No. 23-927

IN THE
# United States Court of Appeals for the Ninth Circuit

UNITED STATES OF AMERICA,
*Plaintiff-Appellee*,
*v.*

JOSEPH SULLIVAN
*Defendant-Appellant*.

On Appeal from the United States District Court
for the Northern District of California
No. 3:20-cr-00337, Hon. William H. Orrick

## OPENING BRIEF FOR APPELLANT JOSEPH SULLIVAN

Christopher J. Cariello
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019

Aravind Swaminathan
ORRICK, HERRINGTON & SUTCLIFFE LLP
401 Union Street, Suite 3300
Seattle, WA 98101
(206) 839-8400

Amari L. Hammonds
ORRICK, HERRINGTON & SUTCLIFFE LLP
355 S. Grand Avenue, Suite 2700
Los Angeles, CA 90071

*Counsel for Defendant-Appellant Joseph Sullivan*

October 10, 2023

# TABLE OF CONTENTS

## TABLE OF AUTHORITIES

**Page(s)**

**Statutes, Rules & Regulations**

Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030

**Other Authorities**

## INTRODUCTION

Joe Sullivan protected hundreds of thousands of Uber drivers' personal information from public exposure—and was prosecuted for it.

In 2015, Uber hired Mr. Sullivan as its Chief Security Officer, a broad remit embracing everything from rider safety, to customer data, to cybersecurity. Before Mr. Sullivan's tenure, Uber had come under scrutiny for all of the above, including a Federal Trade Commission investigation into Uber's cybersecurity practices. This case involves a November 2016 data security incident that began when an anonymous emailer claimed to have found a security vulnerability in Uber's system.

At one time this scenario might have triggered fears of tech-noir hackers sowing chaos for sport. But by 2016, cybersecurity experts knew better. They had come to "embrace" people who found and reported security vulnerabilities as "security researchers." 9-ER-1777. So, when Uber received the email, it activated its "Bug Bounty" program—a cybersecurity approach that offers a monetary reward to people who find and report vulnerabilities.

It worked. Mr. Sullivan and his team fully resolved the 2016 incident through a Bug Bounty agreement. Two young men agreed to

disclose the vulnerability, destroy a database of 600,000 drivers' license numbers they had downloaded, and not disclose the data or incident publicly; Uber paid a $100,000 reward and pursued no legal action. No data was ever exposed. No Uber user was ever injured. Mr. Sullivan and his team had done their jobs.

But according to the government, Mr. Sullivan had also committed crimes. In 2017, Uber, under new senior leadership, decided to notify the FTC of the 2016 incident. Ultimately, the government blamed Mr. Sullivan—and the Bug Bounty agreement—for Uber's failure to do so sooner. It alleged (1) obstruction of an FTC proceeding, 18 U.S.C. § 1505, and (2) misprision of felony, 18 U.S.C. § 4, for concealment of purported violations of the Computer Fraud and Abuse Act (CFAA).

The government's theory was tenuous. It accused Mr. Sullivan of executing a cover-up. But Mr. Sullivan never lied to the FTC or destroyed evidence. Thirty others at Uber knew of the incident and Mr. Sullivan never told any of them to conceal anything. And one of those people was Uber's CEO, who Mr. Sullivan had kept continuously informed and who approved the Bug Bounty agreement. None of the 31

people aware of the incident even raised the prospect of informing the FTC, probably because the matter was so comprehensively resolved.

So the government built a case on innuendo. It asked the jury to view the Bug Bounty agreement not as an effective way to protect users, but as hush money. It faulted Mr. Sullivan for not directing Uber's legal department to notify the FTC (a job for Uber's CEO, if anyone), and for not editing submissions to the FTC that Mr. Sullivan had not drafted, signed, and in some instances even read. The government theorized, without proof, that Mr. Sullivan was motivated by a need to protect his own reputation as a cybersecurity professional.

The resulting conviction is profoundly flawed. The obstruction verdict flouts essential limits under § 1505—one that bars convictions based on conduct as far attenuated from an official proceeding as Mr. Sullivan's was here, and another that squarely forecloses criminal liability based on bare inaction alone. The district court erred as a matter of law by forsaking both requirements. *Infra* § I.

As for the misprision charge, the government could never resolve its central paradox: The predicate felony Mr. Sullivan was accused of concealing was the researchers' access to Uber's systems "without

authorization," 18 U.S.C. § 1030, Add.2; but Uber, with CEO approval, had ratified that very access through a Bug Bounty agreement. No one at Uber regarded the researchers as felons after that—and indeed no researcher had ever before been convicted of violating § 1030 in like circumstances. The government thus failed to show that Mr. Sullivan believed the researchers had committed felonies. *Infra* § II.

The government may wish that federal law required Uber or its employees to disclose data security incidents—a step Congress has not taken. And it is fair to ask whether Mr. Sullivan should have, in his words, "expand[ed] [his] aperture" beyond protecting Uber's systems and users' data. 2-ER-257. But Mr. Sullivan committed no crimes. Government and defense witnesses alike agreed that he "act[ed] in good faith to solve a complicated problem," 8-ER-1475, 8-ER-1528, and "was trying to do the right thing," 16-ER-3288. Stretching criminal statutes to punish Mr. Sullivan for doing his job—and not doing someone else's—is not only unjust for Mr. Sullivan, it sets a frightening precedent for others on the cybersecurity front lines.

This Court should reverse.

## JURISDICTION

The district court had jurisdiction under 18 U.S.C. § 3231. It entered judgment on May 9, 2023. 1-ER-1-7. Mr. Sullivan timely filed his notice of appeal on May 12, 2023. 4-ER-775-76. This Court has jurisdiction under 28 U.S.C. § 1291.

## STATEMENT OF THE ISSUES

1. Whether the district court legally erred by rejecting, and failing to instruct the jury on, the requirement that to prove obstruction of the FTC proceeding under 18 U.S.C. § 1505, the government had to demonstrate a nexus between conduct and the FTC proceeding.

2. Whether the district court legally erred by rejecting, and failing to instruct the jury on, the requirement that to prove obstruction of the FTC proceeding under 18 U.S.C. § 1505 based on silence, the government had to demonstrate an independent duty to disclose.

3. Whether, to support the charge of misprision of felony under 18 U.S.C. § 4, the evidence was sufficient to prove Mr. Sullivan's "knowledge" that the researchers' computer access was "without authorization," 18 U.S.C. § 1030, in the face of undisputed evidence of

Mr. Sullivan and his team's reasonable belief that Uber, with its CEO's approval, ratified the researchers' access.

4. Whether the district court abused its discretion under Federal Rule of Evidence 403 by permitting the government to introduce the guilty plea agreement of one of the researchers as substantive evidence of Mr. Sullivan's guilt of misprision of felony.

## ADDENDUM

The addendum to this brief contains the relevant statutes and rules. Ninth Cir. R. 28-2.7.

## STATEMENT OF DETENTION STATUS

Mr. Sullivan is currently serving his sentence of probation. 1-ER-3. He is neither detained nor on bail.

## STATEMENT OF THE CASE

### *The FTC Investigates Uber's Data Security Practices.*

The FTC's inquiries into Uber's data security practices started before Mr. Sullivan was at the company. The popular ride-hailing company obtains and stores immense amounts of data from both drivers and riders. 7-ER-1313. Like many companies, Uber uses Simple Storage Service repositories (or "S3 buckets") on Amazon Web Services ("AWS") to store this data. 3-ER-459; 7-ER-1320.

In May 2014, someone was able to find a passcode to Uber's S3 buckets that an Uber engineer had mistakenly stored in a publicly accessible place online. 3-ER-458-59; 6-ER-1091. Using the broad access the key conferred, the individual obtained an unencrypted database with "approximately 50,000" drivers' names and license numbers. 6-ER-1077; 3-ER-459-60.

Uber disclosed this incident publicly in early 2015. 3-ER-468. When the FTC learned of it, it launched an inquiry, 3-ER-456-57, issuing a broad Civil Investigative Demand, or CID, seeking to determine whether Uber had violated the FTC Act by misrepresenting the quality of its security practices. 3-ER-548-67.

***Uber Hires Joe Sullivan, Who Rapidly Revamps Uber's Data Security Operation.***

In April 2015, still in the midst of the FTC's investigation, Uber hired Mr. Sullivan. His resumé was sterling. He had been a cybercrime prosecutor, worked in information security for eBay and PayPal, and was Facebook's CSO from 2009 to 2015. 3-ER-569. The CSO role was not a legal one. 3-ER-573; 6-ER-1145. Mr. Sullivan's job was to build and supervise a team that handled all security-related matters at Uber. 3-ER-573; 10-ER-1949.

In the year-and-a-half after Mr. Sullivan was hired, he expanded the Security Team from around 10 members to more than 100. 3-ER-576; 15-ER-3026-27. This growing team "assess[ed] Uber's systems and data comprehensively and tr[ied] to make them more secure," including with respect to the AWS S3 buckets at the center of the 2014 breach. 9-ER-1615-16.

Mr. Sullivan was never in charge of Uber's response to the FTC's investigation—Uber's outside counsel handled "95 percent of [the] communications" with the FTC, 7-ER-1242; 6-ER-1079-80, while in-house counsel "took the laboring oar" on responses to the FTC. 10-ER-1963; 10-ER-1866-70; 10-ER-1992-95; 3-ER-586. Uber did put Mr. Sullivan before the FTC twice. In March 2016, the company trotted him out for what the FTC called a "dog-and-pony show[]" designed to "show [the FTC] everything that [wa]s most impressive" about Uber's improved security team. 6-ER-1123. Then later that year, Uber designated Mr. Sullivan a "corporate representative" to appear on Uber's behalf at a deposition. 10-ER-1977-79.

The FTC deposed Mr. Sullivan on November 4, 2016. The deposition addressed "broad topics," 7-ER-1189-91, concerning Uber's

security practices before and after the 2014 breach, *see generally* 3-ER-580-650. Mr. Sullivan described the progress Uber had made in its security practices. 3-ER-588; 3-ER-600-603; 3-ER-613. But he also acknowledged the challenges a company like Uber faces, and he was forthright about where things stood: "[W]e're far from perfect and probably nobody's perfect." 3-ER-597-98.

***Uber Resolves A 2016 Security Incident Through Its "Bug Bounty" Program.***

As one member of the security team agreed, "[i]t is impossible to achieve perfect security." 15-ER-3047. And as long as there are vulnerabilities, there will be hackers—"good hackers, bad hackers, and everything in between"—that seek those vulnerabilities out. *See* 9-ER-1775-76; 15-ER-3045-49. Bug Bounty programs are how many forward-thinking organizations address this reality.

