App. A

FOR PUBLICATION

UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT

UNITED STATES OF AMERICA, *Plaintiff - Appellee*, v. JOSEPH SULLIVAN, *Defendant - Appellant*.	No. 23-927 D.C. No. 3:20-cr-00337-WHO-1 ORDER AND AMENDED OPINION

Appeal from the United States District Court
for the Northern District of California
William Horsley Orrick, District Judge, Presiding

Argued and Submitted October 8, 2024
San Francisco, California

Filed March 13, 2025
Amended November 12, 2025

Before: M. Margaret McKeown, Anthony D. Johnstone, and Ana de Alba, Circuit Judges.

Order;
Opinion by Judge McKeown

SUMMARY*

Criminal Law

The panel filed (1) an order amending its March 13, 2025, opinion and denying a petition for rehearing en banc; and (2) an amended opinion affirming Joseph Sullivan's jury conviction for obstruction of justice and misprision of a felony arising from his efforts, while the Chief Security Officer for Uber Technologies, to cover up a major data breach even as Uber underwent investigation by the Federal Trade Commission into the company's data security practices.

Sullivan argued that the district court erred in rejecting two of his proposed jury instructions regarding the obstruction charge.

- The panel held that *United States v. Bhagat*, 436 F.3d 1140 (9th Cir. 2006), forecloses Sullivan's argument that the district court erred by rejecting an instruction that would have required the jury to find that there was a "nexus" between his conduct and the pending FTC proceeding. The panel explained that Supreme Court cases cited by Sullivan are not clearly irreconcilable with *Bhagat*.
- Regarding Sullivan's contention that the district court erred by rejecting his "duty to disclose" instruction, the panel held that any error was harmless beyond a reasonable doubt. Sullivan

* This summary constitutes no part of the opinion of the court. It has been prepared by court staff for the convenience of the reader.

argued that, because this proposed instruction was not given, the jury may have convicted on a theory—inaction by a defendant under no duty to disclose—that was invalid under 18 U.S.C. § 1505, and that the verdict must be set aside because it is impossible to tell which ground the jury selected. The panel concluded that there is no reasonable possibility that the jury rested its conviction on the § 1505 charge based *only* on the claimed invalid theory and not *also* on a concededly valid causing-to-be-done theory, which rests on 18 U.S.C. § 2(b). The panel therefore did not need to reach the question of validity under § 1505.

Sullivan argued that the evidence of his alleged misprision was insufficient as a matter of law. Misprision is the crime of "having knowledge of the actual commission of a felony" and "conceal[ing]" or failing to "as soon as possible make known the same to some judge or other person in civil or military authority under the United States." To establish misprision, the government is obliged to show that the principal committed and completed the felony alleged. Here, that meant proving that hackers had intentionally accessed Uber's computers without authorization and thereby obtained information from those protected computers, in violation of the Computer Fraud and Abuse Act (CFAA).

- The panel held that the hackers' illegal conduct could not be laundered through Uber's *post hoc* authorization, via a non-disclosure agreement (NDA), of their computer access.

- The panel held that the evidence does not support Sullivan's claim that, even if the hackers were

unauthorized within the meaning of the CFAA, he reasonably believed that the NDA cleansed the felonious access of its illegality.

- The panel held that a rational jury could have found that Sullivan, who had been an Assistant U.S. Attorney in a "Computer Hacking and IP Unit," knew that the conduct in question was a felony punishable by more than a year in prison.

The panel held that the district court did not abuse its discretion in permitting the introduction of the guilty plea agreement signed by one of the hackers. Any unfair prejudice did not substantially outweigh the probative value.

COUNSEL

Ross D. Mazer (argued) and Andrew F. Dawson, Assistant United States Attorneys; Merry Jean Chan, Chief, Appellate Section, Criminal Division; Matthew M. Yelovich, Attorney for the United States Acting Under Authority Conferred by 28 U.S.C. § 515; Craig H. Missakian, United States Attorney; Office of the United States Attorney, United States Department of Justice, San Francisco, California; for Plaintiff-Appellee.

Christopher J. Cariello (argued) and Eliza Lehner, Orrick Herrington & Sutcliffe LLP, New York, New York; Aravind Swaminathan, Orrick Herrington & Sutcliffe LLP, Seattle, Washington; Amari L. Hammonds, Orrick Herrington & Sutcliffe LLP, Los Angeles, California; for Defendant-Appellant.

