER 465, 498-504.

request, called the police.[81] When two deputies arrived about 20-30 minutes later, Moon "explained the situation[,]" namely, what Mooers had told him about the files being deleted.[82]

Moon and the hotel staff person returned to Polequaptewa's room with the deputies and knocked again with no response.[83] The deputies instructed the staff person to unlock the door, which was still secured from the inside by a security latch such that it opened only a couple inches.[84] The deputies spoke through the crack for five to ten minutes but still got no response.[85] At some point, a second set of deputies arrived at the scene in response to a call made from inside the room, but they soon left and allowed the deputies already there to handle the matter.[86]

Eventually, those deputies got Polequaptewa to respond by repeatedly threatening over several minutes to enter the room without his consent.[87] As Moon described it: "[T]he sheriff officer finally said, look, we are going to go in there.

---

[81] ER 465-66, 497, 504.

[82] ER 466, 504-06.

[83] ER 467, 506.

[84] ER 467, 506.

[85] ER 467, 506-07.

[86] ER 468-69, 507-08.

[87] ER 467, 508-11.

Let's make it easy. Can you please open the latch, open it and have a conversation and so forth. No response. The officer persisted in, you know, asking the door to be opened. But, you know, at some point the officer said one way or another we are going to go in, but let's make it easy. Repeated many times."[88] When that prompted a response from Polequaptewa, the deputy said something like, "we are trying to retrieve the computer[.]"[89] Polequaptewa opened the door.[90] Polequaptewa insisted it was his computer, and Moon insisted that the computer belonged to Blue Stone.[91] Moon said he never went inside Polequaptewa's room.[92] And although he never saw the deputies go inside the room, he wasn't with them the entire time.[93] But he did hear the deputies tell Polequaptewa that he would have to surrender the computer to them and work out the "formalities" of

---

[88] ER 467.

[89] ER 467.

[90] ER 511-12.

[91] ER 467-68.

[92] ER 469, 517.

[93] ER 466-67, 512. Moon told an FBI agent that a deputy entered the room to speak with Polequaptewa and later came out with his laptop, which he then gave to Moon. ER 60.

ownership later.[94] Eventually, sometime around 1:00 to 1:30 a.m. EST, the deputies gave Moon the laptop they took from Polequaptewa.[95]

4. *Yolanda Polequaptewa's Trial Testimony*. Polequaptewa's wife Yolanda shared the hotel room—a suite consisting of a living-room area, a kitchenette, and a bedroom.[96] She testified that Polequaptewa returned to the room at about 5:30 p.m. EST and took the family out for dinner and shopping, returning to the suite by 7:00 p.m. EST.[97] Sometime between 8:00 and 8:30 p.m. EST, Moon started pounding loudly on the door and screaming angrily.[98] Moon left for a while but then returned, resumed his pounding, and demanded the laptop, so Polequaptewa called the police.[99] At some point, police deputies arrived and also started pounding on the door very loudly.[100] Later, a second set of deputies arrived, apparently in response to Polequaptewa's call.[101] The deputies were "saying to

---

[94] ER 512-13.

[95] ER 469-70, 513.

[96] ER 1067-68, 1079.

[97] ER 1068-71, 1086.

[98] ER 1071-74, 1086.

[99] ER 1074-75, 1086, 1089.

[100] ER 1075-76, 1086.

[101] ER 1086-87, 1089.

'open up,' to 'give back the laptop,' like, if he didn't open up, that they were going to break down the door or open the door or get in."[102] Eventually, the door was opened from the outside, at least to the extent allowed by the inside security latch.[103] The deputies continued to tell Polequaptewa to open the door and hand over the laptop.[104] Polequaptewa responded that the laptop didn't belong to Blue Stone.[105] At that point, Polequaptewa invoked his Fourth Amendment rights, provoking a mocking response from the deputies.[106] Yolanda could hear Mooers on a speakerphone in the hallway telling Moon and the deputies to get the laptop.[107] The deputies again told Polequaptewa that they were going to open the door either way, so he needed to let them in and give them the laptop.[108] Yolanda was in the bedroom when the deputies entered the suite's kitchenette area, but she heard them tell Polequaptewa that they would not leave without the laptop,

---

[102] ER 1076.

[103] ER 1076.

[104] ER 1076.

[105] ER 1076, 1090.

[106] ER 1076-77, 1089.

[107] ER 1077-78.

[108] ER 1078, 1089.

although he could password-protect it first.[109] When she came out of the bedroom sometime between 8:30 to 9:00 p.m. EST, the deputies and the laptop were gone.[110] When asked whether the events she described might have happened later in the evening, Yolanda said she didn't know.[111]

B. *The Suppression Motion*. Polequaptewa filed a motion to suppress the evidentiary fruits of the laptop seizure, arguing (among other things) that the sheriff deputies violated his Fourth Amendment rights by entering his hotel room and taking his laptop without a warrant and without his consent.[112] That motion was supported by Polequaptewa's declaration (discussed above).[113]

The government opposed the motion.[114] Its primary argument was that Polequaptewa had no reasonable expectation of privacy in the laptop because he had purportedly stolen it from the University of California, Irvine (UCI), his former employer, by not returning it after he was fired.[115] To support that

---

[109] ER 1078-79, 1087, 1105-07.

[110] ER 1079-81, 1087.

[111] ER 1087-88.

[112] ER 30-47.

[113] ER 103-06.

[114] ER 109-37.

[115] ER 123-27.

argument, the government proffered declarations from UCI employees.[116] Alternatively, the government argued that the Florida sheriff deputies entered Polequaptewa's hotel room lawfully and took the laptop with his consent.[117] To support that argument, the government proffered Deputy Hall's declaration and police report (discussed above).[118] Finally, the government asserted that even if there was a Fourth Amendment violation, the independent-source and good-faith exceptions to the exclusionary rule applied.[119]

In his reply, Polequaptewa noted that the government's claim that UCI owned the laptop conflicted with his assertion that the laptop was his and Moon's claim in 2014 that it belonged to Blue Stone.[120] Furthermore, he argued that regardless of who owned the computer, the sheriff deputies violated the Fourth Amendment in entering his hotel room to seize it.[121]

---

[116] ER 146-83.

[117] ER 128-31.

[118] ER 184-90.

[119] ER 132-36.

[120] ER 192-93.

[121] ER 192-94.

The government insisted that no evidentiary hearing was necessary because the district court could rule in its favor based on the declarations alone.[122] Polequaptewa, however, requested an evidentiary hearing where he could cross-examine the government's declarants.[123]

Without holding any hearing (evidentiary or otherwise), the district court issued a written order denying Polequaptewa's suppression motion.[124] That ruling was based entirely on the government's factual claim that UCI owned the laptop and its legal argument that that purported fact precluded Polequaptewa's Fourth Amendment claim.[125] Because it concluded that Polequaptewa lacked standing to challenge the search and seizure of the laptop, the district court decided that it "need not reach his arguments regarding the constitutionality of the search and seizure of that laptop."[126] The district court also didn't address the government's independent-source and good-faith arguments.[127]

---

[122] ER 197-200.

[123] ER 200.

[124] ER 1-8.

[125] ER 6-8. The facts related to ownership of the laptop are discussed below. *Infra* Argument, Part 1.B.

[126] ER 8 n.2.

[127] ER 1-8.

3. At trial, the government's claim that Polequaptewa caused at least $5,000 in damage was based not only on the specifically-charged act of wiping a particular desktop computer but also on a purportedly related course of conduct affecting several other computers.

The jury learned that Blue Stone is a consulting business working primarily with Native American communities that was headquartered in Irvine in 2014.[128] In April of that year, the company hired Polequaptewa (a Native American himself) as a senior strategist to work on projects across the country, as well as marketing.[129] At that time, responsibility for handling Blue Stone's information-technology (IT) needs had been outsourced to Runner Boys, a company owned by Eldad Yacobi, for several years.[130] But shortly after Polequaptewa was hired, Blue Stone granted his request to expand his role to take over IT from Yacobi.[131] Thereafter, among other things, Polequaptewa switched the company to Google services, purchased Apple computers, began hosting Blue Stone's website on the

---

[128] ER 277-81, 310-11, 435-38.

[129] ER 311-15, 334-35, 350-51.

[130] ER 318, 345-46, 349, 706, 806-11, 861-62.

[131] ER 316-18, 594-99, 706.

company's own Synology-brand server instead of having an outside company do that, and created a database for client relationship management (CRM) information.[132]

In August 2014, only four months after joining the company, Polequaptewa asked John Mooers (Blue Stone's co-founder and his supervisor at the time) for a raise and the title of chief technology officer, and he got the raise because he was doing a good job.[133] Around the same time, however, William Moon joined Blue Stone and became Polequaptewa's supervisor.[134] Soon thereafter, Moon informed Blue Stone's management that, in his opinion, Polequaptewa's IT and marketing duties distracted from his primary responsibilities as a senior strategist such that his job performance suffered across the board.[135] Moon also complained about Polequaptewa's reluctance to travel.[136]

On Friday, November 14, Blue Stone's management met with Polequaptewa to inform him that his IT duties would be reassigned back to Yacobi (also present at

---

[132] ER 590-93, 782-83.

[133] ER 585-87, 601-05, 682-84.

[134] ER 439, 605, 685.

[135] ER 319, 439-51, 473-79, 605-06, 685-86.

