No. 19-___

IN THE

Supreme Court of the United States

NATHAN VAN BUREN,

Petitioner,

v.

UNITED STATES OF AMERICA,

Respondent.

On Petition for a Writ of Certiorari
to the United States Court of Appeals
for the Eleventh Circuit

PETITION FOR A WRIT OF CERTIORARI

Saraliene Smith Durrett
SARALIENE SMITH DURRETT, LLC
1800 Peachtree Street
Suite 300
Atlanta, GA 30309

Rebecca Shepard
FEDERAL DEFENDER PROGRAM, INC.
101 Marietta Street NW
Suite 1500, Centennial Tower
Atlanta, GA 30303

Jeffrey L. Fisher
Counsel of Record
Pamela S. Karlan
Brian H. Fletcher
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@stanford.edu

QUESTION PRESENTED

Whether a person who is authorized to access information on a computer for certain purposes violates Section 1030(a)(2) of the Computer Fraud and Abuse Act if he accesses the same information for an improper purpose.

RELATED PROCEEDINGS

United States v. Van Buren, No. 1:16-cr-00243-ODE-JFK-1 (N.D. Ga. May 3, 2018)

United States v. Van Buren, No. 18-12024 (11th Cir. Oct. 10, 2019)

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Legislative Materials

Other Authorities

PETITION FOR A WRIT OF CERTIORARI

Petitioner Nathan Van Buren respectfully petitions for a writ of certiorari to review the judgment of the United States Court of Appeals for the Eleventh Circuit.

OPINIONS BELOW

The opinion of the United States Court of Appeals for the Eleventh Circuit (Pet. App. 1a) is published at 940 F.3d 1192. The relevant order of the district court is unpublished.

JURISDICTION

The decision of the court of appeals was issued on October 10, 2019. Pet. App. 1a. This Court has jurisdiction pursuant to 28 U.S.C. § 1254(1).

RELEVANT STATUTORY PROVISIONS

The Computer Fraud and Abuse Act, 18 U.S.C. § 1030, is reproduced in the appendix to this brief at Pet. App. 33a-46a.

STATEMENT OF THE CASE

The Computer Fraud and Abuse Act (CFAA) makes it a federal crime to "access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). Under the Act, to "exceed[] authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id.* § 1030(e)(6).

This case presents a recurring question about the interpretation of these provisions, on which the

courts of appeals are openly divided: Does a person obtain information on a computer that he is "not entitled so to obtain" when he has permission to access the information, but does so for an improper purpose? The answer to this question has sweeping implications. Every day, "millions of ordinary citizens" across the country use computers for work and for personal matters. *United States v. Nosal*, 676 F.3d 854, 862-63 (9th Cir. 2012) (en banc). Accessing information on those computers is virtually always subject to conditions imposed by employers' policies, websites' terms of service, and other third-party restrictions. If, as some circuits hold, the CFAA effectively incorporates all of these limitations, then any trivial breach of such a condition—from checking sports scores at work to inflating one's height on a dating website—is a federal crime.

1. In 1984, Congress became concerned about "the activities of so-called 'hackers' who have been able to access (trespass into) both private and public computer systems." H.R. Rep. No. 98-894, at 10 (1984). To deter and punish this "new dimension of criminal activity," *id.*, Congress created a federal crime, codified at 18 U.S.C. § 1030. Two years later, Congress amended the statute, and it became known as the CFAA. Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213. In the ensuing years, Congress amended the CFAA several more times, expanding both the types of information and the types of computers it covers.

The provision of the CFAA at issue here provides that "[w]hoever intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information" from a "protected computer" commits a federal crime. 18 U.S.C.

§ 1030(a)(2). A "protected computer" is one "used in or affecting interstate or foreign commerce or communication"—in other words, any "computer[] with Internet access." *Nosal*, 676 F.3d at 859. As noted above, the phrase "exceeds authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser *is not entitled so to obtain* or alter." 18 U.S.C. § 1030(e)(6) (emphasis added).

Violations of Section 1030(a)(2) are punishable by a fine or imprisonment of one year, or both. 18 U.S.C. § 1030(c)(2)(A). That misdemeanor becomes a felony, punishable by imprisonment for up to five years, if "the offense was committed for purposes of commercial advantage or private financial gain." *Id.* § 1030(c)(2)(B)(i). The statute also contains a civil cause of action, allowing any person who suffers damage or loss because of a violation of the CFAA to sue for damages or equitable relief. *Id.* § 1030(g).

2. Petitioner was a police sergeant in Cumming, Georgia, a small town in the northern part of the state. Pet. App. 3a. As a result of patrolling the town over the years, petitioner knew a local man named Andrew Albo. *Id.* 3a. Albo "allegedly paid prostitutes to spend time with him" and then called the police to "accuse[] the women of stealing the money he gave them." *Id.* 4a. Claiming to fear retaliation from these women, he sometimes also asked officers to run searches of allegedly suspicious license plate tags. Tr. 409 (Oct. 25, 2017).