Jeffrey R. Babbin and Nathan J. Guevremont, Wiggin & Dana LLP, New Haven, Connecticut; Anjali Dalal, Wiggin and Dana LLP, New York, New York; Gia L. Cincone, NACDL Amicus Committee, San Francisco, California; for Amici Curiae National Association of Criminal Defense Lawyers and Due Process Institute.

Nathan R. Morales, Stoel Rives LLP, Portland, Oregon; Matthew D. Segal, Stoel Rives LLP, Sacramento, California; for Amici Curiae Cloud Security Alliance and Security Innovation Network.

ORDER

The opinion filed March 13, 2025, is hereby amended. The amended opinion will be filed concurrently with this order. Judge Johnstone and Judge de Alba have voted to deny the petition for rehearing en banc, and Judge McKeown has so recommended. The petition for rehearing en banc is **DENIED**. Dkt. No. 92. No future petitions for rehearing or rehearing en banc will be entertained.

IT IS SO ORDERED.

OPINION

McKEOWN, Circuit Judge:

Cybersecurity has become a major preoccupation of businesses as network hacks and data breaches multiply. Companies now turn to seasoned experts to address these challenges. Among the ranks of these experts is Joseph Sullivan, who served as the Chief Security Officer ("CSO") for Uber Technologies ("Uber") from 2015 to 2017. When he began at Uber, Sullivan's reputation was that of a "world-class" cybersecurity expert, with a stint as an Assistant U.S. Attorney and several years of private-sector leadership experience under his belt. This case arose from choices Sullivan made as Uber's CSO in the wake of a major data breach—specifically, his efforts to cover up that breach, even as Uber underwent investigation by the Federal Trade Commission ("FTC") into the company's data security practices.

When the breach and its cover-up came to light after having remained hidden for over a year, the government brought criminal charges against Sullivan. A jury convicted him of obstruction of justice and misprision of a felony. On appeal, Sullivan challenges several jury instructions, the sufficiency of the evidence, and an evidentiary ruling. We affirm.

Background

In 2014, Uber experienced a data breach. A hacker discovered an Amazon Web Services (AWS) "key"—a type of log-in—embedded in code displayed publicly on GitHub, a platform on which developers store and sometimes share code. The hacker used the key to access the troves of data

that Uber stored privately on AWS. From the AWS database, the hacker downloaded sensitive information pertaining to tens of thousands of Uber drivers.

Shortly after this breach became public, the FTC commenced an investigation into Uber's data security practices, including its storage of rider and driver information on AWS and the company's "alleged deceptive statements" about those practices.

In 2015, Uber hired Sullivan as its CSO. In August 2016, Sullivan took on the additional title of Deputy General Counsel. By then, Sullivan was very involved in Uber's response to the FTC's ongoing investigation: He made a presentation to FTC staff on Uber's data security program, and he testified before the Commission in an investigational hearing, including on Uber's practices of data encryption. He also supervised the preparation of at least two of Uber's official statements to the FTC.

Another data breach occurred in October 2016. Hackers gained access to Uber's private account on GitHub—the same platform as in the 2014 attack. Embedded in the code stored in that account, the hackers found AWS keys—the same types of keys, discovered in a similar way, as in the 2014 attack. The hackers used the keys to access Uber's AWS datastore and download the names and driver's license numbers of some 600,000 individuals—the same type of breach on the same infrastructure, at an even larger scale, as in the 2014 attack. The downloaded data was unencrypted.

Despite the similarities between the 2016 incident and the 2014 incident that the FTC was already investigating, no one at Uber informed the FTC of this new breach. Instead, unbeknownst to federal officials, Sullivan and a group of Uber staffers decided to track down the hackers and pressure

them into signing a non-disclosure agreement ("NDA") that purported to re-characterize the hack as "research" into "vulnerabilities" under Uber's Bug Bounty Program. Through bug bounty programs, companies solicit and reward external security researchers' discovery and disclosure of their systems' vulnerabilities. *See* Jasmine Arooni, *Debugging the System: Reforming Vulnerability Disclosure Programs in the Private Sector*, 73 Fed. Comm. L.J. 443, 448–50 (2021). In ostensible exercise of the Bug Bounty Program, Uber paid the hackers $100,000 in exchange for their signatures on an NDA and an agreement to delete the downloaded data. Sullivan was involved in drafting the NDA and ultimately informed Travis Kalanick, then Uber's Chief Executive Officer, that the hackers had signed the "contract."[1] Sullivan did not inform Uber's general counsel of these developments, despite telling other employees to the contrary.

