

UNITED STATES COURT OF APPEALS
FOR THE TENTH CIRCUIT

December 29, 2020

Christopher M. Wolpert
Clerk of Court

UNITED STATES OF AMERICA,

Plaintiff - Appellee,

v.

MICHAEL D. GOLIGHTLEY,

Defendant - Appellant.

No. 19-3135
(D.C. No. 6:18-CR-10097-JWB-1)
(D. Kan.)

ORDER AND JUDGMENT*

Before **HOLMES, SEYMOUR, and MORITZ**, Circuit Judges.

After Michael Golightley followed through on his threats to take down a website called Nex-Tech Classified, the government apprehended Golightley and charged him with seven counts of damaging a protected computer in violation of 18 U.S.C. § 1030(a)(5)(A) and one count of threatening to damage a protected computer in violation of 18 U.S.C. § 1030(a)(7). A jury convicted Golightley on all counts. At sentencing, the district court classified the seven counts for damaging a protected computer as felonies. It then sentenced Golightley to eight concurrent sentences of 27 months' imprisonment followed by two years of supervised release. Golightley

* This order and judgment is not binding precedent, except under the doctrines of law of the case, res judicata, and collateral estoppel. But it may be cited for its persuasive value. *See* Fed. R. App. P. 32.1(a); 10th Cir. R. 32.1(A).

appeals aspects of his convictions and sentence. For the reasons below, we affirm in part, reverse in part, and remand for resentencing.

Background

The government presented the following evidence at trial. Nex-Tech, a broadband and technology company headquartered in Lenora, Kansas, provides telecommunication services such as internet, phone service, cable TV, and advertising services. Its advertising services include a classified-ad website—Nex-Tech Classified—where users can buy and sell items online. Before using Nex-Tech Classified, an individual must become a registered user by providing a username, password, location, and email address. Customers can contact the help desk by phone, email, or through a form on the website.

On March 26, 2017, an individual created a Nex-Tech account under the username `grass_is_green`, identifying the user's location as Larned, Kansas, and providing the email address `ntcsucks@mail.com`. The user submitted listings seeking to sell several electronic items and a motorcycle and invited buyers to call or text an offer using a phone number ending in 1011. Nex-Tech removed the electronics listing because the description of the electronics suggested that the user had violated third-party intellectual-property rights, which in turn violated Nex-Tech's terms of service.

The following day, Nex-Tech's help desk received two threatening messages from `grass_is_green`, with a contact email address of `ntcsucks@mail.com`. The first message, at 10:24 p.m., stated:

take my ad down again when my description doesnt violate copy right, i will violate this site by bringing it offline, fix the ad. if u make me upset, i will retaliate, your choice, and im not making a threat im very capable of bringing down this website.

Supp. R. 34 (spelling and punctuation in original). The second message, sent eight minutes later, said:

ip address 24.225.8.90 will be submitted at exostress.in for 24 hours if my demands are not met with in 12 hours, your choice, and remember, you have been warned...

Id. at 35 (spelling and punctuation in original).

Following these threats, Nex-Tech deactivated grass_is_green's account and notified grass_is_green via email of the deactivation.

Several days later, the help desk received a call from someone who identified himself as the Wichita-based user water_is_blue. Nex-Tech had removed that user's electronics listing because it was essentially identical to grass_is_green's listing and therefore violated Nex-Tech's terms of service. During the call, Nex-Tech Classified went offline because of a distributed-denial-of-service, or DDoS, attack.¹ Over the next few days, a total of seven individual DDoS attacks overwhelmed Nex-Tech's and Nex-Tech Classified's websites and internal corporate systems. Nex-Tech employees recorded their time spent responding to these attacks, resulting in total labor costs to Nex-Tech of \$16,978.19.

¹ A DDoS attack "flood[s] an IP address with data" to render a site or service slow or unavailable. Aplt. Br. 4.