A Bug Bounty program broadly invites individuals to find and report vulnerabilities (i.e., "bugs") within a company's system, deputizing them as "security researchers." 15-ER-3047-48. Once a researcher accepts the invitation, the researcher and the company enter into a Bug Bounty agreement. The basic terms are this: The researcher is permitted to look for security vulnerabilities on a

company's systems; once discovered, the researcher discloses the vulnerability to the company instead of using it maliciously; the company then rewards the researcher for the disclosure and agrees "not to turn [them] over to law enforcement[] [and] not to sue them" for accessing the company's system, 13-ER-1778; *see* 9-ER-1775-78. Everybody wins—the researcher earns compensation, the company learns of a vulnerability (that it can fix), and user data gets safer.

Uber's Bug Bounty program was broad by design. It invited "anybody on the internet," 9-ER-1784, to share with Uber "any vulnerability that could negatively affect the security of [its] users," 3-ER-476 (Uber policy guidelines); 3-ER-474-75 (Uber program terms). Participation was resounding. In its first 100 days, Uber received over 2,000 reports and paid $345,000 in bounties for "over 160 security flaws." 9-ER-1785. And in November 2016—two weeks after Mr. Sullivan was deposed by the FTC—Uber's security team used the program to address the security incident that underlies this case.

On November 14, 2016, a pseudonymous sender emailed Mr. Sullivan claiming to "have found a major vulnerability." 3-ER-482. Uber initiated its Bug Bounty process, "extending an olive branch" in

hopes of reaching a Bug Bounty agreement with what Uber would later learn were two researchers. 10-ER-1818; 15-ER-3031-32. Conducting "an experiment," 3-ER-524, the researchers had "gain[ed] access" to "a number of [access] keys," and then "used those keys to gain access to an S3 bucket." 7-ER-1356. Once there, they downloaded an unencrypted backup database that contained approximately 600,000 drivers' license numbers. 8-ER-1575. The pseudonymous sender seemed amenable to a Bug Bounty agreement, but wanted "6 digits," 3-ER-521—an amount that was "much higher" than Uber's usual amount and "fe[lt] extortionate" to some on Mr. Sullivan's team, 8-ER-1439-42.

The parallels between the 2014 and 2016 incidents were frustrating, as well. Though the team had adopted new practices in response to the FTC inquiry, the incident "showed … there was a piece that [they] had missed." 9-ER-1625. Mr. Sullivan noted that it "m[ight] … play very badly" if the "worst case" scenario materialized and the researcher "dox[ed] the data" (i.e., "dump[ed] it on the internet," 8-ER-1425-26). 3-ER-493.

That worst case scenario never materialized thanks to Mr. Sullivan and his team. Twenty-five team members worked to verify the

vulnerability, determine the researchers' identities, and negotiate mutually agreeable terms for a Bug Bounty agreement. 15-ER-3034; 3-ER-651-56; 9-ER-1754; 15-ER-3099-114. The team meticulously recorded its steps and contingency plans in a central tracking document. 3-ER-483-513. Two in-house lawyers, 10-ER-1953; 12-ER-2422; 3-ER-516, and three members of Uber's communications team, 16-ER-3302-07, were also made aware of the incident as it unfolded.

Meanwhile, Mr. Sullivan reported directly up to Uber's CEO, Travis Kalanick. Mr. Sullivan informed Kalanick immediately once Uber confirmed the vulnerability. 3-ER-515; 8-ER-1493-94. The two texted about Uber's preference for reaching a Bug Bounty agreement. 3-ER-515. And Mr. Sullivan kept Kalanick constantly updated. 17-ER-2802-03; 3-ER-514.

Uber and the researchers ultimately reached an agreement. The researchers agreed to disclose the vulnerability to Uber, not disclose the incident or vulnerability publicly, and delete all driver data. 3-ER-527. Uber agreed to pay $100,000, which was more than Uber's usual amount, but "appropriate" for the significance of the vulnerability, 15-ER-3056; 9-ER-1750. Explained one team member, it was "a great deal"

for Uber, 15-ER-3056, and it satisfied Uber's highest "priority": "protect the data" from exposure. 3-ER-547.

Uber also followed up to verify that the data was safe and confirm the researchers' identities: a 19-year-old in Florida named Brandon Glover and a 20-year-old in Toronto named Vasile Mereacre. 15-ER-3099; 15-ER-3116. Uber's Head of Investigations reported to Mr. Sullivan that he was "very, very comfortable" that the drivers' data would never be exposed. 16-ER-3173. No Uber user was ever injured.

***The Government Learns Of The 2016 Security Incident And Indicts Mr. Sullivan.***

All told, 31 Uber employees knew of the 2016 security incident as it was unfolding. *Supra* 11-12; 3-ER-662; 3-ER-517; 3-ER-723-24; 3-ER-728-29; 13-ER-2567; 3-ER-725-27; 14-ER-2855-56; 8-ER-1510-11; 3-ER-657-61. After it was resolved with no harm to Uber's users, none of the 31 raised it to the FTC. While Uber had touted its Bug Bounty program to the FTC, the FTC had never asked about it "over the course of [its] 32-month investigation." 7-ER-1279-81. And Uber had never reported a Bug Bounty agreement to the FTC before. 10-ER-2007.

Nor did Uber disclose the incident pursuant to any state-law disclosure statutes. In-house counsel Craig Clark reasoned that Uber's

decision to cooperate with Glover and Mereacre triggered an exception in state law for "employees" of a company. 11-ER-2109-10. At trial several years later, Clark would claim this advice was influenced by a "directive" from Mr. Sullivan, 11-ER-2109; *infra* 17, but no one expressed disagreement with the analysis at the time. *E.g.*, 8-ER-1522 (security team member did not "recall anybody expressing the view in Mr. Sullivan's presence that this incident was a reportable data breach"). And again, no user had been injured. *See, e.g.*, Wash. Rev. Code § 19.255.010 ("Notice is not required if the breach … is not reasonably likely to subject consumers to a risk of harm.").

As for federal law enforcement, there was nothing to report. The whole premise of a Bug Bounty program is that a company invites researchers onto its system and, if an agreement is reached, ratifies their conduct. *Supra* 9-11. As Clark later confirmed—this time offering his own "view"— "if something is treated as a bug bounty, then, by definition, it wouldn't be considered a data breach" because "the access would, for all intents and purposes, have been authorized." 11-ER-2213.

No one second-guessed this until later in 2017. Several board members had appointed a "Special Matters Committee," or "SMC," to investigate CEO Kalanick's management, 13-ER-2582-83, and Uber would soon replace him as CEO. 13-ER-2562; 13-ER-2579. When the SMC learned of the 2016 security incident, it interviewed Mr. Sullivan about it. According to notes kept by outside counsel, Mr. Sullivan explained that "if we didn't contain it, it would be something we might have to report," 3-ER-744, but that "it's legal's job to decide," and in particular "Craig [Clark]," 3-ER-745. He also explained that he had kept Kalanick informed "from day 1 to conclusion on a very regular basis," 3-ER-745, and that Kalanick had "signed off on the [$]100K" Bug Bounty agreement, 3-ER-749; 15-ER-3018.

When Uber's new CEO asked Mr. Sullivan directly about the incident, however, he believed Mr. Sullivan's response was "incomplete or misleading." 13-ER-2565-71. He fired Mr. Sullivan and Clark. 13-ER-2577; 13-ER-2591. And though he thought it was "absolutely right to pay money to ensure our customers' data is safe" and that "the team did a great job technically," 13-ER-2599-600, he "thought that the

decision not to disclose at the time was the wrong decision," 13-ER-2577.

When Uber informed the FTC, the FTC "proposed a new complaint and order that included additional facts" about the 2016 incident and had "some revised terms." 7-ER-1234-37; 3-ER-700 (FTC complaint); 8-ER-714-22 (FTC order). But the government indicted Mr. Sullivan, accusing him of orchestrating a cover-up.

### *Mr. Sullivan Is Convicted Of Obstruction Of Justice And Misprision Of Felony And Sentenced To Probation.*

The government charged Mr. Sullivan with (1) obstruction of the FTC proceeding under 18 U.S.C. § 1505, Add.12-13, and (2) misprision of felony, 18 U.S.C. § 4, Add.2, for allegedly concealing Glover and Mereacre's violations of the CFAA, 18 U.S.C. § 1030, Add.2-12. 2-ER-445-51. In September 2022, the district court held a jury trial.

***Obstruction of FTC proceeding.*** To establish its obstruction case, the government had to prove (among other things) that Mr. Sullivan had "corruptly … influence[d], obstruct[ed], or impede[d]" the FTC proceeding. 18 U.S.C. § 1505, Add.13. But no witness testified that Mr. Sullivan lied to the FTC, told anyone else to lie, asked anyone to withhold information, or destroyed documents related to the 2016

incident. Witness after witness testified he had never done so. 8-ER-1482-83; 9-ER-1622-23; 10-ER-1856; 13-ER-2557; 15-ER-3056-57; 16-ER-3175; 16-ER-3287-88.

Instead, the government asserted that the way Mr. Sullivan and his team had *resolved* the 2016 incident was *itself* the cover-up. It called the Bug Bounty agreement a "cho[ice] to pay th[e] hackers $100,000 … to buy their silence," 6-ER-1013, and the attendant NDA "a critical step in the cover-up," 6-ER-1031. It elicited Clark's testimony—obtained in exchange for Clark's immunity, 11-ER-2255—that Mr. Sullivan had "direct[ed]" him to develop a legal theory to avoid disclosure under state law. 11-ER-2109. And it pressed an omissions-based theory, asserting that Mr. Sullivan "never once told the attorneys representing Uber" before the FTC "what had happened." 6-ER-1021-22.

The government was aided by two legal rulings. First, the district court refused to instruct the jury that there must be "a nexus between the defendant's conduct and the pending FTC proceeding." 1-ER-154; 16-ER-3158. It thus allowed the government to rely on attenuated conduct Mr. Sullivan undertook not in connection with the FTC

proceeding, but while managing a security incident. 1-ER-13-15 (order denying motion for acquittal).

Second, the district court rejected Mr. Sullivan's request for an instruction that "[i]f the corrupt act at issue involved the withholding of information, the government must prove … that Mr. Sullivan had a specific duty … to disclose the withheld information." 1-ER-160; 16-ER-3158. The court thus also allowed the government to make its case without ever showing that Mr. Sullivan owed any duty to disclose to the FTC. 1-ER-15-17 (order denying motion for acquittal).