[136] ER 447, 451-53.

the meeting) and that someone else would take over his marketing projects.[137] Polequaptewa wasn't demoted—he retained his position as a senior strategist—and he didn't exhibit any negative reaction to the news.[138] Moreover, Blue Stone offered Polequaptewa the opportunity to participate in a months-long project in Florida for an important client, and despite his purported dislike of travel, he agreed.[139]

Immediately after that meeting, Polequaptewa and Yacobi met to pass along IT-access information.[140] Yacobi claimed that Polequaptewa seemed displeased with the reassignment of his IT duties and was therefore uncooperative and provided incomplete information.[141] Thereafter, Yacobi had "administrator" access to Blue Stone's systems, but according to him, Polequaptewa also retained some ability to access certain systems as an administrator.[142] In addition, Polequaptewa remained able write and delete some data as a user even without administrator access, just

---

[137] ER 318-20, 346, 472-73, 540-41, 607-08, 786-87, 799, 811-13.

[138] ER 351, 381, 608.

[139] ER 351-52, 454-55, 479-88, 684-87.

[140] ER 813-14, 819.

[141] ER 814-15, 868-70.

[142] ER 369-70, 696, 819-21.

like any other employee.[143] At some point later that day, Mooers, an office manager, and Yacobi decided to reset everyone's passwords except Polequaptewa's for a "fresh start."[144] Given Polequaptewa's prior role, other employees still occasionally sought his help for IT problems in the days that followed.[145]

On Monday, November 17, several Blue Stone employees, including Polequaptewa and Moon, were in Florida for client meetings, with everyone staying at the Residence Inn.[146] Yacobi (still in Irvine) testified that his meeting with Polequaptewa the prior Friday left him feeling that Polequaptewa "might do something with his computer remotely" and that "something [was] going on."[147] Therefore, early in the morning of Tuesday, November 18, he went to Blue Stone's offices to backup Polequaptewa's Mac Pro desktop computer to the company's internal Synology server.[148] Although Yacobi said he was able to access that

---

[143] ER 821-23.

[144] ER 609-11, 695-96, 824.

[145] ER 611-14, 692-98, 788-91, 826-27.

[146] ER 371, 455-56, 525-26.

[147] ER 868-70.

[148] ER 824, 867-72, 876-77.

desktop computer without a password because Polequaptewa had left it on,[149] Polequaptewa's wife testified that she was with her husband when he left his office on Friday evening and saw that the computer was off.[150] Yacobi purportedly didn't recall accessing any of Polequaptewa's personal information when he went onto his desktop computer.[151] And while Yacobi acknowledged that he was familiar with software that allows IT specialists to access computers remotely, he insisted that he didn't have the ability to remotely access either Polequaptewa's Mac Pro desktop computer or the MacBook Pro laptop computer he had in Florida.[152]

At a group get-together with the client tribe in Florida that Tuesday at about 7:10 p.m. EST, Polequaptewa publically resigned without notice and then left.[153] But Polequaptewa didn't disparage Blue Stone as he did so; in fact, he told the tribe that the company would continue to do a good job.[154] Moon told Mooers (who was in California) about Polequaptewa's resignation.[155]

---

[149] ER 824, 872-75.

[150] ER 1056-62, 1065-66.

[151] ER 872, 877-78, 896.

[152] ER 825, 846, 868, 882-83.

[153] ER 455-59, 491-93, 527-29.

[154] ER 528, 531.

[155] ER 459-60, 615-16.

According to the government, various computer records purportedly established that the following occurred on November 18:

- Someone using the Residence Inn's IP address accessed Blue Stone's account for MailChimp (a marketing service that maintained a database of Blue Stone's potential clients) and deleted its files.[156] Blue Stone could not recover that data.[157]
- Someone using IP addresses associated with the Residence Inn and Polequaptewa's phone, along with Polequaptewa's login credentials, accessed Blue Stone's Google Drive account (a file-sharing service) and deleted files there.[158] Blue Stone was able to recover that data.[159]
- Someone using Florida IP addresses and the login credentials for Polequaptewa and another employee (whose login credentials were purportedly available to Polequaptewa) accessed Blue Stone's internal Synology server (which held CRM data, website files, backups, and other

---

[156] ER 281-82, 384, 403, 410-11, 418-19, 783-85, 1006-07, 1010, 1249.

[157] ER 794-95, 840-41.

[158] ER 820-21, 823, 829-31, 836, 1006-09, 1250.

[159] ER 546, 554-55, 836.

information) and deleted its data.[160] Blue Stone could not recover that data.[161]

- Someone using Polequaptewa's login credentials deleted Blue Stone's offsite backup files with Cox Communications.[162] Blue Stone could not recover that data.[163]
- Someone using Polequaptewa's login credentials purportedly deleted files held by Bluehost (the company that maintained Blue Stone's website before Polequaptewa moved the website to Blue Stone's internal server).[164] Blue Stone apparently recovered that information because it was used to rebuild its website.[165]

At some point on November 18 after Polequaptewa resigned, a Blue Stone employee in Irvine noticed that certain files were being deleted, so she told Mooers, who informed Moon.[166] The jury heard the above-described testimony

---

[160] ER 791-94, 802-03, 816, 828-29, 832-35, 837, 1245.

[161] ER 829.

[162] ER 817-18, 841, 896-97, 993-96, 1251.

[163] ER 841-42.

[164] ER 782-83, 790, 801-02, 847, 920-21, 934-35, 1005, 1154-55, 1248.

[165] ER 793, 796-97.

[166] ER 461, 494, 544-45, 615-17, 707-08.

from Moon and Polequaptewa's wife about how Moon then came to get Polequaptewa's MacBook Pro laptop.[167] After passing through many more hands, the laptop eventually made it to the FBI.[168]

A significant amount of the government's evidence was derived from an FBI agent's forensic examination of the laptop.[169] Among other things, the agent testified that: the laptop was password protected with Polequaptewa as the only named user; on November 18, the laptop was used to access the websites for Blue Stone, Synology, Google, and Bluehost; that day, searches were run for "how to delete all files on a Synology DiskStation," "how to reset a Synology DiskStation," "how to reformat a Synology DiskStation," "Google apps for business," "MailChimp, what if I accidentally delete my list," "my Synology," "Synology, how to access my php admin remotely," and "Cox Business"; the laptop was last accessed and turned off at 11:40 p.m. EST on November 18; and settings permitting remote access were turned off (although the agent conceded on cross-examination that a skilled hacker could still gain access).[170]

---

[167] *Supra* Parts 2.A.3 & 2.A.4.

[168] ER 470-71, 513-14, 617-18, 688-90, 972-73, 1028-29.

[169] ER 900-64, 1270-73, 1280-81.

[170] ER 910-55.

The evidence about Blue Stone's internal server and its accounts with Google, MailChimp, Cox, and Bluehost pertained to the felony enhancement for a "related course of conduct," not the core misdemeanor crime of impairing the Mac Pro desktop computer used by Polequaptewa at Blue Stone's offices.[171] Other evidence reflected that at 12:50 a.m. EST on November 19—in other words, *after* Polequaptewa's laptop was taken from him—someone using the Residence Inn's IP address and his Apple iCloud credentials initiated a "wipe" of that desktop computer.[172] A "wipe" (or "erase") command issued remotely using an application on an iPhone or Apple computer will delete the data on the target computer but will not damage the computer's hardware.[173] At about 4:00 p.m. PST on November 19, the Mac Pro desktop computer was turned on, received the wipe command issued earlier that day, and shut down.[174] Thereafter, that computer had

---

[171] *Supra* Part 1.

[172] ER 816, 1011-13, 1020-21, 1246. Two minutes later, a "wipe" of Polequaptewa's MacBook Pro laptop was initiated in the same way, but because it never again connected to the internet, it didn't receive and execute that command. ER 769, 1012-13, 1026-27.

[173] ER 757-58, 760, 768-69, 772.

[174] ER 768, 845-46, 1013-14.

no data or system software, so it would not boot up.[175] The operating system could be recovered, rendering the computer useable again, but the data would be lost unless backed up elsewhere.[176] The wipe command did not affect any other computer.[177]

Polequaptewa's wife testified that after the police took her husband's laptop and left their hotel room by 9:00 p.m. EST on November 18, Polequaptewa discovered that he couldn't access his personal e-mail accounts or his Apple iCloud account, and he received an alert from his bank.[178] For the next hour or so, they tried to regain access, but apparently someone else in Irvine was trying to access the accounts.[179] Sometime around 10:00 or 10:30 p.m. EST, Polequaptewa (who wanted to totally disassociate from Blue Stone) deleted all the company files he had on his phone.[180] Polequaptewa's wife also testified that she and her husband

---

[175] ER 846, 570, 988.

[176] ER 570-71, 573-74, 772-73.

[177] ER 1022, 1026.

[178] ER 1081.

[179] ER 1081-84.

[180] ER 1083-84, 1114, 1117.

were probably asleep at 12:50 a.m., when someone sent the command to wipe the Mac Pro desktop.[181]

On Wednesday, November 19, Polequaptewa arrived at Blue Stone's Irvine offices, and part of that visit was captured on cellphone video.[182] Polequaptewa tried to get personal belongings from his office, but Mooers prevented him from doing so, claiming at trial that police officers instructed him to not let Polequaptewa take anything without their approval.[183] At one point, Jaime Fullmer (Blue Stone's CEO) said he wanted to "get all of our stuff as well"—in his mind, referring to the deleted data.[184] Polequaptewa responded: "What stuff? I deleted it. That's the point."[185] Fullmer and Mooers acknowledged that Polequaptewa had his

---

[181] ER 1085, 1103-04, 1116-17.