In the summer of 2015, petitioner was struggling with financial difficulties and asked Albo for a loan. Pet. App. 4a-5a. "Unbeknownst to [petitioner],

however, Albo recorded their conversations." *Id.* 3a-4a. Albo shared the recordings with the Forsyth County Sheriff's Office, which referred the matter to the Cumming Police Department, which in turn referred the matter to the FBI. U.S. C.A. Br. 4-5.

The FBI devised a sting operation "to test how far [petitioner] was willing to go for money." Pet. App. 4a. To set up the operation, the FBI invented a favor for Albo to request of petitioner in exchange for the loan. *Id.* 4a-5a. In particular, the FBI instructed Albo to ask petitioner to run a computer search for the supposed license plate number of a dancer at a local strip club. *Id.* It directed Albo to say that he liked her and wanted "to know if she was an undercover officer before he would pursue her further." *Id.* 5a.

Petitioner agreed to complete the search. When Albo gave him $5000 in return, petitioner "offered to pay Albo back, but Albo waved that off." Pet. App. 5a. Still, petitioner insisted, "I'm not charging for helping you out." *Id.* 25a. Several days later, Albo "followed up" with petitioner on the request, bringing him an additional $1000 and the "fake license plate number created by the FBI." *Id.* 5a.

After that meeting, petitioner accessed the Georgia Crime Information Center (GCIC) database, which contains license plate and vehicle registration information. Pet. App. 6a. As a law enforcement officer, petitioner was authorized to access this database "for law-enforcement purposes." *Id.* 28a. He ran a search for the license plate number that Albo had given him. He then texted Albo that he had information to provide. *Id.* 6a.

The next day, the FBI "arrived at [petitioner's] doorstep" and revealed that it had been tracking his interactions with Albo and believed petitioner had engaged in criminal activity. Pet. App. 6a.

3. The Government charged petitioner in the U.S. District Court for the Northern District of Georgia with "one count of felony computer fraud, in violation of 18 U.S.C. § 1030" and "one count of honest-services wire fraud, in violation of 18 U.S.C. §§ 1343 and 1346." Pet. App. 6a.

After the Government presented its case at trial, petitioner moved for a judgment of acquittal on the CFAA count. Petitioner argued that "accessing [information] for an improper or impermissible purpose does not exceed authorized access as meant by" Section 1030(a)(2). Tr. 391 (Oct. 25, 2017). The Government conceded in response that the circuits were "split" over that issue. *Id.* at 396-97. But it claimed that the Eleventh Circuit's decision in *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), required the district court to reject petitioner's argument. As the Government explained, *Rodriguez* held that a defendant violates the CFAA not only when he obtains information that he has no "rightful[]" authorization whatsoever to acquire, but also when he obtains information "for a nonbusiness purpose." Tr. 396-97 (Oct. 25, 2017).

The district court denied petitioner's motion. Tr. 399 (Oct. 25, 2017). The jury then convicted on both counts. Pet. App. 6a. The district court sentenced petitioner on each count to eighteen months in prison, to be served concurrently. U.S. C.A. Br. 3.

4. The Eleventh Circuit affirmed petitioner's CFAA conviction, rejecting petitioner's argument that he was "innocent of computer fraud because he accessed only databases that he was authorized" to access. Pet. App. 26a-28a.[1] Like the Government in the district court, the Eleventh Circuit acknowledged that "other courts have rejected *Rodriguez*'s interpretation of 'exceeds authorized access.' " *Id.* at 27a. But the court of appeals declared itself bound by *Rodriguez*, barring "abrogation by the Supreme Court" or new precedent otherwise rendering the case defunct. *Id.* at 28a. Under *Rodriguez*, the Eleventh Circuit observed, it is enough that petitioner ran the tag search for "inappropriate reasons." *Id.* at 27a.

REASONS FOR GRANTING THE WRIT

The courts of appeals are openly divided four-to-three over whether a person with permission to access information on a computer violates the Computer Fraud and Abuse Act when he accesses that information for an improper purpose. This Court should use this case to resolve the conflict. This case squarely presents the issue, and the Eleventh Circuit's expansive construction of the CFAA is incorrect. The most natural reading of the CFAA is that a person "obtain[s] information in the computer that [he] is not entitled so to obtain," 18 U.S.C. § 1030(e)(6), only if he had no right at all to access the information. Reading the statute more broadly would criminalize ordinary computer use throughout

---

[1] For reasons not relevant here, the court of appeals also vacated petitioner's conviction for honest-services wire fraud. Pet. App. 8a-22a, 32a.

the country, thereby inviting arbitrary enforcement and flouting the principle that a federal criminal statute should not be construed to encompass a broad swath of everyday behavior unless the statute's text unambiguously demands that result.

I. The courts of appeals are intractably divided over the reach of the CFAA.

1. In this case, the Eleventh Circuit reaffirmed its view that a person violates Section 1030(a)(2) of the CFAA if he uses a computer to access information that he is otherwise authorized to access but does so for an improper purpose. The Eleventh Circuit first adopted that position in *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), holding that a person with access to a computer for business reasons "exceed[s] his authorized access" whenever he "obtain[s] . . . information for a nonbusiness reason." Pet. App. 27a. The Eleventh Circuit asserted that "the plain language of the Act" requires this result. *Rodriguez*, 628 F.3d at 1263.