***Misprision of felony.*** To prove misprision, the government had to show that Mr. Sullivan knew of "the actual commission of a felony" and concealed it. 18 U.S.C. § 4; Add.2. The predicate felonies the government pointed to were Glover and Mereacre's alleged violations of the CFAA, § 1030, which bars accessing a protected computer "without authorization." The government's case thus turned on a central legal question: Where someone *initially* accesses a computer without authorization, but ultimately their access is ratified by a Bug Bounty agreement, are they in violation of § 1030? The government had to show beyond a reasonable doubt that Mr. Sullivan believed Glover and

Mereacre were felons even after Uber authorized their access by Bug Bounty agreement.

To do so, the government provided evidence that Mr. Sullivan had prosecuted § 1030 cases over a decade prior, 6-ER-1138-40; 14-ER-2820-27, as well as statements from team members that the researchers' demands, prior to entering a Bug Bounty agreement, felt like "extortion." 14-ER-2862-63. But undisputed evidence established Mr. Sullivan and his team's understanding that if Uber entered into a Bug Bounty agreement, it would not need to notify law enforcement. *E.g.*, 11-ER-2213 (Clark opining that "access would, for all intents and purposes, have been authorized"). And the government offered evidence of not a single § 1030 conviction, as of the 2016 incident, obtained after a company and the defendant had entered into a Bug Bounty agreement.

In fact, the government identified only one such prosecution since then—the guilty plea of Mereacre himself. Over Mr. Sullivan's objection, 2-ER-383-89, the district court allowed the government to use the plea agreement as *substantive evidence* of Mr. Sullivan's guilt. The court found that the plea agreement would not prejudice Mr. Sullivan

because he was charged with a "separate crime" from Mereacre's. 1-ER-88.

The jury found Mr. Sullivan guilty on both charges, 2-ER-357, and the district court denied Mr. Sullivan's post-trial motions. 1-ER-8-24. The government pursued a custodial sentence, recommending 15 months in prison. 2-ER-267. Backing Mr. Sullivan were 186 letters filed by friends, family, and colleagues, supporting the person a witness at trial called "one of the most honest and ethical people I've known." 15-ER-3090.

At sentencing, the district court recognized that "this was really sort of an unprecedented prosecution." 2-ER-262. It acknowledged that Mr. Sullivan and his team had successfully ensured that no Uber user was harmed. 2-ER-263. And it appreciated that "the way … the evidence came in," the notion that the NDA was "an act of a coverup" "doesn't really fly." 2-ER-263. The court sentenced Mr. Sullivan to probation. 2-ER-274.

## SUMMARY OF THE ARGUMENT

**I.** The obstruction conviction rests on two separate errors of law.

**A.1.** First, in instructing the jury and upholding the conviction under § 1505, the district court erroneously rejected the requirement that the government prove a nexus between alleged conduct and the proceeding at issue. Two circuits have recognized that § 1505 contains a nexus requirement, and the Supreme Court and other courts have recognized it in analogous obstruction statutes. The only case to reject such a requirement, *United States v. Bhagat*, 436 F.3d 1140 (9th Cir. 2006), is clearly irreconcilable with intervening Supreme Court authority, so the panel need not follow it.

**2.** The government failed to satisfy the nexus requirement because it could not show that Mr. Sullivan's conduct had the "natural and probable effect" of obstructing the FTC proceeding. *See United States v. Aguilar*, 515 U.S. 593 (1995). That conduct had no connection to the FTC proceeding at all; it was undertaken to address a security incident that thirty other people knew about and were free to disclose.

**3.** At a minimum, and for much the same reasons, the district court's failure to instruct the jury on § 1505's nexus requirement was not harmless beyond a reasonable doubt, requiring a new trial.

**B.1.** Second, in instructing the jury and upholding the conviction, the district court erroneously permitted the government to rely on mere silence, without having to prove that Mr. Sullivan breached an independent duty to disclose. Bedrock principles of criminal law, the text of § 1505, case law from analogous statutory contexts, and principles of lenity all bar criminal liability for mere inaction absent a duty.

**2.** The government failed to prove that Mr. Sullivan breached any duty. He owed no personal duty to the FTC and discharged his duty to Uber by fully informing Uber's CEO of the 2016 incident.

**3.** At a minimum, and for much the same reasons, the district court's failure to instruct the jury on the duty requirement was not harmless beyond a reasonable doubt, requiring a new trial.

**II.** The misprision of felony conviction must be overturned for two independent reasons.

**A.1.** The conviction should be reversed because the government failed to prove that Mr. Sullivan knew that Glover and Mereacre had "actual[ly] commi[tted]" a violation of § 1030. *See* 18 U.S.C. § 4. Uber's in-house counsel testified to the understanding that where access that was initially unauthorized is later authorized by Bug Bounty agreement, it does not violate § 1030. That is the most natural, and at least a reasonable, reading of § 1030's grant of broad discretion to computer owners to authorize access to their systems how and when they choose.

**2.** Undisputed evidence establishes that Mr. Sullivan and his team understood Uber to have this broad and flexible discretion; to have exercised it by adopting a robust Bug Bounty program; and to have duly authorized Glover and Mereacre's access, with CEO approval, by entering into a Bug Bounty agreement.

**3.** The government failed to overcome this unshakeable doubt as to Mr. Sullivan's reasonable belief. It adduced no evidence that anyone at Uber regarded Glover and Mereacre as criminals after they entered the Bug Bounty agreement. And it pointed to no instance (besides this case) of someone who had been convicted despite entering into a Bug

Bounty agreement. Because no rational juror could find that Mr. Sullivan had knowledge of commission of a felony, this Court should reverse.

**B.1.** Independently, the district court abused its discretion by admitting Mereacre's guilty plea agreement as substantive evidence of Mr. Sullivan's guilt. The plea agreement was highly prejudicial because, as a judicial document, the jury naturally would give it undue weight on the all-important questions of whether Mereacre's conduct violated § 1030 and whether Mr. Sullivan believed the same. The agreement had virtually no probative value beyond that improper purpose, because the government could and did introduce evidence through Mereacre himself of his underlying conduct. The agreement should have been excluded under Federal Rule of Evidence 403.

**2.** Admission of the guilty plea more likely than not affected the verdict, because it filled a central void in the government's case—its inability to point to an instance of a researcher being convicted of a § 1030 violation after entering into a Bug Bounty agreement. This merits a new trial.

## STANDARD OF REVIEW

"[W]hen the parties dispute a legal determination" by the district court that underlies the jury instructions, this Court "review[s] de novo." *United States v. Perdomo-Espana*, 522 F.3d 983, 986 (9th Cir. 2008). It also reviews de novo the sufficiency of the evidence and the denial of a motion for judgment of acquittal under Federal Rule of Criminal Procedure 29. *United States v. Chapman*, 528 F.3d 1215, 1218 (9th Cir. 2008). The court "'view[s] the evidence in the light most favorable to the government and determine[s] whether any rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt.'" *Id.*

Evidentiary rulings are reviewed for abuse of discretion. *United States v. Beckman*, 298 F.3d 788, 792 (9th Cir. 2002).

## ARGUMENT

### I. The Obstruction Conviction Is Infected By Two Errors Of Law.

In instructing the jury and upholding the conviction under § 1505, the district court misread that provision in two respects. First, it erroneously read § 1505 not to require a "nexus" between Mr. Sullivan's conduct and the FTC's inquiry—a requirement the government failed to

satisfy. *Infra* § A. Second, the district court permitted the government to obtain a conviction based on Mr. Sullivan's mere nondisclosure of information, with no showing that Mr. Sullivan owed a duty to disclose information in the first place. *Infra* § B. Error as to either requirement independently merits a new trial as a result of the court's failure to instruct the jury. And if the Court agrees that the evidence is insufficient as to both, *infra* §§ A.2., B.2., the errors require acquittal.

### A. The district court erroneously rejected § 1505's nexus requirement.

#### 1. Section 1505 requires a showing that conduct has the "natural and probable effect" of obstructing an agency proceeding.

Two circuits have held that § 1505 carries a nexus requirement under which the government may rely only upon conduct that has the "natural and probable effect" of obstructing an agency proceeding. Still more decisions—including three by the Supreme Court—have applied that requirement to closely related federal obstruction statutes. But the district court rejected Mr. Sullivan's request for a nexus instruction and denied his motion for acquittal, believing the requirement foreclosed by this Court's decision in *United States v. Bhagat*, 436 F.3d 1140. *Supra*

17-18. *Bhagat* is no obstacle here because it is clearly irreconcilable with intervening Supreme Court precedent.

**a.** The Supreme Court first addressed the nexus requirement in *United States v. Aguilar*, 515 U.S. 593 (1995). *Aguilar* involved 18 U.S.C. § 1503, which criminalizes conduct directed at various people ("grand or petit juror," "officer … of any court"), and ends with a catch-all prohibiting obstruction of "the due administration of justice." The question in *Aguilar* was whether, despite this "general language," a conviction under § 1503 requires a nexus between alleged conduct and an official proceeding. *Id.*

The Court held that it does. To be criminal, an act must have the "'natural and probable effect' of interfering with the due administration of justice" based on the conduct's "relationship in time, causation, or logic with" a particular proceeding. *Aguilar*, 515 U.S. at 599. So, in *Aguilar*, it was not enough that the defendant lied to the FBI about a topic he knew was the subject of a grand jury proceeding. *Id.* at 600. Merely "uttering false statements to an investigating agent … who *might or might not testify* before [the grand jury]" is insufficient. *Id.*

(emphasis added). Without "knowledge that his actions are likely" to affect a proceeding, a defendant "lacks the requisite intent." *Id.* at 599.

Soon after *Aguilar*, this Court applied the natural-and-probable-effect standard to the statute at issue here, § 1505. *United States v. Hopper*, 177 F.3d 824, 831 (9th Cir. 1999). Two other circuits followed suit. *United States v. Quattrone*, 441 F.3d 153, 174-75 (2d Cir. 2006) (adopting nexus requirement for § 1505); *United States v. Senffner*, 280 F.3d 755, 762 (7th Cir. 2002) (same). This makes good sense. *Aguilar* read a catch-all provision that had no reference to a "proceeding" to nevertheless require a nexus to one; provisions like § 1505 that explicitly reference a "proceeding" have that nexus requirement rooted in their text.