Sullivan also did not correct old statements, and instead signed off on new statements, to the FTC that Uber's stores of private data on AWS were encrypted, even though the breach had exposed the fact that some of this data was unencrypted. Sullivan did so despite his and his team's awareness that he "was just deposed on this specific topic" and that news of the breach would "play very badly based on previous assertions" to the FTC about data encryption. In the fall of 2017, Uber hired a new CEO, Dara Khosrowshahi. Soon after, Sullivan informed Khosrowshahi of the hack, but he omitted and misrepresented key details: He falsely stated that no data had been downloaded; mischaracterized the

[1] The NDAs were initially signed with the hackers' pseudonyms. After further investigation by Uber, the agreements were subsequently re-signed with the hackers' real names.

timing of the payment to the hackers; and omitted the magnitude of the breach and the amount of money paid to resolve it. When Khosrowshahi discovered the truth, he fired Sullivan and publicly disclosed the breach.

Upon learning of the breach, the FTC revised its complaint against Uber, withdrew acceptance of its original consent agreement with Uber, and prepared a new consent agreement that would impose additional reporting obligations on Uber. The revised complaint specifically referenced the 2016 data breach and the state of Uber's data security as of November 2016.

Meanwhile, federal prosecutors brought felony charges against one of the hackers, Vasile Mereacre, for violating the Computer Fraud and Abuse Act ("CFAA"), 18 U.S.C. § 1030. In 2019, Mereacre pled guilty. Criminal charges were also brought against Sullivan. Sullivan was then tried and convicted for obstruction of justice and misprision of a felony. After sentencing, Sullivan moved for a judgment of acquittal or a new trial on the grounds that the district court erred in formulating the jury instructions and in admitting Mereacre's guilty plea into evidence; and that the evidence of his conviction was insufficient as a matter of law. The court denied his motion. We have jurisdiction under 28 U.S.C. § 1291.

Analysis

I. The Jury Instructions—Obstruction Conviction

Sullivan claims error with respect to two of his proposed jury instructions regarding the obstruction conviction—the "nexus" instruction and the "duty to disclose" instruction.

A. Nexus Instruction

We review de novo the district court's rejection of Sullivan's proposed "nexus" instruction, which would have required the jury to find that "there was a nexus between the defendant's conduct and the pending FTC proceeding."[2] *United States v. Munoz*, 412 F.3d 1043, 1046 (9th Cir. 2005) (reviewing de novo a claim that "a jury instruction misstated an element of the charged offense"). The proposed instruction did not define "nexus."

Section 1505 provides that "[w]hoever corruptly, or by threats or force, or by any threatening letter or communication influences, obstructs, or impedes or endeavors to influence, obstruct, or impede the due and proper administration of the law under which any pending proceeding is being had before any department or agency of the United States . . . [s]hall be fined under this title, imprisoned not more than 5 years or, if the offense involves international or domestic terrorism (as defined in [S]ection 2331), imprisoned not more than 8 years, or both." 18 U.S.C. § 1505.

In accord with the statutory language, the jurors were instructed: "For the defendant to be found guilty [under Section 1505], the government must prove each of the following elements beyond a reasonable doubt: First, there was a proceeding pending before a department or agency of the United States; Second, the defendant was aware of the proceeding; and Third, the defendant intentionally

[2] After some back-and-forth, the parties ultimately agreed that a Section 1505 conviction necessitates a *finding* of a nexus between the allegedly obstructive conduct and the pending proceeding. They continue to disagree as to whether an additional *instruction* as to a nexus finding was required.

endeavored corruptly to influence, obstruct, or impede the pending proceeding." This instruction precisely mirrors the elements of Section 1505, as spelled out in *United States v. Price*, 951 F.2d 1028, 1031 (9th Cir. 1991) ("First, there must be a proceeding pending before a department or agency of the United States. Second, the defendant must be aware of the pending proceeding. Third, the defendant must have intentionally endeavored corruptly to influence, obstruct or impede the pending proceeding." (citations omitted)).