[182] ER 298-304, 364-69, 379-80, 618-19, 730, 733-36, 842-45, 892-94, 990-91, 1030-31. The video was Exhibit 66 and a transcript of it (shown to the jury but not in evidence) was Exhibit 66A. ER 302, 1237-41. Because this transcript and the trial record adequately describe what happened for purposes of this appeal, Polequaptewa is not seeking leave to transmit CDs with copies of the video pursuant to Circuit Rule 27-14, but if the Court nevertheless wants copies, he will gladly provide them.

[183] ER 372-73, 729-31, 736-39, 1062-65, 1238-41.

[184] ER 304, 1241.

[185] ER 740, 1241.

phone in his hand at the time, but they insisted that he could not have been referring to deleting company data from that phone in accordance with Blue Stone's confidentiality agreement.[186] In an interaction not captured by the video, Fullmer asked Polequaptewa "why he did it" and Polequaptewa supposedly responded something like, "I did it and it's done."[187] At that point, police arrived and told Polequaptewa to leave the premises.[188]

Blue Stone filed a civil suit against Polequaptewa in connection with the data deletion.[189] He filed a countersuit alleging that Blue Stone improperly paid tribal leaders to obtain contracts, that it retaliated against him for whistleblowing, that it hacked into his personal e-mail accounts, and that it failed to return his personal property.[190] There may have been settlement discussions at some point, but the civil case was stayed until the criminal case was over.[191]

Blue Stone claimed that it spent more than $50,000 responding to the data deletions, but it didn't break out how much of that loss was caused by the Mac Pro

---

[186] ER 304-05, 373-79, 732-33, 740-41.

[187] ER 305-06.

[188] ER 306, 730-31.

[189] ER 307-08, 331-33, 1029.

[190] ER 308-10, 336-45, 381-82, 722-29, 1029-30.

[191] ER 308, 325-31, 720-22.

wipe.[192] Likewise, in its closing arguments, the government contended that the loss from all the activity exceeded $50,000, but it never suggested that any loss caused by wiping of the Mac Pro desktop alone exceeded the $5,000 threshold required to bump the charged crime from a misdemeanor to a felony.[193]

Summary of Argument

A jury found Nikishna Polequaptewa guilty of intentionally causing damage to a computer via transmission of a command (by itself, a misdemeanor) with the loss resulting from the offense and "a related course of conduct" amounting to at least $5,000 (making the crime a felony).

1. A significant amount of evidence at Polequaptewa's trial was obtained from his laptop computer—purportedly the tool he used to remotely delete most of the data at issue. Sheriff deputies seized that laptop from him after entering his hotel room without a warrant. Polequaptewa filed a motion to suppress the fruits of that Fourth Amendment violation, but the district court denied it on the ground that he lacked standing as to the laptop.

---

[192] ER 296-98, 306, 320-25, 623-32, 678, 698-705, 711-12, 795-97, 847-49, 1242-43.

[193] ER 1139-41, 1162-63, 1197-98.

A. The district court ignored that, regardless of Polequaptewa's interest in the laptop, he undisputedly had Fourth Amendment standing to challenge an unlawful entry into his hotel room. He contended that the deputies unlawfully entered his room because warrantless searches and seizures are per se unreasonable, he did not consent to the entry or to the seizure of the laptop, and no other exception to the Fourth Amendment's warrant requirement rendered the deputies' conduct reasonable. The exclusionary rule encompasses both evidence seized during an unlawful search and any indirect products of such invasions—so-called "fruit of the poisonous tree." Because the laptop was the evidentiary fruit of the entry into Polequaptewa's hotel room, any evidence obtained from the laptop should have been suppressed if that entry was unlawful, regardless of whether he had independent standing to challenge the search of the laptop directly.

B. To the extent it matters whether Polequaptewa also had standing to directly challenge the seizure and search of the laptop, the district court erred in not holding an evidentiary hearing on that contested issue. Polequaptewa filed a declaration stating that the computer was his. In response, the government presented declarations from his former employer claiming that the laptop was its property and that Polequaptewa "stole" it when he didn't return it after being fired. Despite the factual dispute about the laptop's ownership, the district court

erroneously accepted the government-proffered declarations at face value, refusing Polequaptewa's request to cross-examine the declarants. Doing so not only conflicted with the well-established principle that cross-examination is the principal means by which the believability of a witness and the truth of his testimony are tested; it also infringed his constitutional rights under the Fourth Amendment, the Due Process Clause, and the Confrontation Clause.

C. Because of its faulty standing ruling, the district court didn't reach the merits of the suppression issues. In particular, the government claimed that the consent and emergency-aid exceptions to the Fourth Amendment's warrant requirement applied. It also argued that if a Fourth Amendment violation occurred, then the independent-source and good-faith exceptions to the exclusionary rule applied. The government bears the burden to prove all these exceptions, so an evidentiary hearing and express factual findings by the district court are required on these contested issues.

D. Precedent requires a new trial when evidence admitted through an erroneous analysis prejudices the opposing party but the record is too sparse to conduct a proper admissibility analysis and decide whether the admission itself was erroneous. That's what happened here, so the Court should reverse Polequaptewa's conviction and remand for the district court to first hold a hearing

on the suppression motion and then hold a new trial regardless of the ruling on the suppression motion.

2. The district court plainly erred in failing to properly instruct the jury about the element that increased the charged crime from a misdemeanor to a felony—that the core offense (wiping one particular computer) and "a related course of conduct" caused at least $5,000 in loss. The plain language of the charging statute establishes three things about this element. First, each step of the course of conduct must be equivalent to the core offense such that the government had to prove that each additional alleged transmission of a command satisfied all three elements of that crime. Second, the government also had to prove all of those transmissions were so connected that each individual act was part of a single episode with a common purpose. Finally, because the core crime required proof that Polequaptewa intentionally caused damage, the felony enhancement required proof of his intent to cause at least $5,000 in loss. There's a reasonable probability that the jury's verdict would have been different had it been properly instructed about these things. The Court should therefore reverse Polequaptewa's conviction and remand for a new trial.

Standards of Review

1. The Court reviews the denial of a motion to suppress de novo and the underlying factual findings for clear error. *United States v. Grey*, 959 F.3d 1166, 1177 (9th Cir. 2020). It reviews the denial of an evidentiary hearing for abuse of discretion. *United States v. Herrera-Rivera*, 832 F.3d 1166, 1172 (9th Cir. 2016).

2. Even when a defendant doesn't object to jury instructions, the Court may grant relief if the district court erred, that error was plain, the error affected his substantial rights, and the error seriously affects the fairness, integrity, or public reputation of judicial proceedings. *United States v. Depue*, 912 F.3d 1227, 1232-33 (9th Cir. 2019) (en banc).

Argument

1. The Court should reverse the district court's denial of Nikishna Polequaptewa's motion to suppress evidence, reverse his conviction, and remand for a new trial after a suppression hearing.

The Fourth Amendment protects people from unreasonable searches and seizures and generally requires a warrant issued upon probable cause. U.S. Const., Amend. IV. Nikishna Polequaptewa filed a motion to suppress the evidentiary

fruits of the constitutional violations that occurred when Florida sheriff deputies entered his hotel room and took his laptop without a warrant and without his consent.[194] The government opposed the motion, asserting the following arguments: Polequaptewa lacked standing because he had no reasonable expectation of privacy in the laptop; anyway, he consented to the deputies entering his hotel room and taking the laptop; alternatively, the deputies properly entered the hotel room under the emergency-aid exception to the Fourth Amendment's warrant requirement; and finally, even if the deputies violated the Fourth Amendment, the independent-source and good-faith exceptions to the exclusionary rule applied.[195] At the government's request and over Polequaptewa's objection,[196] the district court denied the suppression motion without a hearing based entirely on its conclusion that he lacked standing as to the laptop; it therefore didn't reach the other issues.[197]

As discussed below, the district court erred because Polequaptewa had standing to challenge the unlawful entry into his hotel room, and the subsequent seizure of

---

[194] ER 30-47, 191-94; *see also supra* Statement of the Case, Part 2.

[195] ER 109-37.

[196] ER 197-200.

[197] ER 1-8.

the laptop was suppressible as the fruit of that unconstitutional conduct regardless of whether the laptop was stolen (as the government alleged). Furthermore, the district court erred in concluding that Polequaptewa did not separately have a Fourth Amendment interest in the laptop itself without holding an evidentiary hearing on that disputed matter. An evidentiary hearing is also required to delve into the issues the district sidestepped with its erroneous standing ruling. The Court should therefore reverse the denial of the suppression motion, reverse Polequaptewa's conviction, and remand for a new trial after a suppression hearing.

A. Polequaptewa had standing to challenge the unlawful entry into his hotel room, and the seized laptop was suppressible as the fruit of that constitutional violation regardless of whether it was stolen.