And so the Supreme Court held in *Arthur Andersen LLP v. United States*, confronting yet another obstruction statute, 18 U.S.C. § 1512(b)(2)(A), (B), which criminalizes certain acts that obstruct an "official proceeding." 544 U.S. 696, 707-08 (2005). Citing *Aguilar*, *Arthur Andersen* overturned the verdict because the jury instructions contained no nexus requirement. *Id.*; *see also Marinello v. United States*, 138 S. Ct. 1101 (2018) (applying *Aguilar*'s nexus requirement to

26 U.S.C. § 7212(a), which addresses interference with "due administration" of the Internal Revenue Code).

By now the "nexus requirement is firmly rooted in law." *United States v. Lonich*, 23 F.4th 881, 905-06 (9th Cir. 2022). At least a dozen obstruction statutes carry an explicit textual nexus requirement, including § 1505. *Valenzuela Gallardo v. Barr*, 968 F.3d 1053, 1064 n.9 (9th Cir. 2020) (citing 18 U.S.C. §§ 1501-03, 1505-10, 1513, 1516-17), *overruled on other grounds by Pugin v. Garland*, 599 U.S. 600 (2023). There is no longer a credible argument that the government can obtain a conviction under § 1505 without demonstrating that allegedly criminal conduct has the natural and probable effect of obstructing a proceeding.

**b.** It is true that this Court in *Bhagat* found no plain error in jury instructions that imposed no nexus requirement under § 1505. 436 F.3d at 1147-48. *Bhagat* distinguished *Aguilar* on the unreasoned basis that "Bhagat was charged … with obstructi[on of] an agency proceeding and not a judicial one." *Id.* at 1148. Just as dubiously, it dismissed this Court's *Hopper* decision as merely "us[ing] *Aguilar*'s 'natural and

probable effect' language to explain how the defendant's conduct affected the … proceeding." *Id.*

*Bhagat* is bad law that this Court need not follow. "[A] three-judge panel … may overrule the decision of a prior panel … where an 'intervening higher authority' is 'clearly irreconcilable' with the reasoning of that decision." *CoreCivic, Inc. v. Candide Grp., LLC*, 46 F.4th 1136, 1141 (9th Cir. 2022). That is so here.

***Arthur Andersen.*** As explained above (at 28), *Arthur Andersen* recognized a nexus requirement under § 1512, which explicitly prohibits certain types of obstruction with "official proceedings." 544 U.S. at 702. In doing so, it rejected the only two bases upon which *Bhagat* rests. First, it required a nexus in a case that involved not purely judicial proceedings, but "regulatory and criminal proceedings and investigations," the former of which is at issue in § 1505. *Id.* This directly refutes *Bhagat*'s distinction of "judicial proceeding" versus "agency proceeding." 436 F.3d at 1147-48. Second, *Arthur Andersen* applied the nexus requirement not to a catch-all, but to a provision explicitly referencing an "official proceeding[]." *Id.* This negates the district court's defense of *Bhagat* as reading *Aguilar* to apply only to the

sort of "broad chatchall phase[] that [is] absent from section 1505." 1-ER-15.

*Arthur Andersen* is technically not intervening authority—it issued nine months *before Bhagat* did. But it should be given the same effect in light of highly unusual circumstances attending the panel's decision in *Bhagat*. *Bhagat* was first submitted in April 2004, long before *Arthur Andersen* was decided; but the submission was vacated in September 2004 as the panel waited for the Supreme Court to decide a Sixth Amendment sentencing issue in *Blakely v. Washington*, 542 U.S. 296 (2004). *See* Order, *United States v. Bhagat*, No. 03-10029 (9th Cir. Sept. 1, 2004) (*Bhagat* Dkt.), Dkt. 50. Once *Blakely* was decided in May 2005, the parties addressed its effect and the case was resubmitted, but no one informed the panel of *Arthur Andersen*. *See Bhagat* Dkt. 51 (Gov't Mot. for Voluntary Dismissal of Cross-Appeal), 57 (28(j) Letter), 62 (Pet. for Reh'g).

Further proof that the panel was unaware of *Arthur Andersen*: the lone case *Bhagat* cited for not applying *Aguilar* to § 1505—a Second Circuit opinion that declined to apply *Aguilar* to a subsection of § 1512—was overruled by *Arthur Andersen* itself. *Bhagat*, 436 F.3d at

1148 (citing *United States v. Gabriel*, 125 F.3d 89 (2d Cir. 1997), recognized as overruled in *Quattrone*, 441 F.3d at 176). In these unusual circumstances, *Arthur Andersen* should bear on this Court's evaluation of *Bhagat*'s continued vitality.

***Marinello.*** Even if this Court does not consider *Arthur Andersen* itself, its import subsists in the Supreme Court's 2018 decision in *Marinello v. United States*, the Court's third decision recognizing a nexus requirement in an obstruction statute. 138 S. Ct. 1101 (2018). *Marinello* held that *Aguilar*'s "nexus" requirement applies to the "Omnibus Clause" of § 7212(a) of the Internal Revenue Code, another broad catch-all criminalizing obstruction of the "due administration of" that code.

Meanwhile, the two dissenting Justices in *Marinello*—explaining why they thought the majority had gone too far with § 7212(a)—made clear precisely why the Court had been unanimous in *Arthur Andersen* when evaluating § 1512(b)(2)(A): "[T]his nexus requirement came from the statutory text, which expressly included 'an official proceeding.'" *Id.* at 1116 (Thomas, J., dissenting). Section 1505 works the same way.

This Court should overrule *Bhagat*, which cannot be reconciled with *Arthur Andersen*, *Marinello*, and the body of case law making plain that § 1505 is among those obstruction statutes that carries a nexus requirement.

**2. The government failed to establish a nexus between Mr. Sullivan's conduct and the FTC proceeding.**

No "rational trier of fact" could find that the government established the nexus requirement. *See Chapman*, 528 F.3d at 1218.

As *Aguilar* explains, the government must show that alleged conduct "ha[s] the 'natural and probable effect' of interfering" with a proceeding. *Aguilar*, 515 U.S. at 599, 601. Conduct that satisfies this requirement is that which "all but assures" the obstruction of a proceeding—for example, "deliver[ing] false documents or testimony" or shredding records. *Id.* at 601 & n.2. But where conduct merely "might or might not" have some effect on a proceeding, its effect is not "natural and probable," and so it "falls … on the other side of the statutory line." *Id.*

That is where the conduct the government relied upon falls. First, the government pointed to statements made by Mr. Sullivan at the

beginning of the 2016 incident urging the security team to keep information "'tightly controlled,'" 8-ER-1579, and stressing that this "can't … get out," 17-ER-3390. A host of witnesses, both the government's and defense's, testified that the level of secrecy was "normal in light of [past] experience." 9-ER-1620-21; *see* 8-ER-1579; 11-ER-2236-37; 16-ER-3273-75; 16-ER-3303.

More importantly, *no one* testified that they understood these statements to restrict them from saying something they otherwise would have—in fact, no one thought the statements had to do with the FTC investigation. 8-ER-1507 ("I think it was general guidance…."); 8-ER-1474-75 ( "I did not" "connect those … in [my] mind."). Nor did the government prove that anything someone might have said—absent Mr. Sullivan's statements urging discretion—would have assuredly wended its way to the FTC.

Second, the government emphasized Mr. Sullivan's statements that he was informing Uber's "A Team" (i.e., top Uber executives) as the incident unfolded, when technically he was informing only CEO Kalanick, 17-ER-3392, who was the head of the A Team, 11-ER-2227. *Supra* 12, 15. It is worth pausing on this: The government's theory of a

criminal cover-up is that Mr. Sullivan *only* informed no less than *the CEO* of his company.

In any event, the theory is again based on a chain of *ifs*—the notion that Mr. Sullivan's statement might have lulled someone else into not saying something to someone, which someone might have said something else, and down the chain someone might have decided for the first time ever to inform the FTC of a Bug Bounty agreement. The government failed to establish that any of this was natural and probable—it was all the sort of might-or-might-not that does not suffice under *Aguilar*.

Third, the government pointed to the Bug Bounty agreement itself as an attempt to "buy [Glover and Mereacre's] silence," 6-ER-1013, and avoid state-law disclosure requirements, 11-ER-2109. As the district court itself recognized at sentencing, the idea that the Bug Bounty agreement's nondisclosure obligations were "an act of a coverup" "doesn't really fly." 2-ER-263. That is because it was not directed to the FTC proceeding at all—it was a mechanism for successfully resolving the incident and ultimately preventing harm to users. *Supra* 9-14. No

witness suggested otherwise. The government's theory that the Bug Bounty agreement was a calculated cover-up was just insinuation.

Even further afield is Clark's testimony that Mr. Sullivan gave him a "directive" to provide legal advice that the incident was not disclosable under *state* law. 11-ER-2109. Section 1505 criminalizes acts designed to obstruct administration of *federal* law. It does not somehow sweep in the administration of every state law that could incidentally, down the chain, result in a federal agency learning information.

And in all events, even if the government did have answers to all the ifs and might-nots above, it could never overcome the biggest one of all: The undisputed fact that *30* others were aware of the 2016 incident —including the CEO, Chief Information Security Officer, Head of Investigations, two in-house counsel, three members of the communications department, and 22 other security team members, *supra* 11-13. A successful cover-up could hardly be the natural and probable consequence of Mr. Sullivan's conduct when that effect would have turned on the independent decisions of 30 other people who were free to discuss whatever they wished.

Without any required nexus between Mr. Sullivan's case and the FTC proceeding, the government built a case on the sort of surmise *Aguilar* flatly rejects. This Court should do the same.

### 3. The district court's failure to instruct the jury on the "nexus" requirement was not harmless.

At a minimum, the Court should order a new trial because the district court erroneously rejected Mr. Sullivan's requested nexus instruction and that error was not harmless.

"Where … [instructional] error lies in *defining the offense*," a conviction can be upheld only where the government "prove[s] [harmlessness] beyond a reasonable doubt." *United States v. Perez*, 962 F.3d 420, 441 (9th Cir. 2020). That stringent standard applies here because the nexus requirement is part of the definition of the offense. Indeed, *Arthur Andersen* swiftly overturned an instruction that, like the one here, "led the jury to believe that it did not have to find *any* nexus between" alleged conduct and an official proceeding. 544 U.S. at 707; *see United States v. Arthur Andersen, LLP*, 374 F.3d 281, 293 (5th Cir. 2004) (instruction required only "intent to subvert, undermine, or impede the fact-finding ability of an official proceeding").