The Eleventh Circuit's interpretation of the CFAA accords with decisions by the First, Fifth, and Seventh Circuits. In *EF Cultural Travel BV v. Explorica, Inc.*, 274 F.3d 577 (1st Cir. 2001), the First Circuit concluded that a person "exceeds authorized access" when he uses information for purposes prohibited by a confidentiality agreement. The defendant there had "authorization . . . to navigate around EF's [public] [web]site." *Id.* at 583. But, in the First Circuit's view, he "exceeded that authorization" by his "wholesale use" of "proprietary information and know-how" to collect data from the website to aid a competitor's strategy. *Id.* at 582-83.

Agreeing with the First Circuit, the Fifth Circuit has concluded that the CFAA's prohibition against "exceed[ing] authorized access" includes "exceeding the *purposes* for which access is 'authorized.' " *United States v. John*, 597 F.3d 263, 272 (5th Cir. 2010), *cert. denied*, 568 U.S. 1163 (2013) (emphasis added). In other words, when a person is authorized to access information on a computer "for limited purposes," the Fifth Circuit holds that the person violates the CFAA by accessing the information for an unauthorized purpose. *Id.*; *see also Merritt Hawkins & Assocs., LLC v. Gresham*, 79 F. Supp. 3d 625 (N.D. Tex. 2015) (applying *John* to a civil defendant's breach of a confidentiality agreement with his employer).

The Seventh Circuit has also held that the CFAA is violated when a person accesses data on his work computer for a purpose that his employer prohibits. *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F.3d 418, 420-21 (7th Cir. 2006). As in the Eleventh, First, and Fifth Circuits, it is no defense in the Seventh Circuit that the person was entitled to obtain the information for certain purposes. *Id.* at 419-20.[2]

---

[2] The Seventh Circuit suggested that once an employee violates a purpose restriction, he breaches a duty of loyalty to his employer, which actually "terminate[s] his . . . authority to access" the computer at all. *Citrin*, 440 F.3d at 420-21. But this reasoning—whatever its merit—does not seem to apply to the initial violation of the purpose restriction that constitutes the breach. Accordingly, subsequent courts have treated the facts of *Citrin* itself as an "exceeds authorized access" case, rather than a "without authorization" case. *See, e.g.*, *United States v. Valle*, 807 F.3d 508, 524 (2d Cir. 2015); *United States v. Nosal*, 676 F.3d 854, 862 (9th Cir. 2012) (en banc).

2. In contrast to the preceding four circuits, the Second, Fourth, and Ninth Circuits have each held that the CFAA's "exceeds authorized access" prong does not impose criminal liability on a person with permission to access information on a computer who accesses that information for an improper purpose. A person violates the CFAA in those circuits only if he accesses information on a computer that he is prohibited from accessing at all, for any reason.

The Ninth and Fourth Circuits adopted this position in nearly simultaneous decisions seven years ago. Declaring that it was "unpersuaded by the decisions of [its] sister circuits," the Ninth Circuit "decline[d] to follow" them. *United States v. Nosal*, 676 F.3d 854, 862-63 (9th Cir. 2012) (en banc). The nine-judge majority reasoned that the text of Section 1030(a)(2) does not cover a person "who has unrestricted physical access to a computer, but is limited in the use to which he can put the information." *Id.* at 857, 862-63. The Ninth Circuit explained, moreover, that reading the CFAA to cover "use restrictions" and thereby to reach activities "routinely prohibited by many computer-use policies" would improperly turn "millions of ordinary citizens" into criminals. *Id.* at 860-63.

The Fourth Circuit likewise "reject[ed] an interpretation of the CFAA that imposes liability" when people have permission to access information on a computer but their "purpose in accessing the information [i]s contrary to company policies regulating use." *WEC Carolina Energy Sols. LLC v. Miller*, 687 F.3d 199, 202, 207 (4th Cir. 2012) (internal quotation marks and citation omitted).

More recently, the Second Circuit adopted the same view of the CFAA in *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015). The defendant in that case was a New York City police officer who used a computer program to access the federal National Crime Information Center database, which he was authorized to access for his official duties. *Id.* at 512-13. He retrieved information about various personal acquaintances, in violation of the department's policies regarding proper use of the database. *Id.*

The Second Circuit noted that "six other circuits have wrestled with the question" whether "exceeds authorized access" is limited "to a scenario where a user has permission to access the computer but proceeds to . . . enter[] an area of the computer to which his authorization does not extend." *Valle*, 807 F.3d at 524. Rejecting the broader approach of "the First, Fifth, Seventh, and Eleventh Circuits," the Second Circuit "agree[d] with the Ninth and Fourth Circuits" that the CFAA is indeed limited to situations where the user does not have access for *any* purpose at all. *Id.* at 524, 527.