During its subsequent investigation, law enforcement analyzed Nex-Tech's internal records and determined that the user grass_is_green shared a location and phone number with another user, larned_seller. And the account for larned_seller provided a street address in Larned, Kansas, as well as the email address ninjagolightley@gmail.com. Law enforcement then determined that the street address for larned_seller was located within 200 yards of the IP addresses that communicated messages from grass_is_green to Nex-Tech. Accordingly, officers executed a search warrant at that address, and when the officers arrived, Golightley was the only person present. The search uncovered a computer, cell phone, and other items that connected Golightley to the accounts for grass_is_green and water_is_blue, the removed ads, and the threatening messages. Law enforcement also discovered that Golightley had accessed a service called DDoS City—a website that launches DDoS attacks—around the times of the attacks on Nex-Tech. The government charged Golightley with seven counts of damaging a protected computer and one count of threatening to damage a protected computer; the jury convicted him on all counts.

At sentencing, the district court classified the seven counts for damaging a protected computer as felonies, rather than misdemeanors, because the aggregate damage to the computers totaled more than \$5,000. It then sentenced Golightley to eight concurrent sentences of 27 months' imprisonment, followed by two years of supervised release. As part of Golightley's supervised release, the district court imposed two relevant special conditions. One condition empowers Golightley's probation officer to determine whether Golightley must inform certain third parties

that he poses a risk to them, and the other requires Golightley to take prescribed medication. Golightley appeals.

Analysis

Golightley raises four issues. He argues that the district court erred by (1) determining that the government produced sufficient evidence on the interstate-commerce element in the threat conviction; (2) classifying the seven counts for damaging a protected computer as felonies; (3) imposing a special condition of release empowering Golightley's probation officer to determine whether Golightley must inform third parties that he poses a threat; and (4) imposing a special condition of release requiring Golightley to take prescription medication. We address each issue in turn.

I. Interstate Commerce

Golightley first contends that the district court improperly denied his motion for acquittal with respect to his conviction for threatening to damage a protected computer. Specifically, he argues that the government's evidence at trial was insufficient to show that he transmitted a threat in interstate commerce.

We review challenges to the sufficiency of the evidence de novo. *United States v. Delgado-Uribe*, 363 F.3d 1077, 1081 (10th Cir. 2004). In doing so, we consider the evidence in the light most favorable to the government, asking whether a reasonable

juror could conclude that the evidence “establish[ed] each element of the crime.”² *Id.* (quoting *United States v. Vallo*, 238 F.3d 1242, 1247 (10th Cir. 2001)).

Threatening to damage a protected computer in violation of § 1030(a)(7)(A) requires the government to prove, among other elements, that Golightley transmitted at least one of his two threats “in interstate or foreign commerce.” § 1030(a)(7). But Golightley argues that the government failed to present evidence that would allow the jury to reasonably infer that he transmitted any threat in interstate commerce. Instead, he argues, the government merely showed that he transmitted his threats over the internet, which is insufficient to prove the interstate-commerce element.

The government concedes that Golightley’s use of the internet alone does not establish the interstate-commerce element. *See United States v. Kieffer*, 681 F.3d 1143, 1153 (10th Cir. 2012) (explaining that defendant’s transmission of material over internet does not, by itself, satisfy interstate-commerce element). Likewise, the

² Golightley acknowledges that his motion for acquittal below did not include the argument he presents on appeal. Accordingly, he forfeited such argument below, and we apply plain-error review on appeal. *See United States v. Goode*, 483 F.3d 676, 681 (10th Cir. 2007) (explaining that where acquittal motion challenges sufficiency of evidence on specific grounds, grounds not specified are forfeited and subject to plain-error review). To obtain relief under plain-error review, Golightley must demonstrate “(1) an error, (2) that is plain, which means clear or obvious under current law, and (3) that affects substantial rights. If he satisfies these criteria, [we] may exercise discretion to correct the error if it seriously affects the fairness, integrity, or public reputation of judicial proceedings.” *Id.* (quoting *United States v. Kimler*, 335 F.3d 1132, 1141 (10th Cir. 2003)). But if Golightley is correct that no reasonable juror could have convicted him of this crime, he will easily satisfy this four-pronged test; it is a “noncontroversial proposition that a conviction in the absence of sufficient evidence of guilt is plainly an error, clearly prejudiced the defendant, and almost always creates manifest injustice.” *Id.* at 681 n.1.

parties agree that Nex-Tech and its servers are located in Kansas and that Golightley transmitted his two threats from Kansas. Thus, the resolution of this issue depends on whether a reasonable jury could infer that one of Golightley's threats traveled through an out-of-state server.