Ninth Circuit precedent forecloses Sullivan's argument. We held in *United States v. Bhagat* that there is no "need to supplement the *Price* instructions with additional elements," including a "nexus" element, for a conviction under Section 1505. 436 F.3d 1140, 1148 (9th Cir. 2006).

Sullivan's counsel candidly acknowledged: "the Ninth Circuit has held in a [Section] 1505 case that *Aguilar*'s nexus requirement did not require a separate jury instruction to that effect." Sullivan asks us to overrule *Bhagat*, claiming that we have authority to do so because the case is "clearly irreconcilable" with intervening Supreme Court precedent. *Miller v. Gammie*, 335 F.3d 889, 900 (9th Cir. 2003) (en banc). Sullivan cites three cases that he construes as irreconcilable: *United States v. Aguilar*, 515 U.S. 593 (1995); *Arthur Andersen LLP v. United States*, 544 U.S. 696 (2005); and *Marinello v. United States*, 584 U.S. 1 (2018).

Although these cases support either a "nexus" requirement or "nexus" instruction in their respective contexts, none is clearly irreconcilable with *Bhagat*. To begin, none of the cases concerns Section 1505. And, in each case, the statutes, facts, or jury instructions created ambiguities that called for clarification as to the existence of a "nexus." No such ambiguities exist in *Bhagat* or here.

The Section 1503 charge in *Aguilar* involved a defendant's statement in an investigation that was "ancillary" to the proceeding covered by the statute. *Aguilar*, 515 U.S. at 599–601. The attenuation in the relationship between Aguilar's act and the covered proceeding necessitated the Court's clarification of Section 1503's implicit "nexus" requirement. *Id.* at 599. The Court in *Aguilar* explicitly did not address jury instructions. *Id.* at 606.

Nor are the other cases cited by Sullivan irreconcilable with *Bhagat*. In *Marinello* the prosecution was brought under the Omnibus Clause of Section 7212(a) of the Internal Revenue Code. 26 U.S.C. § 7212(a). That provision does not refer to a "proceeding," but only to "the due administration of [the Internal Revenue Code]." 26 U.S.C. § 7212(a). The district court "did not instruct the jury that it must find that Marinello knew he was under investigation and intended corruptly to interfere with that investigation." *Marinello*, 584 U.S. at 5. Given the statute's silence and the lack of jury instruction as to either the defendant's awareness of, or intended effect upon, any investigation, the Court clarified that the Omnibus Clause requires instruction that the government must show a "'nexus' between the defendant's conduct and a particular administrative proceeding." *Id.* at 13. Even if *Arthur Andersen* is intervening authority, and we are dubious that it is, the jury instructions in that Section 1512 case erroneously conveyed that the defendant need not even have "ha[d] in contemplation any particular official proceeding." 544 U.S. at 708.

The text of Section 1505, the wording of the *Price* instructions, and the factual relevance of only one proceeding distinguish *Bhagat* from *Aguilar*, *Marinello*, and *Arthur Andersen*. Like *Bhagat*, this case involved only one

proceeding, of which the defendant was undisputedly aware. Under *Bhagat*, the *Price* elements require a nexus by implication, and no other jury instruction given here undermined or contradicted that implication. Sullivan was not entitled to an additional instruction that "merely duplicates" what the jury had already been told. *United States v. Lopez-Alvarez*, 970 F.2d 583, 597 (9th Cir. 1992). Consistent with *Bhagat*, we conclude that nothing more was needed. The district court did not err in declining to give Sullivan's proposed instruction.[3] Finding no error, we decline to reach the question of harmlessness.