The Second Circuit reasoned that the "ordinary tools of legislative construction" do not resolve the issue; the language of the statute is "readily susceptible to different interpretations." *Valle*, 807 F.3d at 524, 526. The court therefore turned to "the rule of lenity," which requires courts to resolve ambiguity in criminal statutes by "adopt[ing] the interpretation that favors the defendant." *Id.* at 526. Stressing that the broader interpretation of the CFAA "would criminalize the conduct of millions of ordinary computer users," the Second Circuit rejected it. *Id.* at 527.

Several district courts in circuits that have not yet addressed the issue have also recognized the conflict and followed the approach taken by the Second, Fourth, and Ninth Circuits. *Teva Pharms. USA, Inc. v. Sandhu*, 291 F. Supp. 3d 659, 669-70 (E.D. Pa. 2018) (citing eight other district court decisions within the Third Circuit that have done the same); *Hedgeye Risk Mgmt., LLC v. Heldman*, 271 F. Supp. 3d 181, 194 (D.D.C. 2017); *Cloudpath Networks, Inc. v. SecureW2 B.V.*, 157 F. Supp. 3d 961, 983 (D. Colo. 2016); *Sebrite Agency, Inc. v. Platt*, 884 F. Supp. 2d. 912, 917-18 (D. Minn. 2012).

3. This issue has sufficiently percolated in the courts of appeals, and the split will not abate without this Court's intervention.

Opposing review of the Fifth Circuit's decision in *John*, the Government conceded that "[t]he circuits have disagreed about whether a person 'exceeds authorized access' of a protected computer, in violation of 18 U.S.C. 1030, when she has access to a computer system for certain legitimate purposes but then accesses the system for a prohibited purpose." Br. in Opp. at 7, *John v. United States*, 568 U.S. 1163 (2013) (No. 12-5201). But the Government maintained that "review of the reach of Section 1030 would be premature" because "the Fourth Circuit's decision in *WEC Carolina* and the Ninth Circuit's decision in *Nosal* [had been] issued within the last seven months." *Id.* at 13.

It has now been seven years, and there is an entrenched four-to-three split. The arguments on both sides of the conflict have now been fully vetted in various majority and dissenting opinions, and courts are just choosing sides. *See, e.g.*, *Teva*

Pharms., 291 F. Supp. 3d at 668-71 (laying out the conflict and siding with the Second, Fourth, and Ninth Circuits). Only this Court can establish a uniform meaning of the CFAA.

II. The question presented is extremely important.

For three reasons, it is critical that this Court resolve the conflict over the scope of the CFAA.

1. At its core, the question presented is whether the CFAA applies only to hacking and related activities or whether it extends to "whole categories of otherwise innocuous behavior." *United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) (en banc). Most people are not hackers. But most everyone who uses a computer (which is to say, most everyone) regularly runs up against conditions on accessing information on the computer—such as "corporate polic[ies] that computers can be used only for business purposes." *Id.*

For example, many law schools provide students with access to the Westlaw legal database for educational use only. But a student might use that access for personal purposes—perhaps to look up local housing laws to negotiate rent or to demand a refund of a security deposit. Whether this conduct constitutes a felony hinges on the answer to the question presented. *See* 18 U.S.C. § 1030(c)(2)(B)(i) (violations of the CFAA committed for "private financial gain" are punishable by five years in prison); *Nosal*, 676 F.3d at 860-62.

To take another example, every March, tens of millions of American workers participate in office

pools for the NCAA men's basketball tournament ("March Madness").[3] Such pools typically involve money stakes. When these employees use their company computers to generate their brackets or to check their standing in the pools, they likely violate their employers' computer policies. Again, the answer to the question presented determines whether these employees are guilty of a felony.

One could go on and on. The question whether such commonplace activities violate the CFAA should not be left unresolved. It is intolerable for a broad swath of conduct to be entirely innocent in parts of the country but to constitute a federal crime in others.[4]

2. The CFAA is also invoked frequently. The Government regularly brings criminal prosecutions under the CFAA. *See* Jonathan Mayer, *Cybercrime Litigation*, 164 U. Penn. L. Rev. 1453, 1474-76 (2016) (noting that "trial and appellate courts are increasingly addressing criminal issues under [the] CFAA"). And reported cases likely undercount the actual frequency of the statute's use. While many

---

[3] Adam Chandler, *One Worker's Fantasy: A March Madness National Holiday*, The Atlantic (Mar. 20, 2015), https://www.theatlantic.com/business/archive/2015/03/one-workers-fantasy-a-march-madness-national-holiday/388327/ (citing an estimate that 77.7 million workers will spend time on March Madness during work hours).

[4] Indeed, the question presented is critical not only for every computer user, but also for every user of a smartphone and many other internet-connected devices that "affect" interstate commerce and thus fall under the Act's broad definition of "computer." *See* 18 U.S.C. § 1030(e)(1).

criminal prosecutions under the CFAA result in convictions and appeals, even more end in pleas without any further proceedings. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1617 n.86 (2003).