The government points to two trial exhibits—Exhibits 4A and 5—as evidence that Golightley's threats traveled in interstate commerce via out-of-state servers. Exhibit 4A contains the two messages Golightley sent to Nex-Tech threatening to bring its website offline. The government contends that Golightley sent these messages from his personal email address, ntcucks@mail.com. Exhibit 5 shows automated correspondence from mail.com to Golightley that Golightley received after creating his ntcucks@mail.com email address. At the bottom of the email from mail.com is the following trademark notice:

mail.com is a registered trademark of 1&1 Mail & Media Inc., 701 Lee Road, Suite 300, Chesterbrook, PA 19087, USA.
© 2017. All rights reserved

Supp. R. 62.

The government first suggests Exhibit 4A establishes that Golightley transmitted the threats via his personal mail.com email address. Next, the government suggests that the jury could infer, based on the trademark notice in Exhibit 5, that mail.com's servers are located in Pennsylvania, or "in a [s]tate nearer Chesterbrook, Pennsylvania." Aplee. Br. 25. Lastly, the government builds on this inference, concluding the jury could infer that when Golightley transmitted his emails from his

mail.com account, the emails traveled in interstate commerce via mail.com's out-of-state servers.

But as we discuss below, the government's argument is fatally flawed because it assumes facts not in evidence. And even if we assumed such facts, the government's argument adopts inferences not permitted by that evidence.

First, as Golightley correctly points out, the government assumes that the messages in Exhibit 4A came from his personal mail.com email address. But Exhibit 4A does not support the government's assumption. The messages show that the sender used a form available on Nex-Tech Classified's online help desk. This form is completed by the user and submitted to Nex-Tech directly from its website. Both threats sent by `grass_is_green` show that they were sent from the email address "info@nextechclassifieds.com." Supp. R. 33–34. And Golightley's personal email address, `ntcsucks@mail.com`, appears only as the "Contact Email." *Id.* As Golightley further notes, given that the sender's email address is `info@nextechclassifieds.com`, the threatening messages appear to have originated from Nex-Tech's own website—meaning that, as Golightley explains, he transmitted the threats by completing an online form on Nex-Tech's website, and not by emailing Nex-Tech via his personal mail.com email address.³ Further, the government's expert witness—a federal

³ Nex-Tech's Help Desk Manager, Amy Normandin, identified Exhibit 4A as containing an "e[]mail between the user and the Help Desk staff." R. vol. 3, 323. But Normandin did not indicate the source of the email. Rather, she testified that "most users of the classified either use our chat system or e[]mail, *which is also available from the website.*" *Id.* at 311 (emphasis added).

forensics examiner who reviewed the digital evidence in this case—testified that someone using Golightley’s cell phone contacted Nex-Tech’s help desk at the time the threats were sent by visiting “the contact portion of the help page for Nex-Tech Classifieds.” R. vol. 3, 665.

Even when this evidence is viewed in the light most favorable to the government, no rational trier of fact could conclude that it shows Golightley sent the threats from his mail.com email address. And yet, the basic premise of the government’s argument is that the jury could infer the use of interstate commerce *because of* the use of the mail.com address. Given that this inference assumes facts not in evidence, the government did not produce sufficient evidence to show that Golightley transmitted his threats in interstate commerce. *See Cnty. Court v. Allen*, 442 U.S. 140, 167 (1979) (“[S]ince the prosecution bears the burden of establishing guilt, it may not rest its case entirely on a presumption unless the fact proved is sufficient to support the inference of guilt beyond a reasonable doubt.”). If anything, Exhibit 4A, coupled with the government’s own expert testimony, strongly suggest that Golightley’s threatening messages—though drafted by Golightley—were sent via Nex-Tech’s own website. And because it is undisputed that Nex-Tech’s servers are located in Kansas, Golightley’s threats would not have traveled in interstate commerce.

Moreover, even if we were to credit the government’s factual assumption that Golightley transmitted the threats from his mail.com account, that assumption wouldn’t bear the weight of the government’s inference that either threat traveled via

an out-of-state server. Specifically, the government suggests that, assuming Golightley used the mail.com account, the jury could have inferred that this email originated from or traveled through an out-of-state server. The government bases this inference on Exhibit 5's automated trademark notice stating that the corporate owner of the mail.com trademark is located in Pennsylvania. But the government offers no explanation tethering the location of the corporate trademark owner to the location of its servers. Nor does Exhibit 5 contain any information regarding the email servers, much less their location. Additionally, the government points to no other record evidence establishing the location of mail.com's email servers. Although the jury can make reasonable inferences without specific instruction or argument, the lack of evidence here precludes the jury from reasonably inferring the location of mail.com's email servers. *See Allen*, 442 U.S. at 167.