B. The "Duty to Disclose" Instruction

Sullivan also claims that the district court erred by rejecting his proposed "duty to disclose" instruction: that, if the basis of the obstruction-of-justice conviction was Sullivan's "withholding of information, the government must prove beyond a reasonable doubt that [he] had a duty to disclose that information to the FTC." Sullivan contends that, because this proposed instruction was not given, the jury may have convicted on a theory that was invalid under Section 1505—that is, inaction by a defendant under no duty to disclose. He urges application of the *Yates* rule that "a verdict [is required] to be set aside in cases where the verdict is supportable on one ground, but not on another, and it is impossible to tell which ground the jury selected." *Yates v.*

[3] Embedded in Sullivan's arguments regarding the jury instructions is a challenge to the sufficiency of the evidence as to obstruction, based on a lack of nexus. Viewing the evidence in the light most favorable to the prosecution, we conclude that a "rational trier of fact" could have found that there was a nexus between Sullivan's choices and the FTC proceeding, *Coleman v. Johnson*, 566 U.S. 650, 654 (2012), whether "nexus" is defined as "natural and probable effect" or as a "relationship in time, causation, or logic." *Aguilar*, 515 U.S. at 599.

United States, 354 U.S. 298, 312 (1957), *overruled on other grounds by Burks v. United States*, 437 U.S. 1 (1978).

We need not resolve this issue. Even assuming that the instruction should have been given and that the error implicates the *Yates* rule, it is well settled that "errors of the *Yates* variety are subject to harmless-error analysis." *Skilling v. United States*, 561 U.S. 358, 414 (2010). A *Yates* error is harmless "if, after a 'thorough examination of the record,' we are able to 'conclude beyond a reasonable doubt that the jury verdict would have been the same absent the error.'" *United States v. Galecki*, 89 F.4th 713, 741 (9th Cir. 2023) (quoting *Neder v. United States*, 527 U.S. 1, 19 (1999)). After carefully examining the trial record, we conclude that any such error was harmless beyond a reasonable doubt.

The premise of Sullivan's *Yates* argument is that the jurors were permitted to convict him of violating Section 1505 based either (1) on the claimed invalid theory that he personally withheld information, even though he himself had no duty to disclose it to the FTC; or (2) on the theory that he caused Uber, which concededly *did* have a duty to disclose, to fail to provide this information to the FTC. There is no dispute that the latter theory, which rests on 18 U.S.C. § 2(b),[4] is legally valid under our court's decision in *United States v. Singh*, 979 F.3d 697, 717–18 (9th Cir. 2020) (concluding that the defendant need not have a

[4] Section 2(b) states: "[w]hoever willfully causes an act to be done which if directly performed by him or another would be an offense against the United States, is punishable as a principal." 18 U.S.C. § 2(b). "[U]nder [Section] 2(b), a defendant may be convicted, even if he did not commit all the elements of the offense . . . ." *United States v. Ubaldo*, 859 F.3d 690, 702 (9th Cir. 2017). In this context, Section 2(b) "is considered embodied in full in *every* federal indictment." *United States v. Michaels*, 796 F.2d 1112, 1118 (9th Cir. 1986).

duty to disclose, so long as the third party whom he causes not to make the disclosure does have such a duty). On this particular record, "there is no reasonable possibility that the jury here rested its conviction[]" on the Section 1505 charge based *only* on the claimed invalid theory and not *also* on the concededly valid causing-to-be-done theory. *Galecki*, 89 F.4th at 742. To convict Sullivan, even under the claimed invalid theory, the jury still would have had to find that he "intentionally endeavored . . . to influence, obstruct, or impede" the pending FTC investigation by "acting with an improper purpose, . . . including . . . withholding[] [or] concealing . . . a document or other information." Given the nature of the ways in which, factually, Sullivan might be found at trial to have withheld information, we discern no reasonable scenario in which the jury could have found that Sullivan personally withheld information *with the intent to endeavor to influence the FTC proceeding* concerning Uber without *also* finding that he thereby willfully caused Uber to violate *its* conceded duty to disclose.[5] We also have no reasonable doubt that this case falls within the rule that "[i]f the evidence that the jury necessarily credited in order to convict the defendant under the instructions given . . . is such that the jury must have convicted the defendant on the legally adequate ground in addition to or instead of the legally inadequate ground, the conviction may be affirmed." *Galecki*, 89 F.4th at 742 (citation modified). We further conclude that it is "absolutely certain" that the jury had to find culpability vis-à-vis willfully causing Uber to violate its

[5] Sullivan makes a sufficiency-of-the-evidence challenge as to his willful causation of nondisclosure, based solely on the fact that he disclosed the 2016 breach to Uber's then-CEO. This argument is neither comprehensive as to the scope of Sullivan's alleged nondisclosure nor supported by law. It therefore fails.

duty in order to find that Sullivan also personally withheld information. *Ficklin v. Hatcher*, 177 F.3d 1147, 1152 (9th Cir. 1999). Because we conclude that any error is harmless, we need not reach the question of validity under Section 1505.