On the civil side, businesses also often bring claims under the statute against employees and competitors. In fact, "[c]ivil cybercrime litigation has unambiguously exploded." Mayer, *supra* at 1472-73. Thus, the answer to the question presented will not only determine the scope of a federal criminal statute but will also bring important clarity for "commercial quarrels" that arise under the Act. *Id.* at 1481.

3. Uniformity in the law is particularly vital under the CFAA because of how the federal venue provision intersects with the statute.

Under federal law, a crime that is "begun in one district and completed in another, or committed in more than one district, may be inquired of and prosecuted in any district in which such offense was begun, continued, or completed." 18 U.S.C. § 3237. In a CFAA case, therefore, venue is typically appropriate not only where the defendant resides but also wherever any computer server he accessed is located. And information that a person accesses on the internet can be stored on one or more servers located in different jurisdictions. Thus, venue in a single CFAA case can routinely be found in several districts around the country, often in different circuits. *See, e.g.*, *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (defendant lived in Missouri but was charged in California—where the website Myspace happened to have its server). This

phenomenon gives rise to a serious danger of forum shopping where, as here, some jurisdictions criminalize conduct that others do not.

The multiplicity of venue options not only raises the risk of forum shopping; it also raises fair notice concerns. Most computer users do not know, and cannot easily ascertain, the location of the servers they are using. Indeed, companies "frequently" transfer data among remote servers without warning or any "human intervention" at all. Br. for the United States at 43, *United States v. Microsoft*, 138 S. Ct. 1186 (2018) (No. 17-2). Therefore, at any given moment, a person using a computer in, say, New York, Virginia, or California has little way of knowing whether he may be committing a crime because he happens to be using a server located in Massachusetts, Texas, Illinois, or Georgia. As the Government itself recently argued in an analogous context, the application of federal law should not "depend on the happenstance of where the data is located at the precise moment when" someone accesses a provider's network. *Id.*

III. This case is the right vehicle for resolving the conflict.

This case is an excellent vehicle for resolving whether the CFAA covers using a computer for an unauthorized purpose. There is no question that, as a Georgia law enforcement official, petitioner had authorization to access the GCIC database. Pet. App. 28a. And petitioner accessed the database in exactly the same way he would have accessed it for a law enforcement purpose; there are no complicating factors like downloads, erasure, or corruption of data. *See* Pet. App. 6a, 28a.

The Eleventh Circuit was able to affirm petitioner's conviction only by applying its broad interpretation of "exceeds authorized access" under the CFAA. Pet. App. 26a-28a. If the Second, Fourth, and Ninth Circuits are correct that the CFAA does not reach violations of conditions placed on access, then petitioner's conviction must be reversed for insufficient evidence.

IV. The Eleventh Circuit's decision is incorrect.

The entrenched conflict over how to construe the CFAA provides ample reason to grant certiorari regardless of which circuits have the better reading of the statute. But the fact that the Eleventh Circuit's interpretation is wrong makes review all the more warranted here.

1. The Eleventh Circuit has pronounced that the CFAA's "plain language" reaches accessing information on a computer for an unauthorized purpose. *United States v. Rodriguez*, 628 F.3d 1258, 1263 (11th Cir. 2010). But the Eleventh Circuit's textual reading is not the only "plausible" one, *United States v. Valle*, 807 F.3d 508, 523-24 (2d Cir. 2015)—or even the better one. The most natural reading of the CFAA does not cover conditions placed on otherwise authorized access to information on a computer.

The CFAA defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. § 1030(e)(6). The ordinary meaning of the word to "obtain" is "to acquire, in any way." And "entitle" means "to give a right." *Webster's New International Dictionary* (2d ed. 1934). In

common usage, then, whether a person is entitled to obtain information turns on whether he has the right to acquire the information *at all*, not on the purpose for his access.

As an illustration of this typical usage, individuals seeking loans often give banks access to their credit history to verify their eligibility for the loans. If a bank were to access that credit information for an improper purpose—such as marketing credit cards—an ordinary speaker would not say that the bank was not entitled *to obtain* the information. Rather, the speaker would say that the bank was entitled to obtain the information but misused it.

Translated to the CFAA, a person, such as petitioner, who has permission to access information on a database is "entitled" to "obtain" that information. That fact does not change if he accesses that information for an improper purpose. While such misuse might trigger some other form of liability, it does not violate the CFAA, which is concerned only with the entitlement to *obtain* information. A person violates the CFAA only if he has no right whatsoever to access that information—because, for instance, it resides in a separate password-protected file.

Indeed, where Congress wants to forbid access merely for an unauthorized purpose, it does so expressly. For instance, a separate computer-crime statute criminalizes "knowingly access[ing] a Government computer, *with an unauthorized purpose*, and by doing so obtain[ing] classified information." 10 U.S.C. § 923(a)(1) (emphasis added). Another federal statute requires safeguards to ensure that certain Social Security Administration information "is not used for unauthorized purposes."