For these reasons, we conclude that even if the evidence established that Golightley sent his threats via his mail.com account, the jury could not have reasonably inferred that such emails travelled through non-Kansas servers simply because the holder of the mail.com trademark is located in Pennsylvania.⁴ *See Delgado-Uribe*, 363 F.3d at 1081. Because no reasonable juror could have

⁴ The government additionally argues that the jury instructions, which properly instructed the jury on the elements of § 1030(a)(7), cured any defects in the evidence. But we need not consider this argument because jury instructions have no bearing on the sufficiency of the evidence. *Musacchio v. United States*, 136 S. Ct. 709, 715 (2016) (“[S]ufficiency review . . . does not rest on how the jury was instructed.”).

determined that Golightley transmitted his threats in interstate commerce, we vacate his conviction for threatening to damage a protected computer.

II. Felony Classification

Next, Golightley argues that the jury instructions do not support the district court's decision to classify his seven convictions for damaging a protected computer as felonies. We review jury instructions *de novo*. In doing so, we consider the instructions "as a whole" and analyze whether they "correctly state the law and provide the jury with an understanding of the issues." *United States v. Gorrell*, 922 F.3d 1117, 1121–22 (10th Cir. 2019) (quoting *United States v. Little*, 829 F.3d 1177, 1181 (10th Cir. 2016)). And we will vacate a conviction only if there is "substantial doubt that the jury was fairly guided." *Id.* (quoting *Little*, 829 F.3d at 1181).

To determine whether the jury instructions correctly state the law, we begin by reviewing the statute of conviction—18 U.S.C. § 1030. This statute first describes the initial offense as damage to "a protected computer." § 1030(a). Subsection (c) then outlines punishments ranging from one year in prison for a misdemeanor offense to life imprisonment for a felony offense. § 1030(c). The classification of the offense and the corresponding punishment depend on various conditions outlined in the statute's subsections. Relevant here, subsection (c)(4) provides that an offense becomes a felony if, among other things, the defendant damaged one or more *other* computers; that is, a computer *other than* the computer that triggered the initial offense. § 1030(c)(4). Quoted more fully, this subsection provides that a conviction

for damaging a protected computer becomes a felony, punishable by up to ten years in prison, if the damage caused

loss to [one] or more persons during any [one]-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 [one] or more other protected computers) aggregating at least \$5,000 in value.

§ 1030(c)(4)(A)(i)(I). We refer to this subsection as the felony-loss provision. The parties agree that subsection (c)(4) is critical to their misdemeanor-versus-felony dispute. In other words, if Golightley’s conduct satisfies this felony-loss provision, then his convictions for damaging a protected computer are felonies; otherwise, his convictions are misdemeanors.⁵

Golightley points out that this is a prosecution brought by the United States, and thus the parenthetical language quoted above applies here. And, he argues, when that language is applied, his convictions can be felonies only if the jury found “loss resulting from a related course of conduct affecting [one] or more *other* protected computers.” § 1030(c)(4)(A)(i)(I) (emphasis added).

Notably, the government agrees that the parenthetical language is critical, explaining that Golightley’s convictions are felonies only “if the aggregate loss caused by the attacks upon Nex-Tech was the result of a ‘related course of conduct,’ i.e. a series of attacks caused by the defendant, *which affected one or more protected*

⁵ The parties dispute whether a conviction under § 1030(a)(5)(A) is by default a felony or a misdemeanor. But given that both parties agree that in this case, Golightley’s conviction becomes a felony only if the loss provision from § 1030(c)(4)(A)(i)(I) applies, this dispute is immaterial.

computers.” Aplee. Br. 33 (emphasis added) (quoting § 1030(c)(4)(A)(i)(I)). But it argues that, contrary to Golightley’s position, the instructions sufficiently communicated the parenthetical language.