II. Sufficiency of the Evidence—Misprision Conviction

We now turn to Sullivan's argument that the evidence of his alleged misprision was insufficient as a matter of law. We review de novo. *See Munoz*, 412 F.3d at 1048. We must determine "whether, after viewing the evidence in the light most favorable to the prosecution, *any* rational trier of fact could have found the essential elements of the crime beyond a reasonable doubt." *United States v. Laney*, 881 F.3d 1100, 1106 (9th Cir. 2018) (quoting *United States v. Atkinson*, 990 F.2d. 501, 502 (9th Cir. 1993) (en banc)).

Misprision is the crime of "having knowledge of the actual commission of a felony" and "conceal[ing]" or failing to "as soon as possible make known the same to some judge or other person in civil or military authority under the United States." 18 U.S.C. § 4. To establish misprision, the government is obliged to show that "the principal committed and completed the felony alleged." *United States v. Ciambrone*, 750 F.2d 1416, 1417 (9th Cir. 1984). Here, that meant proving that the hackers had "intentionally accesse[d]" Uber's computers "without authorization . . . and thereby obtain[ed]" information from those "protected computer[s]," in violation of the CFAA. 18 U.S.C. § 1030(a)(2).

The hackers' use of stolen credentials to access protected, private servers was a typical CFAA violation. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 31 F.4th 1180, 1201 (9th

Cir. 2022) (holding that violation occurs "when a person circumvents a computer's generally applicable rules regarding access permissions, such as username and password requirements, to gain access to a computer"). Nobody here argues that their access, and subsequent downloading of data, was authorized beforehand.[6]

Sullivan argues that Uber's *post hoc* authorization, via the NDA, retroactively rendered the hackers' access authorized—thereby erasing their felony. But this is a false premise, inconsistent with the most plain and natural reading of the CFAA. In the statute, "without authorization" modifies the present-tense verb "accesses." 18 U.S.C. § 1030(a)(2). An actor's authorization, or lack thereof, is assessed at the moment of access.[7] Our prior decisions support this reading. *United States v. Nosal*, 844 F.3d 1024, 1038 (9th Cir. 2016) (upholding a jury instruction that "[a] person uses a computer 'without authorization' when the person *has not received permission*" and noting that the jury

[6] We need not decide whether a bug bounty program may endow qualified researchers with *prior* authorization to access protected computers.

[7] Sullivan's alternative interpretation would allow companies to "modify the terms of authorization after initial access" and require courts to assess "authorization" at some undetermined point after such modification. The effects of that interpretation could endanger the existence of bug bounty programs: If a company could apply modified terms retroactively, then a good-faith researcher who had accessed a computer yesterday *while authorized* could have that access retroactively deauthorized today. Yesterday's access might then constitute a violation of the CFAA. Uncertainty regarding criminal liability could deter participation in bug bounty programs. And allowing *post hoc* authorization could encourage extortionary schemes: hackers could download sensitive data, demand a data ransom, and then insist that the company alter its bug bounty program terms to retroactively immunize their conduct.

was to determine "whether such permission *was given*") (emphases added), *overruled in part on other grounds by Lagos v. United States*, 584 U.S. 577 (2018); *LVRC Holdings LLC v. Brekka*, 581 F.3d 1127, 1135 (9th Cir. 2009) ("[A] person uses a computer 'without authorization' under [the CFAA] . . . when the employer *has rescinded permission* to access the computer and the defendant uses the computer anyway.") (emphasis added). Because the hackers had not been given authorization by the time of access, their access was unauthorized. Their illegal conduct could not be laundered through an NDA.

The government also needed to show that Sullivan had "full knowledge" "that the principal[] had committed and completed the felony alleged." *Lancey v. United States*, 356 F.2d 407, 409 (9th Cir. 1966). Sullivan claims that, even if the hackers were unauthorized within the meaning of the CFAA, he reasonably believed that the NDA recharacterizing the hackers' conduct as part of Uber's Bug Bounty Program retroactively authorized the breach—thereby cleansing the felonious access of its illegality. Given this belief, he argues, he could not have had "full knowledge" as required for conviction of misprision.