Under the applicable standard, error is not harmless "if 'the defendant contested the omitted element and raised evidence sufficient to support a contrary finding.'" *United States v. Conti*, 804 F.3d 977, 981 (9th Cir. 2015) (quoting *Neder v. United States*, 527 U.S. 1, 19 (1999)). Mr. Sullivan vigorously contested whether the decisions and statements he made in responding to the 2016 security incident would even plausibly result in nondisclosure of the 2016 incident to the FTC, and the government's case was riddled with holes on these questions. *Supra* 33-36. A properly instructed jury could easily have found that Mr. Sullivan's conduct, undertaken as he discharged his job responsibilities, was far too attenuated from the FTC proceeding to naturally and probably impede it.

### B. The district court erroneously failed to require the government to prove a duty to disclose to support a conviction based on omissions.

The district court independently erred by permitting the government to seek a conviction based on mere silence, without having to prove that Mr. Sullivan breached any duty to disclose information. Relieved of that obligation, the government argued that Mr. Sullivan obstructed justice because he "never talked about [the incident]" with

in-house lawyers responsible for the FTC response—even though he talked about it extensively with Uber's CEO. 17-ER-3371. It also faulted Mr. Sullivan for not proposing corrections or edits to submissions Uber made to the FTC—submissions drafted by counsel that were never Mr. Sullivan's professional or legal responsibility. 10-ER-2003.

This Court should reject the government's guilt-by-silence theory. As the government conceded, no federal law required Uber—let alone its individual employees—to tell the federal government of the security incident. 6-ER-1096. And fundamental principles of criminal law, the text of § 1505, and case law from analogous statutory contexts all reject criminal liability for mere nondisclosure absent proof of an independent duty to disclose. As with the nexus error discussed above, the government failed to satisfy the duty requirement as a matter of law, and at a minimum, the court's instructional error warrants a new trial.

### 1. Criminal liability under § 1505 cannot rest on pure omissions absent a duty to disclose.

**a.** "[O]ur legal system generally does not impose liability for mere omissions, inactions, or nonfeasance." *Twitter, Inc. v. Taamneh*, 143 S. Ct. 1206, 1220-21 (2023). This is emphatically so in criminal law.

Criminal liability requires either "an act, or an omission to act where there is a legal duty to act," Wayne R. LaFave, *Substantive Criminal Law* § 6:1 (3d ed.)—the latter of which the law regards as "the equivalent of affirmative action," *id.* § 15.4(b).

Congress enacted § 1505 against this common law backdrop. *See United States v. Bailey*, 444 U.S. 394, 415 n.11 (1980) ("Congress in enacting criminal statutes legislates against a background of Anglo-Saxon common law."). Section 1505, as relevant, prohibits individuals from "corruptly … influenc[ing], obstruct[ing], or imped[ing]" an agency proceeding. 18 U.S.C. § 1505, Add.13. The term "corruptly," in turn, is defined in § 1515(b), Add.15. It means: "*[A]cting* with an improper purpose, personally or by influencing another, *including* making a false or misleading statement, or withholding, concealing, altering, or destroying a document or other information." *Id.* § 1515(b), Add.15 (emphasis added).

This statutory definition thus explicitly requires that the defendant "act[]," then enumerates types of acts that are "include[d]." To be sure, as explained above, an "act" may be an affirmative act or it may be a "negative act"—i.e., "the failure to do something that is legally

required," *Act*, *Black's Law Dictionary* (11th ed. 2019). But § 1515(b)'s requirement that the defendant be "acting" means that the provision does not embrace liability for mere *inaction*—i.e., nonfeasance where there is no duty to act. And § 1515(b)'s enumerated types of conduct (false statements, concealment, withholding, and so forth) must be interpreted in accord with that age-old limitation.

**b.** The district court nevertheless rejected the argument that "for the government to convict [Mr. Sullivan] … under an omission-based theory, it must show that he had a specific legal duty to disclose." 1-ER-16. It noted that the definition of "corruptly" refers to "withholding and concealing information … without any reference to a duty to disclose." *Id.* But this reasoning both ignores the common-law principle encoded into § 1515(b), just discussed, and misapprehends the meaning of the statutory terms it relied upon—"withholding" and "concealing." Neither refers to inaction simpliciter.

To "withhold" means "[t]o retain in one's possession that which belongs to or is claimed or sought by another." *Black's Law Dictionary* 1602 (6th ed. 1990); *see also Withhold*, *Webster's Third New International Dictionary* 2627 (1993) (to "refrain from granting, giving,

or allowing," or "to hold back from action"). In the context of a federal agency proceeding, the word "withhold" most naturally criminalizes the act of retaining information that was requested pursuant to a subpoena. After all, the very existence of a "proceeding" under § 1505 depends on the agency's "power to issue subpoenas and compel testimony." *United States v. Kirst*, 54 F.4th 610, 621 (9th Cir. 2022), *cert. denied*, 143 S. Ct. 2681 (2023). It stands to reason that to "act[]" by "withhold[ing]" means to fail to disclose something requested by that power.

Similarly, both the ordinary and customary legal understandings of "concealing" are distinct from bare inaction. To "conceal" means "to *prevent* disclosure or recognition of," *Webster's Third New International Dictionary* 469 (1993) (emphasis added), and therefore connotes active conduct. As for legal understanding, the term tracks the same affirmative act-negative act principle described above. "[N]umerous decisions expressly distinguish between passive concealment—mere nondisclosure or silence—and active concealment." *United States v. Colton*, 231 F.3d 890, 899 (4th Cir. 2000) (tracing history and collecting cases). The latter requires the "affirmative suppression of the truth"; the former does not, and therefore is criminal only where there is an

"independent disclosure duty." *Id.* at 899-900; *accord Rutledge v. Bos. Woven Hose & Rubber Co.*, 576 F.2d 248, 250 (9th Cir. 1978) (recognizing distinction between "silence or passive conduct" and "[t]he affirmative act of denying wrongdoing"); *United States v. Steffen*, 687 F.3d 1104, 1115 (8th Cir. 2012) (similar).

**c.** Case law interpreting analogous criminal statutes regularly recognizes that silence alone cannot support a criminal conviction. For instance, this Court has made clear that while "[m]ail and wire fraud can be premised on either a non-disclosure or an affirmative misrepresentation," "[a] non-disclosure[] … can support a fraud charge only when there exists an independent duty that has been breached by the person so charged." *Eller v. EquiTrust Life Ins. Co.*, 778 F.3d 1089, 1092 (9th Cir. 2015) (internal quotation marks omitted) (addressing 18 U.S.C. §§ 1341, 1343); *see United States v. Shields*, 844 F.3d 819, 822 (9th Cir. 2016) (addressing wire fraud).

The Supreme Court (and this Court) have similarly found that a securities-fraud conviction cannot be premised on "silence" absent a "duty to disclose"—that is, "a relationship of trust and confidence between parties." *See Chiarella v. United States*, 445 U.S. 222, 225,

229-30 & n.3 (1980) (addressing 15 U.S.C. § 78ff(a)); *United States v. Laurienti*, 611 F.3d 530, 543 (9th Cir. 2010) (addressing 18 U.S.C. § 371, 15 U.S.C. § 78j(b), and 15 U.S.C. § 78ff). And the Tenth Circuit has applied this principle to 18 U.S.C. § 1001, the federal false statement statute. To sustain a conviction based on "concealment or nondisclosure" under § 1001, "it [i]s incumbent on the Government to prove that the defendant had [a] duty to disclose." *United States v. Irwin*, 654 F.2d 671, 678 (10th Cir. 1981), *abrogated on other grounds by Kungys v. United States*, 485 U.S. 759 (1988).

Even closer to home for this case, it is long-established that someone cannot be held guilty for misprision of felony based merely on silence, because criminalizing the mere "fail[ure] to report one's knowledge of a felony" is "inconsistent with American values." *United States v. Phillips*, 827 F.3d 1171, 1174-75 (9th Cir. 2016). The rationale driving these decisions is not confined to any particular federal statute. And there is no reason to believe that Congress departed from it in § 1505.

**d.** If there were any doubt, principles of lenity and fair notice would resolve it in favor of a duty requirement. "[T]he canon of strict

construction of criminal statutes, or rule of lenity, ensures fair warning by so resolving ambiguity in a criminal statute as to apply it only to conduct clearly covered." *See, e.g.*, *United States v. Lanier*, 520 U.S. 259, 266 (1997).

Without a duty requirement, § 1505 is effectively boundless. Mr. Sullivan's conviction is hardly the outer limit of a theory with no limiting principle. Under the government's approach, any employee of the subject of an agency proceeding who knows of that proceeding and has information the agency may wish to learn could be prosecuted for not telling the right people at the right times. If Congress wants to impose upon companies or their employees a duty to disclose security incidents to the FTC, it has ample power to do so. It has not. 6-ER-1096 (head of FTC investigation acknowledging no such duty in "federal law"). This Court should not countenance the government's attempt to create such disclosure obligations through ad hoc criminal enforcement.

### 2. The government failed to establish that Mr. Sullivan breached any duty to disclose.

The government failed to satisfy § 1505's duty requirement.

**a.** A duty to disclose can exist by virtue of either "a fiduciary duty"—that is, a relationship of trust and confidence—"or an

independent explicit statutory duty created by legislative enactment," *United States v. Dowling*, 739 F.2d 1445, 1449 (9th Cir. 1984), *rev'd on other grounds sub nom Dowling v. United States*, 473 U.S. 207 (1985); *see also Shields*, 844 F.3d at 822.

The government has never argued that Mr. Sullivan owed a statutory duty. To be sure, *Uber* was duty-bound to respond to formal FTC inquiries issued to *Uber*. 15 U.S.C. § 43. But the FTC specifically instructed Uber, as is typical, that "'You or a duly authorized manager of the company shall certify that the response to this CID is complete.'" 6-ER-1085. Mr. Sullivan was not that designated person. And the FTC "[n]ever received the certification of compliance" from Uber at all. *Id.*

Nor did the government establish that Mr. Sullivan breached some personal fiduciary duty to the FTC. To be sure, it was at pains to exaggerate his role in Uber's response to FTC inquiries, noting that Mr. Sullivan served as Uber's corporate representative at a deposition. *Supra* 8. But it is uncontested that Mr. Sullivan was never responsible for the response to the FTC more generally, *supra* 8, and the government never advanced the dubious proposition that a one-time corporate representative owes an ongoing personal disclosure duty.

The government instead focused on actions it thought Mr. Sullivan ought to have taken *within* Uber—like discuss the 2016 incident with in-house counsel. 17-ER-3371. But Mr. Sullivan's duty as an employee of Uber was to *Uber*, not scattered Uber employees. And he discharged his duty: He reported the information directly to Kalanick, his supervisor and the CEO. Nothing supports the notion that Mr. Sullivan also owed and breached individualized duties to particular Uber employees in different departments from his.