Although the district court used the term "standing,"[198] the Supreme Court has explained that "Fourth Amendment 'standing' ... is not distinct from the merits and is more properly subsumed under substantive Fourth Amendment doctrine." *Byrd v. United States*, 138 S.Ct. 1518, 1530 (2018) (quotation marks omitted). "The concept of standing in Fourth Amendment cases can be a useful shorthand for capturing the idea that a person must have a cognizable Fourth Amendment

[198] ER 6-8.

interest in the place searched before seeking relief for an unconstitutional search," however. *Id*. Polequaptewa will use "standing" in this manner.

A defendant has Fourth Amendment standing if he had either a proprietary interest or a reasonable expectation of privacy in the area searched or property seized. *Florida v. Jardines*, 569 U.S. 1, 5 (2013); *United States v. Jones*, 565 U.S. 400, 404-08 (2012). A "guest in a hotel room"—like Polequaptewa—"is entitled to constitutional protection against unreasonable searches and seizures" because he has a reasonable expectation of privacy. *Stoner v. California*, 376 U.S. 483, 490 (1964); *see also Minnesota v. Olson*, 495 U.S. 91, 99 (1990) ("We are at our most vulnerable when we are asleep because we cannot monitor our own safety or the security of our belongings. It is for this reason that, although we may spend all day in public places, when we cannot sleep in our own home we seek out another private place to sleep, whether it be a hotel room, or the home of a friend. Society expects at least as much privacy in these places as in a telephone booth—a temporarily private place whose momentary occupants' expectations of freedom from intrusion are recognized as reasonable[.]") (quotation marks omitted); *Hoffa v. United States*, 385 U.S. 293, 301 (1966) ("A hotel room can clearly be the object of Fourth Amendment protection as much as a home or an office."); *United States v. Young*, 573 F.3d 711, 716 (9th Cir. 2009) ("Part of what a person purchases

when he leases a hotel room is privacy for one's person and one's things."). The government did not contend otherwise below.[199] Thus, Polequaptewa had standing to challenge an unconstitutional entry into his hotel room.

If the factual disputes about the circumstances surrounding the deputies' entry into Polequaptewa's hotel room and the seizure of his laptop are ultimately resolved in his favor after a hearing, the entry violated the Fourth Amendment.[200] But the district court, following the government's lead,[201] jumped past Polequaptewa's undisputed Fourth Amendment interest in his hotel room to whether he also had an independent Fourth Amendment interest in the seized laptop.[202] Doing so ignored that the exclusionary rule encompasses both evidence seized during an unlawful search and any indirect products of such invasions—so-called "fruit of the poisonous tree." *United States v. Gorman*, 859 F.3d 706, 716 (9th Cir. 2017); *see also United States v. Pulliam*, 405 F.3d 782, 785 (9th Cir. 2005) ("The exclusionary rule reaches not only primary evidence obtained as a direct result of an illegal search or seizure, but also evidence later discovered and

---

[199] ER 109-37.

[200] *Infra* Part C.

[201] ER 125-27.

[202] ER 6-8.

found to be derivative of an illegality or fruit of the poisonous tree. It extends as well to the indirect as the direct products of unconstitutional conduct.") (citation and quotation marks omitted). Because the laptop was the evidentiary fruit of the entry into Polequaptewa's hotel room, any evidence obtained from the laptop should have been suppressed if that entry was unlawful.

The district court accepted at face value the government's claim that Polequaptewa "stole" the laptop by not returning it to a previous employer when he was fired, and it cited two cases for the proposition that "a defendant does not have a reasonable expectation of privacy in stolen property."[203] First, it pointed to *United States v. Wong*, where (with little analysis) the Court asserted that a "laptop searched belonged to Wong's former employer" so he did "not have standing to object to the search of that laptop because he failed to establish that he had a reasonable expectation of privacy in it." 334 F.3d 831, 838 (9th Cir. 2003). In contrast to the present case, however, the laptop in *Wong* was not the evidentiary fruit of a constitutional violation because the defendant had abandoned that laptop when he left it behind upon quitting his subsequent job. *Id*. at 835. And in *United States v. Caymen*, police found and seized a laptop when executing a search warrant for the defendant's home based on probable cause that the laptop had been

[203] ER 6-7.

fraudulently purchased from a store with another person's credit card. 404 F.3d 1196, 1197 (9th Cir. 2005). Police then got the store's consent to search the laptop's hard drive. *Id*. at 1198. Given evidence developed at an evidentiary hearing, the Court held that the district court didn't clearly err in finding that the laptop did not belong to the defendant and therefore he had no reasonable expectation of privacy in its contents. *Id*. at 1200-01. In doing so, however, the Court expressly noted that the laptop was in police possession pursuant to the valid search warrant, so that case did not raise questions about whether the laptop had been unconstitutionally seized before it was searched. *Id*. at 1199.

Unlike in *Wong* and *Caymen*, the laptop at issue here was the fruit of an unlawful entry into Polequaptewa's hotel room. He had Fourth Amendment standing to seek suppression of the laptop evidence derived from that constitutional violation regardless of whether he had independent standing to challenge the seizure and search of the laptop directly. Analogously, the Court has held that although a car passenger with no possessory interest in the vehicle doesn't have standing to challenge a search of the car directly, he may still argue that the evidence found during the car search was evidentiary fruit of his own illegal detention. *Pulliam*, 405 F.3d at 786-87; *United States v. Twilley*, 222 F.3d 1092, 1095 (9th Cir. 2000). Similarly, the Tenth Circuit has recognized that while a

person driving a stolen van "lacks standing to object to the search of the van, he has standing to object to his detention[,]" so if that "detention was illegal, evidence obtained as a result of that illegal detention must be excluded to the extent it was fruit of the poisonous tree." *United States v. Miller*, 84 F.3d 1244, 1250 (10th Cir. 1996), *overruled on other grounds*, *United States v. Holland*, 116 F.3d 1353 (10th Cir. 1997). These cases are consistent with "the principle that the relevant inquiry in determining whether a defendant has standing to challenge evidence as fruit of a poisonous tree is whether his or her Fourth Amendment rights were violated, not the defendant's reasonable expectation of privacy in the evidence alleged to be poisonous fruit." *United States v. Olivares-Rangel*, 458 F.3d 1104, 1117 (10th Cir. 2006). The district court ignored this principle when it erroneously concluded that Polequaptewa lacked standing to bring his suppression motion.

B. To the extent it matters whether Polequaptewa also had standing to directly challenge the seizure and search of the laptop (separate from his standing to challenge the unlawful entry into his hotel room), the district court erred in not holding an evidentiary hearing on that disputed issue.

Although Polequaptewa's standing to challenge the unlawful search of his hotel room is sufficient for him to prevail on his motion to suppress the laptop evidence,

the district court erred in finding that he did not also separately have a Fourth Amendment interest in the laptop itself. It could not properly make that finding without first holding an evidentiary hearing because the motion, opposition, and declarations established that there were contested facts pertaining to that issue. *See United States v. Cook*, 808 F.3d 1195, 1201 (9th Cir. 2015).

Polequaptewa's suppression motion was supported by his declaration, in which he stated that he told the deputies the laptop was not Blue Stone's property and they demanded proof of his ownership.[204] His sworn declaration states: "I tried to search for proof of ownership of *my computer*, but I could not find anything in my email at that time."[205] He also asserted that the deputies did not have a warrant "to seize *my computer*."[206] Polequaptewa also submitted an FBI search-warrant affidavit recounting William Moon's statement that Polequaptewa claimed the laptop "was his personal computer."[207] Consistent with this evidence, Polequaptewa's suppression motion repeatedly referred to "Defendant's laptop."[208] Thus, the district court wrongly wrote that "Defendant did not address his

---

[204] ER 104-05.

[205] ER 105 (emphasis added).

[206] ER 106 (emphasis added).

[207] ER 60.

[208] ER 31, 34, 38, 44, 47.

possessory or ownership interest in the [] laptop in his declaration or briefing on this motion."[209]

In an attempt to rebut Polequaptewa's claim that he owned the laptop, the government presented declarations from two employees of the University of California, Irvine (UCI).[210] These declarants claimed that Polequaptewa purchased the laptop using UCI funds when he worked there in July 2012.[211] Allegedly, his ownership interest in, and use of, the laptop was limited by UCI's policies,[212] but the government did not point to any particular relevant policy.[213] When Polequaptewa stopped working for UCI in March 2014, he was purportedly "required to return the laptop at that time, as documented in" his termination letter.[214] But that letter included only this general statement: "You are directed to immediately return all UC equipment, including without limitation computers, laptops, cell phone, other electronic devices and audio-visual equipment that is in

---

[209] ER 8.

[210] ER 146-83.

[211] ER 146, 149-50, 176-77, 182-83.

[212] ER 146, 152-54.

[213] ER 116-18.

[214] ER 146.

your possession."[215] It did not specifically mention the particular laptop at issue. Tellingly, UCI did not send a letter to Polequaptewa asking for the laptop's return, or even seek its own police department's help in retrieving that laptop, until January 2015—*after* the laptop had been seized from Polequaptewa in Florida and made its way to the FBI.[216] Thus, UCI's contention that it viewed the laptop as "stolen property"[217] was an after-the-fact judgment apparently manufactured at the government's behest.

In his reply, Polequaptewa reasserted his ownership interest in the laptop, noting that it was included among his "personal property" he was seeking in his civil-suit cross-claim against Blue Stone, where he had identified the computer as

---

[215] ER 157.