38 U.S.C. § 5318(b). Yet another statute establishes procedures to ensure that homeland security information "is not used for an unauthorized purpose." 6 U.S.C. § 482(b)(3)(A).

If Congress had wanted the CFAA to criminalize accessing information on computers for unauthorized purposes, it would have simply said "without authorization or *for an unauthorized purpose*." That Congress did not do so is telling.

2. The CFAA's structure confirms the ordinary meaning of its text. Section 1030(a)(2) criminalizes accessing a computer "without authorization" or "exceed[ing] authorized access"—different but related terms. Accessing a computer "without authorization" refers to a scenario where a user lacks permission to access *any* information on the computer. The meaning of "exceeds authorized access" is complementary, referring to a distinct scenario in which a user has permission to access *some* information on the computer, but then accesses *other* information to which her authorization does not extend. *Nosal*, 676 F.3d at 858.

3. The Eleventh Circuit's broad reading of the CFAA also goes far beyond the statute's objective, which is to forbid computer hacking.

The CFAA is not an all-purpose statute covering any misdeed that occurs on a computer. Congress enacted the CFAA to address the problem of computer "hackers." H.R. Rep. No. 98-894, at 10. Congress thus consistently described "authorization" in terms of "computer files or data" that an individual has permission to "enter" and sought to forbid "trespass[ing]" into such computerized records. *See id.*; S. Rep. No. 99-432, at 6 (1986).

Interpreting the statute's prohibition against "exceeding authorized access" as limited to scenarios where the user is categorically forbidden from accessing particular information on the computer "maintains the CFAA's focus on hacking rather than turning it into a sweeping Internet-policing mandate." *Nosal*, 676 F.3d at 858. The statute's "without authorization" prong applies to "outside hackers" (those who break into a computer they are not allowed to access at all) and its "exceeds authorized access" prong applies to "inside hackers" (those who have authorization to use a computer but obtain information they are not allowed to access). *Id.*

There is no reason to stretch the CFAA any further. Insofar as accessing information for an inappropriate purpose merits the imposition of criminal sanctions, other federal statutes prohibit such conduct. For example, 18 U.S.C. § 1832 criminalizes the theft of trade secrets. Many other criminal statutes similarly prohibit accessing or using information for improper purposes. *See, e.g.*, 17 U.S.C. § 506(a)(1) (prohibiting distribution of a copyrighted work); 42 U.S.C. § 1320d-6(a)(3) (prohibiting disclosure of individually identifiable health information). Misappropriating information on a computer can also subject people to state criminal laws and common-law contract and tort claims.

4. The dramatic consequences of the Eleventh Circuit's reading of the CFAA provide still further reason to reject that construction.

This Court has consistently refused to construe imprecisely worded federal statutes so expansively as to criminalize (and federalize) vast swaths of conduct. *See, e.g.*, *Yates v. United States*, 135 S. Ct. 1074,

1083 (2015); *Bond v. United States*, 134 S. Ct. 2077, 2091-92 (2014). It has been especially leery of doing so where, as here, such constructions would criminalize everyday conduct of ordinary people. In *United States v. Kozminski*, 487 U.S. 931 (1988), for instance, the Court held that the term "involuntary servitude" excludes "psychological coercion." *Id.* at 944. Otherwise, the Court reasoned, even the "parent who coerced an adult son or daughter into working in the family business by threatening withdrawal of affection" would commit a criminal act, as would the "political leader who uses charisma to induce others to work without pay." *Id.* at 949. Absent an explicit directive, a federal criminal statute does not reach such "a broad range of day-to-day activity," "subject[ing] individuals to the risk of arbitrary or discriminatory prosecution." *Id.* at 949, 952.

The Eleventh Circuit's interpretation of the CFAA would similarly reach commonplace activities of nearly all computer users, going far beyond the objectives of the statute. It would attach criminal liability to the multitude of private computer-use policies—policies "that most people are only dimly aware of and virtually no one reads or understands," *Nosal*, 676 F.3d at 861—and grant the Executive Branch virtually unfettered prosecutorial discretion.

The Government has responded that "whatever the scope of the CFAA, it won't prosecute minor violations." *Nosal*, 676 F.3d at 862; *see also United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015). That assurance appears questionable: Over the past decade, the Government has, in fact, brought cases against individuals who have violated companies' terms of service agreements. *See, e.g.*, Indictment, *United States v. Swartz*, No. 1:11-cr-10260 (D. Mass.

July 14, 2011), ECF No. 2 (violation of JSTOR terms of service); *United States v. Lowson*, No. 10-114, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (violation of Ticketmaster terms of service); *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009) (violation of Myspace terms of service). "The Justice Department has repeatedly taken the position that such violations are felonies." Tim Wu, *Fixing the Worst Law in Technology*, The New Yorker (Mar. 18, 2013). But even if the Government did, in fact, promise to forego pursuit of such minor CFAA violations, a free society should not be required to entrust its liberty to the grace of prosecutors. *See United States v. Stevens*, 559 U.S. 460, 480 (2010).