Without a duty to ground its theory of liability-by-silence, the government went to the jury with bare conjecture. Take, for example, its charge that Mr. Sullivan obstructed justice by "sign[ing] off" on a letter Uber sent to the FTC in April 2017 touting Uber's "exhaustive" response to the FTC's inquiry. 6-ER-1022. It is undisputed that Mr. Sullivan played no role in preparing the letter, and that his "signing off" consisted of the following response *six minutes* after receiving the letter in an email attachment: "Letter looks ok to me." 10-ER-2002-05; 3-ER-542. That is because it was not his job to do more.

Or consider the government's assertion that in May 2017, months after the 2016 incident, Mr. Sullivan should have edited a statement in

the FTC's Complaint stating that Uber "ceased storing encrypted personal information on AWS after March 2015." 2-ER-341; *see* 3-ER-688-94 (redlined complaint). There is no evidence that Mr. Sullivan reviewed this particular statement. 3-ER-686-87 (Mr. Sullivan had "not looked at all at the complaint"). Again, it was not his job to do so. *See* 10-ER-2025-31 (in-house counsel describing Mr. Sullivan's role). Not only that, it is undisputed that Candace Kelly, one of the in-house lawyers who was informed of the 2016 incident as it was unfolding, 12-ER-2422, *was* directly responsible for all of these responses to the FTC, *see* 3-ER-542; 3-ER-686-87.

The duty requirement exists to prevent convictions based on equivocal inaction like this.

**b.** The government's theory also cannot be upheld, as the district court erroneously concluded, on the ground that "the government proceed[ed] under a theory of liability under [18 U.S.C. § 2(b)]." 1-ER-18. That provision imposes liability on someone who "willfully causes an act to be done which if directly performed by him or another would be an offense." According to the district court, as long as the government pairs § 2(b) with an obstruction statute, "no … duty is

required." 1-ER-18. All the government would have to show is that the defendant was willfully silent, and that this silence caused A to remain silent despite A's duty to disclose something to B—even though the defendant owed no duty to A or B.

That theory has neither law nor logic to commend it. Just like the government's (and district court's) understanding of § 1505, it violates the axiomatic principle that the law does not criminalize "bad thoughts" alone. LaFave, *supra*, §§ 6.1, 6.1(b). Congress would not have silently cast that principle aside in any case that happens, by fortuity, to involve a fact pattern implicating § 2(b).

Certainly *United States v. Singh*, 979 F.3d 697 (9th Cir. 2020), the lone case the district court relied upon, does not support a § 2(b) theory here. *See* 1-ER-18. Singh provided professional services to various election campaigns, but did not tell them that he was being paid by a third party; he did so knowing that these campaigns were required to disclose the third-party funding source to federal election authorities. 979 F.3d at 707-08, 716-719. So, although Singh had no duty to the federal election authorities, he *did* have a relationship of trust and confidence with the campaigns. His breach of that duty caused the

campaigns to breach theirs. *Id.* Thus, in the one instance where Singh did intimate to a campaign that his funding was "'taken care of,'" he had discharged his own duty, and the evidence was insufficient to convict. *Id.*

The theory in *Singh* could never work here for reasons already explained: Mr. Sullivan discharged any duty he had to disclose information to Uber by providing full information to the CEO of the company. That disclosure is far more robust than the "taken care of" utterance that defeated a charge in *Singh*, and it forecloses the required showing that Mr. Sullivan willfully caused a nondisclosure that violated the law.

Because no rational juror could find that Mr. Sullivan breached an independent duty to disclose, the government's omissions-based theory cannot support a § 1505 conviction. And if this Court agrees that the evidence was also insufficient to establish § 1505's nexus requirement, *supra* 33-37, it must reverse the district court and order acquittal on the obstruction charge as a whole.

### 3. The district court's failure to instruct the jury on the duty to disclose was not harmless.

At a minimum, the district court's failure to instruct the jury on a duty requirement merits a new trial. Omitting this core requirement was "tantamount to" "the omission of an element." *Perez*, 962 F.3d at 441. The government cannot come close to the required showing that this error is harmless "beyond a reasonable doubt." *Id.*

As explained above, the government pointed to no formal legal duty. A jury could also easily have rejected the government's attempts to suggest that Mr. Sullivan was formally or practically responsible for Uber's responses to the FTC. And it likewise could have concluded that Mr. Sullivan satisfied any duty owed to Uber by informing its CEO.

So too a jury could easily have rejected the government's theory under § 2(b). Even beyond the flaws addressed above (at 48-49), the government was required to prove that Mr. Sullivan's silence was willful—that is, done with knowledge that it was unlawful, 16-ER-3356. A jury could have rejected that based on testimony that Mr. Sullivan acted "in good faith," 8-ER-1475; 8-ER-1528, and, again, because Mr. Sullivan informed the head of the company about the incident. *Supra* 12, 15.

In the end, there was ample basis for the jury to doubt that Mr. Sullivan, through ambiguous conduct and inaction, intentionally orchestrated a cover-up of an incident that 30 other independent actors knew about. The obstruction conviction should be overturned.

## II. The Misprision Of Felony Conviction Is Not Supported By Sufficient Evidence And Is Tainted By Improperly Admitted Evidence.

The misprision of felony conviction also cannot stand. A person is guilty of misprision of felony where, "having knowledge of the actual commission of a felony," he affirmatively "conceals" it from law enforcement. 18 U.S.C. § 4, Add.2; *United States v. Ciambrone*, 750 F.2d 1416, 1418 (9th Cir. 1984). The government failed to prove that Mr. Sullivan knew that Glover and Mereacre had violated the CFAA in the face of irrefutable evidence that he and his team reasonably believed that the Bug Bounty agreement had authorized the researchers' conduct. That requires acquittal. *Infra* § A. And at a minimum, a new trial is required because the government persuaded the jury to convict only on the strength of an erroneously admitted and highly prejudicial piece of evidence—Mereacre's own guilty plea agreement. *Infra* § B.

### A. The government failed to prove that Mr. Sullivan believed Glover and Mereacre had violated § 1030 despite Uber's authorization of their conduct.

The government's misprision theory marries two of the most infamous criminal statutes on the books: the "little used and much maligned" crime of misprision, *United States v. Olson*, 856 F.3d 1217, 1222 n.2 (9th Cir. 2017), and the notoriously vague CFAA, § 1030. The former is the unusual statute that requires a defendant to understand the criminal *legal* status of someone else's conduct, *Olson*, 856 F.3d at 1220-25; yet the latter is "remarkably unclear, … with courts and commentators disagreeing sharply as to how much conduct counts and what principle of authorization the statute adopts." Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1562 (2010). It is a poor match.

The incompatibility proves fatal here. The government alleged that Glover and Mereacre violated § 1030 by "access[ing] a computer *without authorization*," *id.* § 1030(a)(2)(C), Add.2-3, and conspiring "to extort … money [through a] threat … to impair the confidentiality of information" obtained "*without authorization*," *id.* § 1030(a)(7)(B), (b), Add.4. 1-ER-53-56 (emphasis added) (jury instructions). But while

Glover and Mereacre arguably *initially* lacked authorization because they did not follow Uber's posted Bug Bounty guidelines, Uber was willing to relax those guidelines and negotiate a Bug Bounty agreement that avoided harm to users. The government's case thus depended on Mr. Sullivan's definitive understanding of an unsettled question of law:

> Where a researcher's access goes beyond what a company's Bug Bounty program authorizes, but the company elects to ratify that access by Bug Bounty agreement, has the defendant violated § 1030's prohibition on access "without authorization"?

Undisputed evidence shows that Mr. Sullivan and his team reasonably understood the answer to be No—and, indeed, that this understanding is fundamental to the Bug Bounty programs that have become indispensable tools for cybersecurity experts. The government failed to refute this belief, meriting acquittal.

### 1. Section 1030 empowers computer owners to decide when and on what terms to authorize access.

Testifying at trial to "his view" of the law, Uber in-house counsel Clark explained why a researcher has not violated § 1030 after entering into a Bug Bounty agreement: "[I]f something is treated as a bug bounty, then, by definition, it wouldn't be considered a data breach"

because "the access would, for all intents and purposes, have been authorized." 11-ER-2213. The government presented no evidence at trial of a contrary view. And as long as Clark's is a "reasonable interpretation" of § 1030, "it would defy history and current thinking to treat" Mr. Sullivan as a "knowing violator" for "adopt[ing]" it, *Safeco Inc. v. Burr*, 551 U.S. 47, 70 n.20 (2007). That reading is not just reasonable—it is the most natural way to interpret § 1030.

Although "authorization" is not defined in § 1030, this Court has interpreted it to mean "'permission or power granted by … authority.'" *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1133 (9th Cir. 2009). And there is no question under the statute *who* the relevant "authority" is: It is the computer owner. Thus, this Court has held in the context of "authorization" of employee access that "[i]t is *the employer's* decision to allow or to terminate an employee's authorization…." *Id.* (emphasis added).

Section 1030, moreover, places no limit on how, when, and in what circumstances a computer owner may authorize access to its systems. It does not limit the purposes for which a computer owner may authorize access. It does not say that a computer owner must give

"prior authorization" or that it may not modify the terms of authorization after initial access. Nor does § 1030 empower courts, prosecutors, or juries to restrict a computer owner's prerogative to authorize access how and when it sees fit. Indeed, this Court has rejected attempts to write "implicit limitation[s] in[to] the word 'authorization.'" *LVRC Holdings*, 581 F.3d at 1133.

This broad recognition of a computer owner's ability to authorize access is essential to sensible regulation in cyberspace. At bottom, the CFAA is a virtual trespass statute, designed to protect computer owners from unwanted intrusions into their computer systems. S. Rep. No. 99-432 at 7-11 (1986). But boundaries are harder to perceive and easier to cross in cyberspace than in the physical world. Ordinary users often transgress them through intentional conduct, but for entirely innocent reasons. *See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" In Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1618-19 (2003). It would be a disastrous—and very possibly unconstitutional—law that treated every misstep as instantly and irretrievably criminal, even when a computer owner willingly decides to permit that access after the fact.

Even the jury appreciated that § 1030 can reasonably be read to avoid that result. It asked by note whether "Uber legally ha[d] the right to extend authorization after the access occurred[.]" 2-ER-358. After the parties disagreed on the answer, the district court simply insructed the jury to reread the jury instructions. 17-ER-3596-602. A legal question that remains so unsettled that *the district court* did not feel comfortable addressing it for the jury can hardly have been settled enough at the time of the 2016 incident to subject *Mr. Sullivan* to criminal liability for adopting a reasonable, commonsense answer. This Court should hold that § 1030 is at least reasonably read to empower a computer owner to authorize a researcher's access after the fact.