[216] ER 146-47, 174. That letter refers to the unreturned laptop as a "MacBook Pro, serial #CI2GX6SNDJQ5[.]" ER 174. A letter sent to Polequaptewa's wife on the same date refers to the same serial number. ER 172. But the serial number for the MacBook Pro at issue here is "CO2HX6SMDKQ5." ER 82, 115, 149, 182. The government tried to explain away this discrepancy in a footnote, claiming it's "clear that the typist shifted on certain parts of the serial number." ER 117. The declarants themselves never made such a claim, however. ER 146-47, 176-77. Those are the kind of details that must be flushed out at an evidentiary hearing.

[217] ER 147.

"Polequaptewa's personal laptop."[218] Thus, the district court wrongly wrote that Polequaptewa did "not contest that UCI is the rightful owner" of the laptop in his reply.[219]

Despite the factual dispute about who owned the laptop, the government asked the district court to rule without an evidentiary hearing, arguing that it should not have to make its declarants available for cross-examination because Polequaptewa didn't do more to contest UCI's purported ownership of the laptop.[220] Although Polequaptewa maintained that there should be an evidentiary hearing where the government's declarants could be cross-examined,[221] the district court refused based on its above-noted mischaracterizations of his declaration, motion, and reply.[222]

This Court's precedent doesn't allow a party to submit, and a court to rely on, a declaration as proof of a contested fact without giving the opposing party the opportunity to question the witness about that fact. "Cross-examination is the principal means by which the believability of a witness and the truth of his

---

[218] ER 193.

[219] ER 8.

[220] ER 116, 126-27, 197-200.

[221] ER 200.

[222] ER 1-8.

testimony are tested." *Davis v. Alaska*, 415 U.S. 308, 316 (1974). Indeed, courts have described cross-examination as "the greatest legal engine ever invented for the discovery of truth." *Winzer v. Hall*, 494 F.3d 1192, 1197 (9th Cir. 2007) (quotation marks omitted). Thus, the "purpose of requiring an evidentiary hearing, rather than permitting a decision to be based solely on written declarations, is to ensure that the district judge is presented with the information necessary to evaluate the truthfulness of the declarants." *United States v. Mejia*, 69 F.3d 309, 318 (9th Cir. 1995). Therefore, once the government presented the UCI declarations to try to rebut Polequaptewa's claim that he owned the laptop, no more was necessary to establish his right to cross-examine the declarants.

Denying cross-examination under these circumstances infringed Polequaptewa's constitutional rights. First and foremost, is the core right to suppression of the fruits of warrantless seizures and searches under the Fourth Amendment. And at hearings meant to safeguard that right, the denial of cross-examination violates the Due Process Clause. *See Ching v. Mayorkas*, 725 F.3d 1149, 1156 (9th Cir. 2013) ("'in almost every setting where important decisions turn on questions of fact, due process requires an opportunity to confront and cross-examine adverse witnesses.'"). It also implicates Confrontation Clause rights. *See United States v. Clark*, 475 F.2d 240, 246-47 (2d Cir. 1973)

(confrontation right applies at pretrial suppression hearing); *see also United States v. Campbell*, 743 F.3d 802, 808-09 (11th Cir. 2014) (citing *Clark* while leaving open whether Confrontation Clause applies to pretrial proceedings); *United States v. Stewart*, 93 F.3d 189, 192 & n.1 (5th Cir. 1996) ("we safeguard the right to cross-examine at the suppression hearing because the aims and interests involved in a suppression hearing are just as pressing as those in the actual trial."). As the D.C. Circuit explained:

> It is clear that a defendant has some right to cross-examine Government witnesses at a suppression hearing. For two centuries judges and lawyers have regarded the opportunity of cross-examination as an essential safeguard of the accuracy and completeness of testimony. Thus cross-examination is not a mere privilege but is the right of the party against whom a witness is offered. The adversary procedure of suppression hearings is well established in the federal courts, and there is no suggestion before us that a District Court could totally eliminate a defendant's right of cross-examination at this stage of the criminal proceedings. Indeed, the suppression hearing is a critical stage of the prosecution which affects substantial rights of an accused person; the outcome of the

> hearing—the suppression vel non of evidence—may often determine the eventual outcome of conviction or acquittal. Thus, whether we describe the right of cross-examination as deriving from the fundamental concepts embedded in the Due Process Clause or as implicit in the rules governing federal criminal proceedings, we have no doubt of the applicability of the right here or of its importance.

United States v. Green, 670 F.2d 1148, 1154 (D.C. Cir. 1981) (citations and quotation marks omitted).

Notably, even if the UCI declarations accurately described how the laptop was purchased, that isn't inconsistent with Polequaptewa having a proprietary interest or an expectation of privacy in it. By not seeking the laptop's return (at least until after it had already been seized and given to the FBI), UCI effectively abandoned its proprietary interest the laptop. In fact, a UCI declaration reflects that the Polequaptewas returned another university laptop when asked,[223] suggesting there was a legitimate reason the laptop at issue was kept. Indeed, Polequaptewa's wife explained at trial that when her husband left UCI, the university gave him a list of items to return that did not include that laptop, and UCI signed off on that list.[224]

---

[223] ER 146.

[224] ER 1116.

At a minimum, Polequaptewa still had an expectation of privacy in the laptop. This situation is somewhat akin to circumstances where a person continues to retain an expectation of privacy in a hotel room past checkout time. *See United States v. Dorias*, 241 F.3d 1124, 1128-29 (9th Cir. 2001) ("[T]he mere expiration of the rental period, in the absence of affirmative acts of repossession by the lessor, does not automatically end a lessee's expectations of privacy.); *cf. United States v. Bautista*, 362 F.3d 584, 590-91 (9th Cir. 2004) (defendant retained expectation of privacy where "motel's manager took no affirmative steps to repossess the room once she learned that it had been reserved with a stolen credit card."). Or in a rental car kept past its return deadline. *See United States v. Henderson*, 241 F.3d 638, 647 (9th Cir. 2000) (defendant had standing to challenge search of rental car even though rental agreement expired because rental-car company made no attempt to repossess the car). The devil is in the details, so to speak, so cross-examination of the UCI witnesses is necessary before any court can find that Polequaptewa did not have Fourth Amendment standing as to the laptop. *See Graham v. State*, 47 Md.App. 287, 294 (1980) ("There may well be situations, for example, in which the unlawfulness of an initial acquisition can become attenuated by other factors, such as the length of time the article is in the defendant's exclusive possession, or an honest, though mistaken, belief that the object in

question actually belongs to him—that his acquisition of it was not unlawful."). Furthermore, because (as discussed in the next section) an evidentiary hearing is required as to the other unresolved suppression issues anyway, there's no reason to not have the district court delve into this matter on remand as well.

C. An evidentiary hearing into the remaining suppression issues not reached by the district court is also necessary.

Because of its faulty standing ruling, the district court didn't reach the merits of the suppression issues, all of which require a suppression hearing.

"[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are per se unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions." *Arizona v. Gant*, 556 U.S. 332, 338 (2009) (quotation marks omitted). The government therefore bears the burden to prove that police officers' actions fell within one of these exceptions. *United States v. Job*, 871 F.3d 852, 860 (9th Cir. 2017). The government raised two such exceptions—consent and emergency aid.

Consent is a "jealously and carefully drawn exception" to the Fourth Amendment's warrant requirement. *Georgia v. Randolf*, 547 U.S. 103, 109 (2006) (quotation marks omitted). Although Deputy Hall's declaration claimed that Polequaptewa consented to him taking the laptop (and was conspicuously silent on

how he entered the hotel room),[225] Polequaptewa's declaration stated unequivocally that he did not consent to the deputies entering his hotel room, that he opened the door only because the deputies threatened to break down the door otherwise, that the deputies then pushed their way into the room and refused his requests for them to leave, and that he let the deputies take the laptop only because they threatened to take him to jail if he did not.[226] Although officers may initiate a consensual encounter by knocking on a person's hotel-room door, "coercive circumstances" like announcing "police" while knocking, being "unreasonably persistent" in the attempt to gain access to the room, and commanding or otherwise compelling the person "to open the door under the badge of authority" render the encounter involuntary. *United States v. Crasper*, 472 F.3d 1141, 1145-46 (9th Cir. 2007) (quotation marks omitted); *see also Bautista*, 362 F.3d at 591 (officers effectuate a search when they gain visual or physical entry by commanding door be opened under claim of lawful authority); *United States v. Spotted Elk*, 548 F.3d 641, 655 (8th Cir. 2008) ("[A] police attempt to 'knock and talk' can become

---

[225] ER 184-90; *supra* Statement of the Case, Part 2.A.2.

[226] ER 103-06; *supra* Statement of the Case, Part 2.A.1. As noted above, the trial testimony of William Moon and Polequaptewa's wife is also inconsistent with Hall's consent story. *Supra* Statement of the Case, Parts 2.A.3 & 2.A.4.

coercive if the police assert their authority, refuse to leave, or otherwise make the people inside feel they cannot refuse to open up[.]"). Thus, an evidentiary hearing is required to resolve the factual dispute about consent.