If there is any lingering doubt, the rule of lenity mandates that "when choice has to be made between two readings of what conduct Congress has made a crime, it is appropriate, before [choosing] the harsher alternative, to require that Congress should have spoken in language that is clear and definite." *United States v. Bass*, 404 U.S. 336, 347 (1971) (internal quotation marks and citation omitted). Here, the "ordinary tools of legislative construction fail to establish that the Government's position is unambiguously correct." *Valle*, 807 F.3d at 526. Moreover, any attempt to wrest an intermediate rule out of the CFAA that would cabin prosecutorial discretion—covering some instances of access for improper purposes but not others—would render the statute hopelessly vague. Crimes must be defined "with sufficient definiteness that ordinary people can understand what conduct is prohibited." *Kolender v. Lawson*, 461 U.S. 352, 357 (1983). And there is no textual footing in the CFAA to intelligibly criminalize only certain violations of terms of service, terms of

use, employer use policies, or other contract-based conditions of access. *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1575-83 (2010).

Accordingly, if nothing else, time-honored principles of leniency and constitutional avoidance require adopting petitioner's more limited reading of the CFAA's "exceeds authorized access" prong.

CONCLUSION

For the foregoing reasons, the petition for a writ of certiorari should be granted.

Respectfully submitted,

Saraliene Smith Durrett
SARALIENE SMITH DURRETT, LLC
1800 Peachtree Street
Suite 300
Atlanta, GA 30309

Rebecca Shepard
FEDERAL DEFENDER PROGRAM, INC.
101 Marietta Street NW
Suite 1500, Centennial Tower
Atlanta, GA 30303

Jeffrey L. Fisher
Counsel of Record
Pamela S. Karlan
Brian H. Fletcher
STANFORD LAW SCHOOL SUPREME COURT LITIGATION CLINIC
559 Nathan Abbott Way
Stanford, CA 94305
(650) 724-7081
jlfisher@stanford.edu

December 18, 2019

APPENDIX

APPENDIX A

[PUBLISH]

UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH

No. 18-12024

D.C. Docket No. 1:16-cr-00243-ODE-JFK-1

UNITED STATES OF AMERICA,

Plaintiff-Appellee,

versus

NATHAN VAN BUREN,

Defendant-Appellant.

Appeal from the United States District Court
for the Northern District of Georgia

(October 10, 2019)

Before MARTIN, ROSENBAUM, and BOGGS,* Circuit Judges. ROSENBAUM, Circuit Judge:

---

* Honorable Danny J. Boggs, United States Circuit Judge for the Sixth Circuit, sitting by designation.

Perhaps Dudley Field Malone said it best when he opined, "One good analogy is worth three hours' discussion."1 Or in this case, 15 pages of discussion. *See infra* at pp. 9–23.

Take, for example, this case.

"[A] lawsuit before a court" is a pretty big deal to most people. But a generic "question" or "matter," in common usage, maybe not so much.

That impression may change, though, if we clarify what we mean by "question" or "matter" in a specific context by analogizing to something else. So if we say that, for our purposes, to qualify as a "question" or a "matter," the question or matter must be of the same significance or scope as "a lawsuit before a court," a person would understand that we are not talking about just any old question or matter; we are referring to

---

1 Richard Nordquist, *The Value of Analogies in Writing and Speech*, ThoughtCo., https:// www.thoughtco.com/ what – is - an-analogy-1691878 (last visited Oct. 8, 2019). Along with Clarence Darrow, Dudley Field Malone defended John Scopes in the 1925 "Scopes Trial," formally known as *State v. Scopes*. *Scopes Trial*, Encyclopaedia Britannica, https:// www.britannica.com/event/ Scopes-Trial (last visited Oct. 8, 2019) ("*Scopes Trial*"); *Malone's Trial Speech (Full Text)*, Historical Thinking Matters, http:// historicalthinkingmatters.org/ scopestrial/1/sources/44/fulltext / (last visited Oct. 8, 2019) ("*Malone's Trial Speech*"). In that case, Tennessee, led by William Jennings Bryan, prosecuted Scopes for allegedly teaching evolution at a Tennessee high school. *Scopes Trial*. Scopes was convicted and fined $100. *Scopes v. State*, 289 S.W. 363, 367 (Tenn. 1927). The Tennessee Supreme Court then vacated the judgment since Tennessee law required a jury—not a judge—to assess any fine of more than $50.00, but in Scopes's case, the trial judge had done so. *Id.* The Tennessee law Scopes was accused of violating was ultimately repealed in 1967. *Scopes Trial*.

only questions or matters on the same scale as "a lawsuit before a court." To use a metaphor, the analogy here is a bridge to understanding.

In this case, though, that bridge was never built. The government charged Nathan Van Buren with honest-services fraud (through bribery) for undertaking an "official act" in his capacity as a police officer, in exchange for money. At the close of the evidence, the district court instructed the jury that an "official act" is a decision or action on a "question" or "matter." But it did not inform the jury that the "question" or "matter" in this context must be comparable in scope to a lawsuit, hearing, or administrative determination. The jury convicted Van Buren.