And so we turn to the instructions. As Golightley points out, the instruction outlining the elements of the crime referenced only a single computer:

First: On or about the dates alleged . . . , [Golightley] knowingly caused the transmission of a program, information, code, or command to *a computer*;

Second: [Golightley], as a result of such conduct, intentionally caused damage to *a computer* without authorization; and

Third: *the computer* was used in or affected interstate commerce or communication.

R. vol. 1, 384 (emphases added). Thus, the elements instruction did not require the jury to find that Golightley’s conduct also affected one or more “other protected computers,” a finding necessary to satisfy the parenthetical language in § 1030(c)(4)(A)(i)(I). *See Banuelos-Galviz v. Barr*, 953 F.3d 1176, 1181 (10th Cir. 2020) (“[I]n most contexts, the singular article ‘a’ refers to only one item.”); *Colorado v. Sunoco, Inc.*, 337 F.3d 1233, 1241 (10th Cir. 2003) (noting that “the definite article ‘the’” connotes a single action (quoting 42 U.S.C. § 9613(g)(2)(A)–(B))).

Despite the absence of this statutory language in the elements instruction, the government insists that the felony-loss instruction remedied any concern. Relevant here, the felony-loss instruction stated:

If you recorded a guilty verdict on one or more counts set forth in the Indictment as [c]ounts [one] through [seven], you must also unanimously decide whether [Golightley’s] conduct in or related to any

of [c]ounts [one] through [seven] for which you recorded a guilty verdict caused an aggregate loss to one or more persons during any one-year period that totaled more than \$5,000.

R. vol. 1, 385. According to the government, this language complies with the statutory language because it asks the jury to determine whether Golightley engaged in “a related course of conduct.” Aplee. Br. 20 (quoting § 1030(c)(4)(A)(i)(I)). But the plain language of the instruction references only “conduct in or related to any of [c]ounts [one] through [seven]”—the instruction does not reference the statutory language requiring a related course of conduct affecting one or more *other* computers. R. vol. 1, 385. Thus, the government is incorrect that the felony-loss instruction remedied the elements instruction reference to a single computer. Taken together, the instructions required the jury to consider only whether Golightley caused damage to a single computer, not whether he also engaged in a course of conduct affecting one or more other computers.

The government additionally defends the instructions on the basis that they “largely followed the Eighth Circuit’s” pattern instruction. Aplee. Br. 35. But the operative word here is “largely.” The Eighth Circuit’s instructions explain that if the jury finds the elements of § 1030(a)(5)(A) satisfied, it must then determine whether “the defendant . . . caused loss resulting *from a related course of conduct affecting one or more other protected computers* of an aggregate value of \$5,000.00 or more.” Manual of Model Crim. Jury Instructs. for Dist. Cts. in the Eighth Cir. § 6.18.1030E (2017) (emphasis added). Critically, as we explained above, the instructions here omit this key language—language the government concedes it was required to prove.

Because the instructions did not require the jury to find that Golightley engaged in a course of conduct affecting one or more other computers, we are left with “substantial doubt that the jury was fairly guided” in reaching its verdict *Gorrell*, 922 F.3d at 1121–22 (quoting *Little*, 829 F.3d at 1181). We therefore vacate these seven convictions and remand to the district court with instructions to reclassify them as misdemeanors and to resentence Golightley accordingly.⁶

III. Supervised Release

We now turn to Golightley’s challenges to two supervised-release conditions: One condition requires Golightley’s probation officer to determine whether Golightley must inform third parties that he poses a threat to them and another requires Golightley to “take prescribed medication as directed.” R. vol. 1, 421. Because Golightley acknowledges that he did not object to either condition in the district court, we review his challenges for plain error. *See Goode*, 483 F.3d at 681. As noted above, under plain-error review, we will vacate these conditions only if Golightley demonstrates a plain error that affects his substantial rights and “seriously affects the fairness, integrity, or public reputation of judicial proceedings.” *Id.* (quoting *Kimler*, 335 F.3d at 1141).

⁶ Golightley also argues that the district court erred by (1) labeling the felony loss as a sentencing factor, rather than an element of the offense, and (2) not instructing the jury to find the felony loss beyond a reasonable doubt. But Golightley frames these challenges as additional reasons to reclassify his convictions as misdemeanors, not as reasons to acquit him. Because we conclude that these convictions must be reclassified as misdemeanors based on the jury instructions and the plain language of the statute, we need not address these additional challenges.