"The emergency aid exception permits law enforcement officers to enter a home without a warrant to render emergency assistance to an injured occupant or to protect an occupant from imminent injury." *Bonivert v. City of Clarkston*, 883 F.3d 865, 876 (9th Cir. 2018) (quotation marks omitted). The officers must have "an objectively reasonable basis for believing that an *actual or imminent injury* was unfolding in the place to be entered." *Id*. at 877 (emphasis in original). The government "bear[s] a heavy burden when attempting to demonstrate an urgent need that might justify warrantless searches or arrests because the emergency exception is narrow and rigorously guarded." *Id*. at 876-77 (citation and quotation marks omitted). In particular, the government must proffer "specific and articulable facts to justify invoking the exception[.]" *Sandoval v. Las Vegas Metropolitan Police Department*, 756 F.3d 1154, 1164 (9th Cir. 2014) (quotation marks omitted). A court must then determine whether: "(1) considering the totality of the circumstances, law enforcement had an objectively reasonable basis for concluding that there was an immediate need to protect others or themselves from serious harm; and (2) the search's scope and manner were reasonable to meet the

need." *Ames v. King County, Washington*, 846 F.3d 340, 350 (9th Cir. 2017) (quotation marks omitted). An evidentiary hearing into "the totality of the circumstances" here is required. Hall claimed he needed to make sure Polequaptewa "was alive" and would not "do harm to himself or his family" because he "was in a new state, no longer had a job, and his former employer was accusing him of engaging in fraud."[227] Those facts don't provide an objectively reasonable basis to believe that an actual or imminent injury was unfolding within the room. At a minimum, Hall must be cross-examined about exactly what information he had and when, particularly given the trial testimony of William Moon (who summoned the police), who stated unequivocally that he was only concerned about the data deletions purportedly being accomplished via the laptop and not Polequaptewa's well-being,[228] and presumably told Hall the same. Finally, even taken at face value, Hall's report and declaration reflect that he dispelled any concern about Polequaptewa's mental state *before* turning to the dispute between

[227] ER 184-85, 190.

[228] ER 465, 496, 500-03, 514; *supra* Statement of the Case, Part 2.A.3.

Moon and Polequaptewa over the laptop.[229] At that point, the emergency-aid exception no longer even arguably applied. *Id*.

The government also argued that, to the extent the Fourth Amendment was violated, the independent-source and good-faith exceptions to the exclusionary rule applied.[230] Again, the government bears the burden to prove each of these exceptions. *See United States v. Camou*, 773 F.3d 932, 944 (9th Cir. 2014) (good faith); *cf. United States v. Reilly*, 224 F.3d 986, 994 (9th Cit. 2000) (inevitable discovery). "[T]he independent source doctrine asks whether the evidence *actually* was obtained independently from activities untainted by the initial illegality." *United States v. Lundin*, 817 F.3d 1151, 1161 (9th Cir. 2016) (emphasis in original) (quotation marks omitted). And the "test for good faith is an objective one: whether a reasonably well trained officer would have known that the search was illegal *in light of all the circumstances*." *Camou*, 773 F.3d at 944 (emphasis added) (quotation marks omitted). These are factual inquiries, yet the government offered no affidavits to support its exclusionary-rule-exception arguments.

---

[229] ER 184-90; *supra* Statement of the Case, Part 2.A.2; *see also* ER 121, 130 (government conceding this point).

[230] ER 132-36.

Assuming the government even proffered enough to put these exceptions at issue, an evidentiary hearing into all the relevant facts is necessary.

Finally, even if the record were fully developed as to any of these issues, the district court did not make findings as to them. "When factual issues are involved in deciding a motion, the [district] court must state its essential findings on the record." Fed. R. Crim. P. 12(d). This rule is mandatory. *United States v. Prieto-Villa*, 910 F.2d 601, 607-10 (9th Cir. 1990). "Essential factual findings are those which will permit appellate review of the legal questions involved." *Id*. at 610. The Court must remand for the district court to make the necessary findings; it cannot simply engage in "appellate fact-finding" to resolve the disputes itself. *Id*. at 608-10.

D. The Court should reverse Polequaptewa's conviction and remand for a new trial.

Because the district court erroneously denied Polequaptewa's suppression motion and therefore allowed the government to present evidence obtained from the laptop without first making the findings necessary to determine that the evidence was admissible, the Court should vacate his conviction and remand for a new trial.

In *United States v. Christian*, the Court concluded that the district court improperly excluded defense-proffered expert testimony because it erred in its gatekeeping function by applying the wrong analysis. 749 F.3d 806, 810-13 (9th Cir. 2014). Because the expert would have bolstered the defendant's diminished-capacity defense, exclusion of that evidence couldn't be dismissed as harmless. *Id*. at 813. Even though the Court recognized that, on remand, the district court might still exclude the expert testimony after a proper hearing, it still determined that reversal of the defendant's conviction and a remand for a new trial was the appropriate remedy. *Id*. at 813-14. It followed precedent holding that "a new trial is warranted when evidence admitted through an erroneous analysis prejudices the opposing party but the record is too sparse to conduct a proper admissibility analysis and decide whether the admission itself was erroneous." *Id*. at 813. The Court extended that precedent to criminal cases and to cases where evidence was erroneously excluded, rather than admitted. *Id*. at 814.

Christian applies here. Until the district court holds an evidentiary hearing and makes the required factual findings, "the record is too sparse to conduct a proper admissibility analysis" under the Fourth Amendment to "decide whether the admission [of the laptop evidence] itself was erroneous[,]" but the Court can and should find that that evidence was "admitted through an erroneous analysis[.]" 749

F.3d at 813. And, as in *Christian*, the admission of that evidence caused the requisite prejudice because it wasn't harmless. *Id*. The government bears the burden to prove a constitutional error harmless beyond a reasonable doubt. *United States v. Lustig*, 830 F.3d 1075, 1091 (9th Cir. 2016). Reversal is required under that standard because "there is a reasonable possibility that the evidence complained of might have contributed to the conviction." *Chapman v. California*, 386 U.S. 18, 23-24 (1967) (quotation marks omitted). As detailed above, the forensic examination of Polequaptewa's laptop—the tool he purportedly used to delete most of the data—was central to the government's case.[231] Under these circumstances, the government can't meet its burden to prove beyond a reasonable doubt that the evidence did not contribute to the jury's verdict. The Court should therefore reverse Polequaptewa's conviction and remand for the district court to first hold a hearing on the suppression motion and then hold a new trial regardless of the ruling on the suppression motion.

[231] *Supra* Statement of the Case, Part 3.

2. The Court should reverse Polequaptewa's conviction and remand for a new trial because the district court plainly erred in failing to properly instruct the jury about the element that increased the charged crime from a misdemeanor to a felony.

The indictment required the government to prove beyond a reasonable doubt that the offense (wiping the Mac Pro desktop computer) and "a related course of conduct" caused at least $5,000 in loss.[232] The district court plainly erred in failing to properly instruct the jury about this element, which increased the charged crime from a misdemeanor to a felony.

A. To understand where the district court went wrong, the Court must apply the canons of statutory construction to 18 U.S.C. §1030.

1. Interpretation begins with the statutory text, and unless otherwise defined, terms are generally given their ordinary meaning. *Sebelius v. Cloer*, 569 U.S. 369, 376 (2013). Moreover, a statute's language cannot be construed in a vacuum; its words must be read in context and in light of their place in the overall statutory scheme. *Sturgeon v. Frost*, 136 S.Ct. 1061, 1070 (2016).

---

[232] *Supra* Statement of the Case, Part 1.

Polequaptewa was charged with violating §1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I).[233] Section §1030(a)(5)(A) provides that whoever "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer ... shall be punished as provided in subsection (c)[.]" That subsection makes this crime a misdemeanor unless certain additional conditions are satisfied. 18 U.S.C. §1030(c)(4)(G)(i). Polequaptewa was charged with a felony under §1030(c)(4)(B)(i), which increases the maximum sentence from one year to ten years "if the offense caused" specific kinds of harms. And under §1030(c)(4)(A)(i)(I), the alleged harm was "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[.]"

The superseding indictment charged a single crime because any fact that increases the statutory penalty is an "element" of the offense such that "the core crime" and the fact triggering the higher sentence "together constitute a new, aggravated crime[.]" *Alleyne v. United States*, 570 U.S. 99, 108, 113 (2013). But

---

[233] ER 235-39.

that's not the way it was presented to the jury. It was instructed that it could find Polequaptewa guilty of violating §1030(a)(5)(A) as "charged in the single-count First Superseding Indictment"—the core misdemeanor crime—if the government proved three elements beyond a reasonable doubt: (1) that he knowingly caused the transmission of a program, a code, a command, or information to the Mac Pro desktop computer; (2) that, as a result of the transmission, he intentionally impaired, without authorization, the integrity or availability of data, a program, a system, or information; and (3) that the Mac Pro desktop computer was used in or affected interstate or foreign commerce or communication.[234] The district court separately instructed the jury that if it found Polequaptewa guilty of that offense, it would then have to decide 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"—the fact triggering

[234] ER 18-19, 1225.

the higher sentence.[235] The jury found Polequaptewa guilty of the core misdemeanor crime and made the loss finding.[236]

"Loss" was defined as "any reasonable cost to Blue Stone Strategy Group including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[237] What constituted a "related course of conduct" was never explained, however.[238] But the jury was generally instructed that it was there only to determine whether the defendant is guilty or not guilty of "the charge in the First Superseding Indictment" because he was "not on trial for any conduct or offense not charged" therein.[239] Again, the jury was told immediately after that that the charge "in the single-count First Superseding Indictment" was only the core misdemeanor crime set forth in §1030(a)(5)(A) with the three elements set forth above.[240] Thus, the clear implication was that whatever

---

[235] ER 20, 1229; *supra* footnote 13.