### 2. Undisputed evidence establishes Mr. Sullivan and his team's reasonable belief that Uber authorized Glover and Mereacre's access by Bug Bounty agreement.

Extensive and undisputed evidence established that Mr. Sullivan and his team understood Uber to have broad power to authorize access to its systems, and to have exercised that power with respect to Glover and Mereacre's access. This "subjective belief" establishes inescapable doubt as to Mr. Sullivan's knowledge of a felony. *Olson*, 856 F.3d at 1224 n.5 (internal quotation marks omitted).

***Uber broadly authorized researchers to access its system.***

As explained above (at 9-11), the very premise of a Bug Bounty program is that a computer owner may permit outsiders onto its systems, without threat of legal sanction, for purposes of discovering and disclosing a security vulnerability. Uber's Bug Bounty program did just that. It invited "anybody on the internet," 9-ER-1784, to share with Uber "any vulnerability that could negatively affect the security of [its] users," 3-ER-476; 3-ER-474-75. And its program guidelines advertised, "[i]f you get access to an Uber server, please report it to us[,] and we will reward you with appropriate bounty." 3-ER-479; 9-ER-1796.

The cybersecurity professionals on Mr. Sullivan's team were devoutly committed to this concept. Collin Greene, an engineer on Uber's team, had "started the Facebook [program]" while working under Mr. Sullivan. 15-ER-3045. He saw these programs as "good for the company, and … good for the world." *Id.* Government witness Rob Fletcher, who ran Uber's program in 2016, recalled the bygone era where researchers who "tried to report" a vulnerability might face "civil or criminal legal action." 9-ER-1776-77. And he extolled the modern

"best practice[]": "Embrace security researchers that are reporting vulnerabilities to you." 9-ER-1777.

In short, it was an article of faith among Mr. Sullivan and his team that Uber had broad discretion to authorize researchers to access its system.

***Uber considered the terms of its Bug Bounty authorization to be flexible.*** Undisputed evidence also established that Uber viewed the guidelines it set for inviting researchers onto its system as subject to modification after access had occurred. Fletcher confirmed without dispute that Uber's "guidelines were considered to be flexible." 9-ER-1798-99. He agreed that "if somebody violates th[e] guidelines" it would not be "out of the ordinary for Uber to still treat it as a bug bounty." *Id.* Greene concurred that the "rules exist in service of" the "bug bounty program"—so even if someone "went against" them, Uber could "treat it as a bug bounty … if it wanted to." 15-ER-3053. The team's view was thus that Uber had the power to ratify the researchers' technically unauthorized access after that access occurred.

***Uber did not regard researchers who entered into Bug Bounty agreements as criminals.*** As explained above (at 54), Mr.

Sullivan and his team also believed, per in-house counsel's advice, that "if something is treated as a bug bounty," "the access would, for all intents and purposes, have been authorized." 11-ER-2213. And authorized access is not access "without authorization," § 1030(a)(2)(C), Add.2-3.

Contemporaneous evidence of Uber's response to the 2016 incident confirms that Mr. Sullivan and his team did in fact view the legality of Glover and Mereacre's conduct as turning on a Bug Bounty agreement. If Uber could not reach an agreement, its incident plan called for treating Glover and Mereacre's access as a security breach, and Uber would "notify FBI/govt. within 3 days." 3-ER-538. Clark and Uber's Head of Investigations, Matt Henley, confirmed to HackerOne, a third-party company that helped operate Uber's Bug Bounty program, that Uber "expected to report to law enforcement" if Glover and Mereacre "didn't cooperate." 13-ER-2675. The Bug Bounty agreement is what altered the analysis—after Uber entered into it and the researchers honored their promises, no one suggested that they should still be regarded as criminals.

***Uber duly authorized Glover and Mereacre's access—with CEO approval.*** Last, when it came to the 2016 incident, Uber's authorization of Glover and Mereacre's access through a Bug Bounty agreement was an organizational effort with approval from the very top of the company.

Irrefutable evidence shows that as Mr. Sullivan and his team pursued a Bug Bounty agreement, Mr. Sullivan kept CEO Kalanick constantly informed. The day after Uber was first contacted by the researcher, Mr. Sullivan told Kalanick that Uber would "engage tomorrow on bounty and amount." 3-ER-515. Kalanick confirmed that "resources can be flexible"—referring to the amount—if the team had "certainty" that "he can truly treat this as a [bug] bounty situation." *Id.* And as Mr. Sullivan kept Kalanick informed, several other members of the team, including Clark and Henley, worked on logistics with HackerOne. 13-ER-2650-60.

Fortunately, the two sides reached a mutually agreeable deal. Kalanick, the company's head decisionmaker, approved of the agreement. Mr. Sullivan told Clark that the "A Team"—the executive team headed by Kalanick—had "made th[e] decision." 11-ER-2113. Mr.

Sullivan would later explain to outside counsel that Kalanick "signed off on the [$]100K" agreement. 3-ER-749. Even Mereacre "knew that Uber's CEO had personally approved th[e] payment to [him]." 9-ER-1729. Once Fletcher signed the agreement on behalf of Uber, Mr. Sullivan forwarded it to Kalanick immediately. 3-ER-539. Among the agreement's provisions was one that Fletcher explained was commonplace for any Bug Bounty agreement, 9-ER-1778: "We … will not seek civil or criminal remedies against you for activity and research that you have disclosed to us." 3-ER-540.

### 3. The government failed to contradict evidence of Mr. Sullivan and his team's reasonable belief.

The government could offer no evidence to refute this reading of § 1030, *supra* 54-57, or the undisputed understanding of Mr. Sullivan and his team, *supra* 57-62. No rational juror could have lacked doubt as to Mr. Sullivan's belief that Glover and Mereacre were felons, and the district court erred in finding otherwise, *see* 1-ER-23. *See United States v. Martinez*, 122 F.3d 1161, 1165-66 (9th Cir. 1997) (reversing where the government's showing was "too ambiguous and too weak" to overcome "undisputed evidence").

**a.** Because there was no evidence that anyone at Uber believed that Glover and Mereacre had violated § 1030 notwithstanding the Bug Bounty agreement, the government largely elided the key issue. For example, it emphasized that Mr. Sullivan was a former cybercrime prosecutor, and it introduced plea agreements he had supervised in which defendants admitted to § 1030 violations. 14-ER-2820-27; 17-ER-3440; *see* 1-ER-23 (district court relying on Mr. Sullivan's prior career experience). But none of the pleas involved defendants who had entered into Bug Bounty agreements, because that had never happened in one of Mr. Sullivan's cases or any other the government could point to.

Similarly, the government highlighted statements by Mr. Sullivan and other security team members that Glover and Mereacre's conduct felt extortionate, *supra* 11, 19, 53; *see, e.g.*, 3-ER-738; 17-ER-3421 (Mr. Sullivan); 8-ER-1440 (Chief Information Security Officer John Flynn), or Mr. Sullivan's later statement that an "unauthorized party gained access," 1-ER-23 (district court noting Mr. Sullivan's statement). But no one disputes that Glover and Mereacre's access was *initially* outside of the authorization granted by Uber's Bug Bounty guidelines. As explained above, Uber absolutely would have regarded their access as

unauthorized under § 1030 if Uber did not reach a Bug Bounty agreement. *Supra* 59-60. But it did reach an agreement, and the government produced evidence of no one who regarded Glover and Mereacre's access as unauthorized *after* that. *Supra* 54, 59-60.

The government also employed the constant refrain that the use of a Bug Bounty agreement in this situation was unusual or novel. It pointed to the size of the bounty payment; the fact that Glover and Mereacre had not followed Uber's Bug Bounty guidelines; and Uber's use of an accompanying NDA. 17-ER-3370. Fletcher—a government witness and the person most familiar with Uber's Bug Bounty program—rejected all this point for point. 10-ER-1842 (amount "was in line with the impact overall"); 13-ER-1798-99 (guidelines "were considered to be flexible"); 10-ER-1842 (NDAs are "not uncommon").

But it is irrelevant anyway. As Greene testified, *supra* 58-59, Uber's Bug Bounty guidelines are Uber's to modify as it wishes. Here it did so, with CEO approval, in order to successfully safeguard its own systems and protect user data. That some employees (wrongly) questioned whether Uber *should have* made a Bug Bounty agreement, or that the government (inexplicably) second guesses that decision *now*,

is utterly irrelevant to Mr. Sullivan's understanding of the legal effect of the agreement once Uber entered into it.

**b.** The government also cannot defend the verdict based on the other § 1030 violation it used as a predicate—the charge of *conspiracy* "to extort … money [through a] threat to… impair the confidentiality of information" obtained through unauthorized access, *id.* § 1030(a)(7)(B), (b), Add.4. That is a non-starter, as the government apparently realized in declining to defend the verdict on this basis post-trial. *See* 2-ER-343-44.

The reason is simple: There is no evidence that, at the time he undertook what the government claims are acts of concealment, Mr. Sullivan knew anything of the nature of Glover and Mereacre's partnership. Though Uber would eventually learn about the two individuals involved, *supra* 12-13, it had no confirmation of their identities or relationship as the incident unfolded. Certainly no one knew who had played what role in identifying the vulnerability and communicating with Uber, let alone the details of their agreement with one another.

To be guilty of misprision, a defendant must have "full knowledge" of actual commission of a felony. *Ciambrone*, 750 F.2d at 1417. Suspicion is not enough. And to *know* that two other people have actually engaged in an unlawful conspiracy, Mr. Sullivan would have had to know more than that two people "met, discussed matters of common interests, acted in similar ways, or perhaps helped one another." 16-ER-3353 (jury instructions). None of that is a conspiracy. *Id.* He would have to know definitively that Glover and Mereacre had agreed to commit a crime together. He had no such knowledge, and the government did not and could not prove otherwise.

Because the government failed to overcome unmistakable doubt concerning Mr. Sullivan's knowledge of the actual commission of a felony, the misprision conviction should be reversed.

### B. The district court abused its discretion by admitting Mereacre's guilty plea agreement as substantive evidence of Mr. Sullivan's guilt.

The misprision conviction must be overturned for the independent reason that the district court improperly allowed the government to introduce Mereacre's guilty plea agreement. *See* 3-ER-702-13 (plea agreement). It is no mystery why the government wanted to admit that

agreement, rather than just prove up Glover and Mereacre's underlying conduct. Apart from Mereacre's plea, the government could point to no instance of anyone being convicted of a § 1030 violation after entering into a Bug Bounty agreement. Mereacre's plea agreement gave the government's theory an air of legitimacy—in the government's words, its "value" was that "it was presented to a court and accepted." 9-ER-1607.