1. Risk-Notification Condition

Golightley argues that the district court improperly delegated judicial authority by imposing the risk-notification condition. This condition states that “[i]f the probation officer determines that [Golightley] pose[s] a risk to another person (including an organization), the probation officer may require [Golightley] to notify the person about the risk” R. vol. 1, 420. Relying on our recent decision in *United States v. Cabral*, 926 F.3d 687 (10th Cir. 2019), Golightley argues this condition is plainly erroneous because it impermissibly delegates judicial authority to the probation officer in a manner that could implicate liberty interests. *See id.* at 697–98 (vacating identical condition and explaining that probation officers cannot determine nature and extent of punishment; further explaining that such conditions infringe on fundamental rights where, for example, defendants must notify family of their risk). Given our rejection of an identical condition in *Cabral*, the government concedes that the district court erred in imposing the risk-notification condition and that remand is required.

In light of our holding in *Cabral* and the government’s concession, we conclude that the district court plainly erred in imposing this risk-notification condition. We therefore vacate the condition.

2. Mandatory-Medicine Condition

Golightley also argues that the district court erred in imposing the mandatory-medicine condition requiring him to “take prescribed medication as directed.” R. vol. 1, 421. More specifically, he asserts that the district court erred because it

“made no particularized medically grounded findings in support of this condition” and failed to “find that the condition would involve no greater deprivation of liberty than reasonably necessary.” Aplt. Br. 41. And he argues that these failures are plainly erroneous under *United States v. Malone*, 937 F.3d 1325 (10th Cir. 2019).

In *Malone*, we held that an identical mandatory-medicine condition was plainly erroneous because the district court had imposed the condition without making any particularized findings to support it. 937 F.3d at 1328. We explained that “this condition, on its face, is an impermissible infringement into a defendant’s significant liberty interests without the justifying support of particularized findings.” *Id.* But here, Golightley does not argue that the special condition is invalid for want of particularized findings. Instead, he asserts that the district court erred in imposing the special condition without making *medically grounded* particularized findings.

But even if we assume that the district court erred, Golightley’s argument fails on the second prong of plain-error review because that error is not plain under *Malone*. See *United States v. Whitney*, 229 F.3d 1296, 1309 (10th Cir. 2000) (explaining that plain error means clear or obvious error). That’s because *Malone* requires only “particularized findings”—it says nothing about whether those findings must include medically grounded findings. See 937 F.3d at 1327–28. Thus, the district court’s failure to make “particularized *medically grounded* findings” cannot be plain under *Malone*. Aplt. Br. 41 (emphasis added).

Likewise, and contrary to Golightley’s argument, *Malone* does not require the district court to find that the mandatory-medicine condition “would involve no

greater deprivation of liberty than reasonably necessary.” *Id.* Instead, and again, *Malone* requires only that the district court make particularized findings to explain the compelling circumstances justifying this special condition. 937 F.3d at 1327–28. Because Golightley’s opening brief does not dispute the district court’s analysis on any other ground, we reject his challenge and conclude that the district court did not plainly err in imposing the mandatory-medicine condition.⁷

Conclusion

Because the government failed to prove that Golightley transmitted a threat through interstate commerce, we vacate Golightley’s conviction for threatening to damage a protected computer. And because we conclude that the district court improperly classified Golightley’s seven convictions for damaging a protected computer as felonies, we reverse the district court’s judgment and remand with instructions to vacate Golightley’s felony convictions, reclassify those convictions as misdemeanors, and resentence accordingly. At resentencing, the district court may not reimpose the risk-notification condition. But we find no plain error in the district

⁷ For the first time in his reply brief, Golightley disputes the sufficiency of the district court’s findings for reasons other than not being medically grounded. He further notes that the Ninth Circuit requires medically grounded findings to justify mandatory-medicine conditions. *See United States v. Williams*, 356 F.3d 1045, 1055 (9th Cir. 2004). Because arguments raised for the first time in a reply brief are waived, we decline to consider these arguments. *See United States v. Sanchez*, 979 F.3d 1256, 1261 n.2 (10th Cir. 2020).

court's imposition of the mandatory-medicine condition.

Entered for the Court

Nancy L. Moritz
Circuit Judge