[236] ER 1202-05, 1255-57.

[237] ER 20-21, 1229.

[238] ER 10-26, 1209-36.

[239] ER 17, 1223.

[240] ER 18-19, 1225.

a "related course of conduct" was, it had nothing to do with these elements. That was wrong.

Section §1030 doesn't define "related course of conduct," but that phrase must be read in context: "the offense caused ... loss to 1 or more persons during any 1-year period []and ... loss resulting from a related course of conduct affecting 1 or more other protected computers[] aggregating at least $5,000 in value[.]" 18 U.S.C. §1030(c)(4)(A)(i)(I). Thus, the "course of conduct" must be "related" to "the offense." The plain meaning of this language has three consequences. First, each step of the course of conduct must be equivalent to the offense—in other words, here, the government had to prove that each additional alleged transmission of a command satisfied all three elements of the core §1030(a)(5)(A) crime. Second, the government also had to prove all of these transmissions were related, plainly meaning so connected that each individual act was part of a single episode with a common purpose. Finally, because §1030(a)(5)(A) requires the defendant to "intentionally cause damage[,]" it necessarily follows that the §1030(c)(4)(i)(I) felony enhancement requires his intent to cause at least $5,000 in loss. Other statutory-construction canons support these plain-language interpretations.

2. The rule of lenity requires resolving any ambiguity in §1030 in Polequaptewa's favor. *United States v. Davis*, 139 S.Ct. 2319, 2333 (2019). To

the extent the government can proffer any contrary plausible interpretation of §1030, that would simply render the statute ambiguous. And in that case, the "tie must go to the defendant." *United States v. Santos*, 553 U.S. 507, 514 (2008) (rule of lenity requires adopting most "defendant-friendly" of any plausible interpretations).

3. Finally, the doctrine of constitutional avoidance encompasses at least two different canons of construction applicable here: first, the Court should, if possible, interpret an ambiguous statute to avoid rendering it unconstitutional; and second, the Court should construe an ambiguous statute to avoid the need even to address serious questions about its constitutionality. *Davis*, 139 S.Ct. at 2332 n.6. The "doctrine prohibiting the enforcement of vague laws rests on the twin constitutional pillars of due process" (because "statutes must give people of common intelligence fair notice of what the law demands of them") and "separation of powers" (because "[o]nly the people's elected representatives in the legislature are authorized to make an act a crime"). *Id.* at 2325 (quotation marks omitted). "Vague statutes threaten to hand responsibility for defining crimes to relatively unaccountable police, prosecutors, and judges, eroding the people's ability to oversee the creation of the laws they are expected to abide." *Id*. If §1030 isn't given the defense-friendly interpretation demanded by its plain language, the

statute is unconstitutionally vague in that it deprived Polequaptewa of fair notice of exactly what conduct would make him guilty of a felony under §1030(a)(5)(A), (c)(4)(B)(i), (c)(4)(A)(i)(I), and it improperly allows unaccountable police, prosecutors, and judges to decide after the fact whether he engaged in such conduct.

B. The foregoing arguments establish not only that the district court erred in failing to instruct the jury about the felony-enhancement element but also that the error was "clear or obvious, rather than subject to reasonable dispute." *United States v. Wang*, 944 F.3d 1081, 1088 (9th Cir. 2019) (quotation marks omitted). "An appellate case need not answer the precise question to show plain error." *Id*. at 1089. "The clear text and structure of a statute ... may also suffice to show plain error." *Id*. Polequaptewa's argument is based on the plain language of §1030, supported by the rule of lenity and the constitutional-avoidance doctrine.

C. The instructional error affected Polequaptewa's substantial rights because there's a reasonable probability that it affected the outcome of the trial. *United States v. Garrido*, 713 F.3d 985, 995 (9th Cir. 2013); *see also United States v. Tydingco*, 909 F.3d 297, 304 (9th Cir. 2018) (prejudice "requires some intermediate level of proof that the error affected the outcome at trial: more than a mere possibility, ... but less than a preponderance[.]"); *United States v. Bear*, 439

F.3d 565, 570 (9th Cir. 2006) (substantial rights affected where erroneous instructions create "genuine possibility" that jury convicted on legally-inadequate ground); *United States v. Alferahin*, 433 F.3d 1148, 1157-58 (9th Cir. 2006) (substantial rights affected unless "strong and convincing evidence" on missing element). As discussed above, the evidence pertaining to the core misdemeanor crime of wiping the Mac Pro desktop (via a single command issued at one discrete moment) was distinct from the evidence pertaining to the felony enhancement (based on a series of many commands to multiple computers over an extended period of time).[241] If the jury had been informed that it had to find each of the elements for each and every one of those additional commands, it might have concluded that others (like William Moon or Eldad Yacobi) were responsible for some or all of those commands, or that Polequaptewa issued some of the commands accidentally. And if the jury had been informed that any commands attributable to Polequaptewa were related only if they were all part of a single episode with a common purpose, it might have concluded that the wipe command to the Mac Pro was distinct enough from the other commands in time and/or in nature to render them unrelated. And because the Blue Stone witnesses didn't

[241] *Supra* Statement of the Case, Part 3.

break down the loss resulting from each individual command,[242] the jury would have been unable to determine if the $5,000 loss threshold was crossed once it disregarded any of the commands. Furthermore, although the government presented evidence that the purported course of conduct caused a certain amount of loss, it didn't even try to prove that Polequapetwa intended to cause at least $5,000 in loss. For all these reasons, there's a reasonable probability the instructional error affected the verdict.

D. Finally, because the faulty instructions allowed the jury to rely on a legally-invalid theory to convict Polequaptewa and a properly-instructed jury probably wouldn't have found him guilty, the error seriously affects the fairness, integrity, or public reputation of judicial proceedings. *Tydingco*, 909 F.3d at 306; *Garrido*, 713 F.3d at 998; *Bear*, 439 F.3d at 570-71; *Alferahin*, 433 F.3d at 1159-60. The Court should therefore reverse his conviction and remand for a new trial.

---

[242] ER 296-98, 306, 320-25, 623-32, 678, 698-705, 711-12, 795-97, 847-49, 1242-43.

Conclusion

The Court should reverse the denial of Polequaptewa's suppression motion, reverse his conviction, and remand for a new trial after a suppression hearing.

July 7, 2020

Respectfully submitted,

CUAUHTEMOC ORTEGA
Interim Federal Public Defender

/s/ *James H. Locklin*
JAMES H. LOCKLIN
Deputy Federal Public Defender

Certificate of Related Cases

Counsel for appellant is unaware of any cases currently pending in this Court that are related for purposes of Circuit Rule 28-2.6.

July 7, 2020

/s/ *James H. Locklin*
JAMES H. LOCKLIN
Deputy Federal Public Defender

Counsel for Defendant-Appellant

Certificate of Compliance re Brief Length

Pursuant to Federal Rule of Appellate Procedure 32(a)(7)(C), I hereby certify that: the foregoing brief uses 14 point Times New Roman proportionately spaced type; text is double spaced and footnotes are single spaced; a word count of the word processing system used to prepare the brief indicates that the brief (not including the table of contents, the table of authorities, the statement of related cases, the certificate of compliance re brief length, the addendum, or the certificate of service) contains approximately 13,977 words.

July 7, 2020

/s/ *James H. Locklin*
JAMES H. LOCKLIN
Deputy Federal Public Defender

Counsel for Defendant-Appellant

Addendum

United States Code Annotated
Constitution of the United States
Annotated
Amendment IV. Searches and Seizures; Warrants

U.S.C.A. Const. Amend. IV-Search and Seizure; Warrants

Amendment IV. Searches and Seizures; Warrants

Currentness

The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

<Historical notes and references are included in the full text document for this amendment.>

<For Notes of Decisions, see separate documents for this amendment.>

U.S.C.A. Const. Amend. IV-Search and Seizure; Warrants, USCA CONST Amend. IV-Search and Seizure; Warrants
Current through P.L. 116-145.

End of Document

United States Code Annotated
Title 18. Crimes and Criminal Procedure (Refs & Annos)
Part I. Crimes (Refs & Annos)
Chapter 47. Fraud and False Statements (Refs & Annos)

18 U.S.C.A. § 1030

§ 1030. Fraud and related activity in connection with computers

Effective: November 16, 2018
Currentness

(a) Whoever--

(1) having knowingly accessed a computer without authorization or exceeding authorized access, and by means of such conduct having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations, or any restricted data, as defined in paragraph y. of section 11 of the Atomic Energy Act of 1954, with reason to believe that such information so obtained could be used to the injury of the United States, or to the advantage of any foreign nation willfully communicates, delivers, transmits, or causes to be communicated, delivered, or transmitted, or attempts to communicate, deliver, transmit or cause to be communicated, delivered, or transmitted the same to any person not entitled to receive it, or willfully retains the same and fails to deliver it to the officer or employee of the United States entitled to receive it;

(2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains--

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

(B) information from any department or agency of the United States; or

(C) information from any protected computer;

(3) intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, accesses such a computer of that department or agency that is exclusively for the use of the Government of the United States or, in the case of a computer not exclusively for such use, is used by or for the Government of the United States and such conduct affects that use by or for the Government of the United States;

(4) knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;

(5)(A) knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;

(B) intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage; or

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss. [1]

(6) knowingly and with intent to defraud traffics (as defined in section 1029) in any password or similar information through which a computer may be accessed without authorization, if--

(A) such trafficking affects interstate or foreign commerce; or

(B) such computer is used by or for the Government of the United States; [2]

(7) with intent to extort from any person any money or other thing of value, transmits in interstate or foreign commerce any communication containing any--

(A) threat to cause damage to a protected computer;

(B) threat to obtain information from a protected computer without authorization or in excess of authorization or to impair the confidentiality of information obtained from a protected computer without authorization or by exceeding authorized access; or

(C) demand or request for money or other thing of value in relation to damage to a protected computer, where such damage was caused to facilitate the extortion;

shall be punished as provided in subsection (c) of this section.