The evidence does not support this argument. By November 15, 2016, Sullivan knew that an unauthorized actor had "compromised" Uber's accounts and potentially "acquired" data. According to his own arguments, he "believed that the hackers' conduct was unauthorized *at the time it occurred*," and he "view[ed] the legality of [the hackers'] conduct as turning on a Bug Bounty agreement." That is, *before* the NDA was signed, he knew and believed that their conduct was illegal. If the NDA were really meant to cleanse the felony, it would have described the incident accurately, rather than omitting the fact that the hackers

downloaded Uber's data. And the evidence suggests that Sullivan's beliefs did not change even after the signing: A year after the incident, Sullivan referred to the hackers as "unauthorized" in an email to Uber's new CEO. Uber's lawyers, too, continued to characterize the hackers as "unauthorized."

Finally, the government had to show that Sullivan knew that the conduct in question was a felony punishable by more than a year in prison. "The defendant need not know the precise term of imprisonment authorized by law, but at least [he] must know the potential punishment exceeds one year in prison." *United States v. Olson*, 856 F.3d 1216, 1224 (9th Cir. 2017). Sullivan had been an Assistant U.S. Attorney in a "Computer Hacking and IP Unit." He had helped prosecute a CFAA violation; the plea agreement, which he signed, noted a maximum sentence of five years. Sullivan's unusual "sophistication" could also be inferred "from [his] experience" as a prosecutor and cybersecurity professional. *Id.*

As detailed above, a rational juror could have found each essential element of misprision beyond a reasonable doubt.

III. Admission of Guilty Plea

Finally, we address Sullivan's contention that the district court abused its discretion in permitting the introduction of the guilty plea agreement signed by one of the hackers. We review for abuse of discretion a district court's evidentiary ruling under Federal Rule of Evidence 403, which is not to be overturned unless it is "manifestly erroneous." *United States v. Tsarnaev*, 595 U.S. 302, 322–23 (2022) (quoting *Gen. Elec. Co. v. Joiner*, 522 U.S. 136, 142 (1997)).

There is no manifest error here. In providing that a court "may exclude relevant evidence if its probative value is substantially outweighed by a danger of . . . unfair prejudice," Rule 403 gives the district court considerable leeway. Fed. R. Evid. 403. The probative value of the plea agreement is unquestionable. The agreement served as evidence of the specific crimes to which one of the hackers had pled guilty, including a felonious violation of the CFAA. The agreement thus proves an element of the crime with which Sullivan was charged. Even if we assess the plea agreement's probative value only "relative to the other evidence in the case," such as the hacker's testimony, that value is still significant. *Old Chief v. United States*, 519 U.S. 172, 185 (1997).

Any unfair prejudice to the defendant resulting from the plea's admission into evidence does not substantially outweigh the plea's probative value. Because the hacker and Sullivan pleaded guilty to separate crimes, the fact of this plea does not improperly impute blame for the hacker's conduct to Sullivan. *Cf. Baker v. United States*, 393 F.2d 604, 614 (9th Cir. 1968) (stating the general rule that "guilty pleas of co-defendants cannot be considered as evidence against those on trial," so that the defendant's guilt is "determined upon the evidence against him, not on whether a Government witness or co-defendant has pleaded guilty to the same charge"), *cert. denied* 393 U.S. 836 (1968). Contrary to Sullivan's arguments, the plea also does not attribute to him any particular belief. Nor are the facts within the plea likely to cause unfair prejudice, as they were subject to a limiting instruction by the district court that they were not to be taken for the truth of the matter asserted. The district court gave "adequate cautionary instruction" to

mitigate prejudice. *United States v. Halbert*, 640 F.2d 1000, 1006 (9th Cir. 1981).

We conclude that the court did not abuse its discretion in admitting the plea and therefore decline to reach the question of harmlessness.

Conclusion

The jury's verdict in this case underscores the importance of transparency even in failure situations—especially when such failures are the subject of federal investigation. The verdict is not tainted by any of the claimed instructional or evidentiary errors, nor can it be overturned for insufficiency of the evidence. We affirm the district court in all relevant respects.

AFFIRMED.