The district court permitted this gambit without limitation, not only admitting the plea agreement, but rejecting Mr. Sullivan's request for an instruction that the plea could not be considered as substantive evidence of his guilt. 2-ER-383-89 (motion in limine), 9-ER-1605-1609 (renewing objection). This was an abuse of discretion under Rule 403. And far from harmless, the error allowed the government to sway the jury on a critical issue—Mr. Sullivan's knowledge of the actual commission of a felony—on which its evidence was woefully deficient.

#### 1. The district court admitted Mereacre's plea agreement for the improper purpose of establishing Mr. Sullivan's guilt.

**a.** Federal Rule of Evidence 403 calls for exclusion of evidence when its "probative value is substantially outweighed by [the] danger

of … unfair prejudice." Add.15. For more than a century, courts have recognized the dangers of admitting another person's guilty plea in a criminal case as substantive evidence of the guilt of the accused. Doing so denies "the right of every defendant to stand or fall with the proof of the charge made against him, not against somebody else." *United States v. Toner*, 173 F.2d 140, 142 (3d Cir. 1949); *Baker v. United States*, 393 F.2d 604, 614 (9th Cir. 1968) (citing *Toner*'s rationale); *Babb v. United States*, 218 F.2d 538, 542 (5th Cir. 1955); *State v. Bowker*, 38 P. 124, 124-25 (Or. 1894). This Court has thus repeatedly recognized the "general rule … that guilty pleas of co-defendants cannot be considered as evidence [of] those on trial." *Baker*, 393 F.2d at 614; *see United States v. Halbert*, 640 F.2d 1000, 1004 (9th Cir. 1981) (same).

The district court thought this principle applicable only in cases that "involve co-defendants or co-conspirators," where "prejudice … is obvious." 1-ER-88. It perceived no prejudice at all flowing from Mereacre's plea because Mr. Sullivan was being tried for a "separate crime than what the hackers pleaded guilty to." *Id.*

Neither case law nor logic supports this categorical restriction. The danger of admitting a guilty plea is that jurors may reflexively

credit the plea and the underlying admissions it reflects rather than basing the verdict "upon the evidence against [the defendant]." *Baker*, 393 F.2d a 614. That risk is only heightened when the government seeks to introduce a formal plea agreement, because jurors are "apt to give exaggerated weight to a judgment." *Greycas, Inc. v. Proud*, 826 F.2d 1560, 1567 (7th Cir. 1987); *cf. United States v. Awadallah*, 436 F.3d 125, 133 (2d Cir. 2006) (recognizing the "real risk that the trial jury will give undue weight" to grand jury testimony). That a jury will accord a plea agreement such undue weight only as to *some* of the essential elements of a criminal offense rather than *all* of them hardly makes it less problematic.

Here, the government, with the court's approval, used Mereacre's plea agreement to precisely the effect the law disapproves. Its avowed purpose was to rebut the defense's arguments "that what happened here wasn't a crime," 9-ER-1606—in other words, the government used it as a stand-in for evidence that Glover and Mereacre had committed a felony. *See also* 2-ER-433 (government opposition to motion in limine). The plea agreement contained a lengthy narrative of Mereacre's admitted-to conduct, and Mereacre's admission that this conduct

satisfied each of the elements of "§ 1030(a)(7)(B) and (c)(3)(A)," including "conspiracy," "extortion," and "information obtained from a protected computer without authorization." 3-ER-703-06. So rather than prove the unsettled question at the heart of this case—whether Glover and Mereacre's conduct was a felony in spite of the Bug Bounty agreement—the government misled the jury into thinking the issue had been finally resolved.

This same unfair inference almost certainly influenced the jury as to the all-important question whether Mr. Sullivan *believed* that Glover's and Mereacre's conduct violated § 1030. Recall that the government's principal strategy on this element was to imply that Mr. Sullivan must have known Glover and Mereacre committed a felony because he had been a cybercrime prosecutor. *Supra* 63. Yet it could point to no conviction for a violation of § 1030 despite an agreement that had ratified the defendant's initially unauthorized conduct. Mereacre's plea agreement was a perfect illusion: It suggested that a § 1030 violation was so obvious in these circumstances that even the defendant (Mereacre) admitted to it.

In short, the district court allowed the government to use the plea agreement for a manifestly improper purpose. The government should have had to prove all of the elements of the charge against Mr. Sullivan based on actual evidence. Instead, it was allowed to base a conviction against Mr. Sullivan on "the result of a [proceeding] over which he had no control, to which he was not a party, and in which he had no right to appear or make a defense," *Bowker*, 38 P. at 125.

**b**. Largely ignoring the above considerations, the district court held that the "risk of prejudice" did not "substantially outweigh the probative value of the evidence." 1-ER-88-89. But apart from the improper purpose that was the government's principal aim, the probative value of the plea agreement was virtually nil.

To begin with, while *commission* of a felony is of course an element of misprision of felony, the government was not required to demonstrate Mereacre or Glover's *conviction* of a felony. 16-ER-3350 (jury instructions). The plea agreement was therefore not necessary as a record of conviction. *Cf. Old Chief v. United States*, 519 U.S. 172 (1997) (addressing admission of guilty plea for that purpose). Nor did the plea agreement have probative value for purposes of proving the

truth of any underlying facts themselves. The government elicited extensive testimony from Mereacre concerning the 2016 incident, spanning more than 100 pages in the transcript. *See* ER-1629-732.

Beyond this, the government argued the guilty plea was relevant to evaluate "'the credibility of [Mereacre].'" 2-ER-434; *see also* 9-ER-1607. But of course that rationale could never justify admitting the plea agreement as *substantive* evidence of Mr. Sullivan's guilt, as the district court permitted.

This Court "ha[s] long held that '[w]here the evidence is of very slight (if any) probative value, it's an abuse of discretion to admit it if there's even a modest likelihood of unfair prejudice or a small risk of misleading the jury.'" *United States v. Preston*, 873 F.3d 829, 841 (9th Cir. 2017). That is so here.

**2. Admission of Mereacre's plea was not harmless.**

The admission of Mereacre's plea agreement was prejudicial and warrants a new trial on the misprision charge. *United States v. Martin*, 796 F.3d 1101, 1105 (9th Cir. 2015) (vacating convictions because improperly admitted evidence "more likely than not affected the verdict").

As already explained (at 69-70), the government introduced the plea agreement as proof that Glover and Mereacre's conduct violated § 1030 notwithstanding the Bug Bounty agreement. As the government put it in closing: "Brandon Glover and Vasile Mereacre committed these felonies. Vasile admitted it. He testified that he admitted to it. You saw his guilty plea to it." 17-ER-3440.

The jury almost certainly accepted that improper invitation, because the plea agreement was all the government offered it. Again, the jury appreciated the unsettled question at the heart of the case, asking the district court whether "Uber legally ha[d] the right to extend authorization after the access occurred[.]" 2-ER-358. After the district court declined to answer, the jury found a way to convict—almost certainly on the basis of Mereacre's plea agreement.

Similarly, the plea agreement likely prejudiced Mr. Sullivan in the jury's determination of whether he knew that a felony had been committed. The government charged Mr. Sullivan with misprision of a felony under a notoriously vague statute, based on circumstances that had never before generated a prosecution or conviction. Witness after witness took the stand, and not one said they believed Glover and

Mereacre's access was still unauthorized after the Bug Bounty agreement. The only thing that supported the government's suggestion that it should have been obvious that Glover and Mereacre's conduct violated § 1030 was Mereacre's plea agreement saying so. If this Court does not reverse, it should at a minimum order a new trial.

## CONCLUSION

For the reasons stated, this Court should reverse the convictions on both counts; at a minimum, it should order a new trial.

Respectfully submitted,

*/s/Aravind Swaminathan*

Aravind Swaminathan
ORRICK, HERRINGTON & SUTCLIFFE LLP
401 Union Street, Suite 3300
Seattle, WA 98101
(206) 839-8400

Christopher J. Cariello
ORRICK, HERRINGTON & SUTCLIFFE LLP
51 West 52nd Street
New York, NY 10019

Amari L. Hammonds
ORRICK, HERRINGTON & SUTCLIFFE LLP
355 S. Grand Avenue, Suite 2700
Los Angeles, CA 90071

*Counsel for Defendant-Appellant Joseph Sullivan*

October 10, 2023

**UNITED STATES COURT OF APPEALS**
**FOR THE NINTH CIRCUIT**

**Form 17. Statement of Related Cases Pursuant to Circuit Rule 28-2.6**

*Instructions for this form: http://www.ca9.uscourts.gov/forms/form17instructions.pdf*

**9th Cir. Case Number(s)** 23-927

The undersigned attorney or self-represented party states the following:

[ X ] I am unaware of any related cases currently pending in this court.

[ ] I am unaware of any related cases currently pending in this court other than the case(s) identified in the initial brief(s) filed by the other party or parties.

[ ] I am aware of one or more related cases currently pending in this court. The case number and name of each related case and its relationship to this case are:

**Signature** *s/ Aravind Swaminathan* **Date** October 10, 2023

*(use "*s/[typed name]*" to sign electronically-filed documents)*

**UNITED STATES COURT OF APPEALS**
**FOR THE NINTH CIRCUIT**

**Form 8. Certificate of Compliance for Briefs**

*Instructions for this form: http://www.ca9.uscourts.gov/forms/form08instructions.pdf*

**9th Cir. Case Number(s)** 23-927

I am the attorney or self-represented party.

**This brief contains 13,877 words,** excluding the items exempted by Fed. R. App. P. 32(f). The brief's type size and typeface comply with Fed. R. App. P. 32(a)(5) and (6).

I certify that this brief *(select only one)*:

[X] complies with the word limit of Cir. R. 32-1.

[ ] is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

[ ] is an **amicus** brief and complies with the word limit of Fed. R. App. P. 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

[ ] is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

[ ] complies with the longer length limit permitted by Cir. R. 32-2(b) because *(select only one)*:
[ ] it is a joint brief submitted by separately represented parties;
[ ] a party or parties are filing a single brief in response to multiple briefs; or
[ ] a party or parties are filing a single brief in response to a longer joint brief.

[ ] complies with the length limit designated by court order dated _____.

[ ] is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

**Signature** *s/ Aravind Swaminathan* **Date** October 10, 2023
*(use "*s/[typed name]*" to sign electronically-filed documents)*