(b) Whoever conspires to commit or attempts to commit an offense under subsection (a) of this section shall be punished as provided in subsection (c) of this section.

(c) The punishment for an offense under subsection (a) or (b) of this section is--

(1)(A) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(1) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than twenty years, or both, in the case of an offense under subsection (a)(1) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(2)(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(B) a fine under this title or imprisonment for not more than 5 years, or both, in the case of an offense under subsection (a)(2), or an attempt to commit an offense punishable under this subparagraph, if--

(i) the offense was committed for purposes of commercial advantage or private financial gain;

(ii) the offense was committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or

(iii) the value of the information obtained exceeds $5,000; and

(C) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(2), (a)(3) or (a)(6) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(3)(A) a fine under this title or imprisonment for not more than five years, or both, in the case of an offense under subsection (a)(4) or (a)(7) of this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph; and

(B) a fine under this title or imprisonment for not more than ten years, or both, in the case of an offense under subsection (a)(4),[3] or (a)(7) of this section which occurs after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

(4)(A) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 5 years, or both, in the case of--

(i) an offense under subsection (a)(5)(B), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused)--

(I) 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;

(II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;

(III) physical injury to any person;

(IV) a threat to public health or safety;

(V) damage affecting a computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security; or

(VI) damage affecting 10 or more protected computers during any 1-year period; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(B) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 10 years, or both, in the case of--

(i) an offense under subsection (a)(5)(A), which does not occur after a conviction for another offense under this section, if the offense caused (or, in the case of an attempted offense, would, if completed, have caused) a harm provided in subclauses (I) through (VI) of subparagraph (A)(i); or

(ii) an attempt to commit an offense punishable under this subparagraph;

(C) except as provided in subparagraphs (E) and (F), a fine under this title, imprisonment for not more than 20 years, or both, in the case of--

(i) an offense or an attempt to commit an offense under subparagraphs (A) or (B) of subsection (a)(5) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(D) a fine under this title, imprisonment for not more than 10 years, or both, in the case of--

(i) an offense or an attempt to commit an offense under subsection (a)(5)(C) that occurs after a conviction for another offense under this section; or

(ii) an attempt to commit an offense punishable under this subparagraph;

(E) if the offender attempts to cause or knowingly or recklessly causes serious bodily injury from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for not more than 20 years, or both;

(F) if the offender attempts to cause or knowingly or recklessly causes death from conduct in violation of subsection (a)(5)(A), a fine under this title, imprisonment for any term of years or for life, or both; or

(G) a fine under this title, imprisonment for not more than 1 year, or both, for--

(i) any other offense under subsection (a)(5); or

(ii) an attempt to commit an offense punishable under this subparagraph.

[(5) Repealed. Pub.L. 110-326, Title II, § 204(a)(2)(D), Sept. 26, 2008, 122 Stat. 3562]

(d)(1) The United States Secret Service shall, in addition to any other agency having such authority, have the authority to investigate offenses under this section.

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage, foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

(3) Such authority shall be exercised in accordance with an agreement which shall be entered into by the Secretary of the Treasury and the Attorney General.

(e) As used in this section--

(1) the term "computer" means an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device;

(2) the term "protected computer" means a computer--

(A) exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or

(B) which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States;

(3) the term "State" includes the District of Columbia, the Commonwealth of Puerto Rico, and any other commonwealth, possession or territory of the United States;

(4) the term "financial institution" means--

(A) an institution, with deposits insured by the Federal Deposit Insurance Corporation;

(B) the Federal Reserve or a member of the Federal Reserve including any Federal Reserve Bank;

(C) a credit union with accounts insured by the National Credit Union Administration;

(D) a member of the Federal home loan bank system and any home loan bank;

(E) any institution of the Farm Credit System under the Farm Credit Act of 1971;

(F) a broker-dealer registered with the Securities and Exchange Commission pursuant to section 15 of the Securities Exchange Act of 1934;

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3) of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) of the Federal Reserve Act;

(5) the term "financial record" means information derived from any record held by a financial institution pertaining to a customer's relationship with the financial institution;

(6) the term "exceeds authorized access" means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter;

(7) the term "department of the United States" means the legislative or judicial branch of the Government or one of the executive departments enumerated in section 101 of title 5;

(8) the term "damage" means any impairment to the integrity or availability of data, a program, a system, or information;

(9) the term "government entity" includes the Government of the United States, any State or political subdivision of the United States, any foreign country, and any state, province, municipality, or other political subdivision of a foreign country;

(10) the term "conviction" shall include a conviction under the law of any State for a crime punishable by imprisonment for more than 1 year, an element of which is unauthorized access, or exceeding authorized access, to a computer;

(11) the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; and

(12) the term "person" means any individual, firm, corporation, educational institution, financial institution, governmental entity, or legal or other entity.

(f) This section does not prohibit any lawfully authorized investigative, protective, or intelligence activity of a law enforcement agency of the United States, a State, or a political subdivision of a State, or of an intelligence agency of the United States.

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses [4] (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

(h) The Attorney General and the Secretary of the Treasury shall report to the Congress annually, during the first 3 years following the date of the enactment of this subsection, concerning investigations and prosecutions under subsection (a)(5).

(i)(1) The court, in imposing sentence on any person convicted of a violation of this section, or convicted of conspiracy to violate this section, shall order, in addition to any other sentence imposed and irrespective of any provision of State law, that such person forfeit to the United States--

(A) such person's interest in any personal property that was used or intended to be used to commit or to facilitate the commission of such violation; and

(B) any property, real or personal, constituting or derived from, any proceeds that such person obtained, directly or indirectly, as a result of such violation.

(2) The criminal forfeiture of property under this subsection, any seizure and disposition thereof, and any judicial proceeding in relation thereto, shall be governed by the provisions of section 413 of the Comprehensive Drug Abuse Prevention and Control Act of 1970 (21 U.S.C. 853), except subsection (d) of that section.

(j) For purposes of subsection (i), the following shall be subject to forfeiture to the United States and no property right shall exist in them:

(1) Any personal property used or intended to be used to commit or to facilitate the commission of any violation of this section, or a conspiracy to violate this section.

(2) Any property, real or personal, which constitutes or is derived from proceeds traceable to any violation of this section, or a conspiracy to violate this section [5]

CREDIT(S)

(Added Pub.L. 98-473, Title II, § 2102(a), Oct. 12, 1984, 98 Stat. 2190; amended Pub.L. 99-474, § 2, Oct. 16, 1986, 100 Stat. 1213; Pub.L. 100-690, Title VII, § 7065, Nov. 18, 1988, 102 Stat. 4404; Pub.L. 101-73, Title IX, § 962(a)(5), Aug. 9, 1989, 103 Stat. 502; Pub.L. 101-647, Title XII, § 1205(e), Title XXV, § 2597(j), Title XXXV, § 3533, Nov. 29, 1990, 104 Stat. 4831, 4910, 4925; Pub.L. 103-322, Title XXIX, § 290001(b) to (f), Sept. 13, 1994, 108 Stat. 2097-2099; Pub.L. 104-294, Title II, § 201, Title VI, § 604(b)(36), Oct. 11, 1996, 110 Stat. 3491, 3508; Pub.L. 107-56, Title V, § 506(a), Title VIII, § 814(a)-(e), Oct. 26, 2001, 115 Stat. 366, 382-384; Pub.L. 107-273, div. B, Title IV, §§ 4002(b)(1), (12), 4005(a)(3), (d)(3), Nov. 2, 2002, 116 Stat. 1807, 1808, 1812, 1813; Pub.L. 107-296, Title XXII, § 2207(g), formerly Title II, § 225(g), Nov. 25, 2002, 116 Stat. 2158; renumbered § 2207(g), Pub.L. 115-278, § 2(g)(2)(I), Nov. 16, 2018, 132 Stat. 4178; amended Pub.L. 110-326, Title II, §§ 203, 204(a), 205 to 208, Sept. 26, 2008, 122 Stat. 3561, 3563.)

Footnotes

1 So in original. The period probably should be a semicolon.
2 So in original. Probably should be followed by “or”.
3 So in original. The comma probably should not appear.
4 So in original. Probably should be “subclause”.
5 So in original. A period probably should appear.

18 U.S.C.A. § 1030, 18 USCA § 1030
Current through P.L. 116-145.

End of Document