Since the jury was not instructed with the crucial analogy limiting the definition of "question" or "matter," and because the government itself did not otherwise provide the missing bridge, we cannot be sure beyond a reasonable doubt that the jury convicted Van Buren of the offense that Congress criminalized when it enacted the honest-services-fraud and bribery statutes. For this reason, we must vacate Van Buren's honest-services-fraud conviction and remand for a new trial on that count. Van Buren was also charged with and convicted of computer fraud, and we affirm that conviction.

I.

Nathan Van Buren was a sergeant with the Cumming, Georgia, Police Department. In his capacity as a police officer, Van Buren came to know a man named Andrew Albo. Albo was a recent widower in his early sixties, who allegedly fancied younger women,

including minors and prostitutes. He allegedly paid prostitutes to spend time with him and then often accused the women of stealing the money he gave them. At least one woman also alleged Albo surreptitiously recorded and harassed her. The Deputy Chief of Police in the Cumming Police Department believed that Albo "had a mental health condition" and considered Albo to be "very volatile," so he warned his officers to "be careful" with Albo.

Van Buren did not heed the Deputy Chief's caveat. Instead, he fostered a relationship with Albo. Van Buren, who first met Albo when he helped arrest Albo for providing alcohol to a minor, often handled the disputes between Albo and various women. At the time, Van Buren was grappling with financial difficulties, and Van Buren saw in Albo a chance to improve his situation. So Van Buren decided to ask Albo for a loan. To justify his request, Van Buren falsely claimed he needed $15,368 to settle his son's medical bills. He explained to Albo that he could not obtain a loan from a bank because he had shoddy credit.

Unbeknownst to Van Buren, however, Albo recorded their conversations. Albo presented the recording of Van Buren's loan solicitation to a detective in the Forsyth County Sheriff's Office. He told the detective that Van Buren was "shak[ing] him down for his money." Albo's complaint drew the suspicion of the FBI, which created a sting operation to test how far Van Buren was willing to go for money. Under the plan, Albo was to give Van Buren some cash, and in exchange, Albo was to ask Van Buren to tell him whether Carson, a woman he supposedly met at a strip club, was an undercover police officer.

Over a series of meetings and communications monitored and recorded by the FBI, Albo put the plan into action. At lunch with Van Buren on August 21, 2015, Albo handed Van Buren an envelope with $5,000, telling him that this was "not the whole thing." Van Buren offered to pay Albo back, but Albo waved that off, saying money was "not the issue." Instead, Albo told Van Buren he had met a woman he liked at a strip club, but he needed to know if she was an undercover officer before he would pursue her further. Van Buren agreed to help.

On August 31, Albo followed up on a previous discussion the pair had had about searching the woman's license plate in the police database. During that conversation, Albo asked Van Buren whether he had had a chance to conduct the search yet. Van Buren replied, "As far as running the plates, I don't—I don't think I got the right plate numbers from you." Van Buren then told Albo to just text him the plate number, so Albo texted Van Buren "Pkp" and "1568," a fake license plate number created by the FBI. Van Buren responded that he would look into the matter, but he would need the "item" first. Albo replied that he had "2," and the pair scheduled to meet for lunch.

At lunch, Albo passed Van Buren an envelope containing $1,000 and apologized that he did not have $2,000, as they had discussed.2 Van Buren asked Albo for the woman's name, explaining that "the car may not [be] registered to her." After learning that her name was Carson, Van Buren promised to attend to

---

2 The FBI actually gave Albo $2,000 to pass to Van Buren, so it appears Albo may have attempted to retain $1,000 for himself.

the matter promptly, and Albo responded, "then I will have all the money for you."

A few days later, on September 2, 2015, Van Buren searched for license-plate number PKP1568 in the Georgia Crime Information Center ("GCIC") database, an official government database maintained by the Georgia Bureau of Investigation ("GBI") and connected to the National Crime Information Center ("NCIC") maintained by the FBI. Van Buren then texted Albo to tell him he had information for him.

The next day, the FBI and GBI arrived at Van Buren's doorstep and conducted an interview with Van Buren. During the interview, Van Buren admitted he had concocted a fake story about his son's need for surgery to justify asking Albo for $15,000. He also conceded he had received a total of $6,000 from Albo. In addition, Van Buren confessed he had run a tag search for Albo and he knew doing so was "wrong." And while Van Buren asserted that $5,000 of the money he received from Albo was a "gift," he did reply "I mean he gave me $1,000" when asked if he received anything in exchange for running the tag. Finally, Van Buren conceded he understood the purpose of running the tag was to discover and reveal to Albo whether Carson was an undercover officer.

A federal grand jury charged Van Buren with one count of honest-services wire fraud, in violation of 18 U.S.C. §§ 1343 and 1346, and one count of felony computer fraud, in violation of 18 U.S.C. § 1030. At trial, the government presented the FBI's recordings of the interactions between Van Buren and Albo, and the jury convicted Van Buren of both counts.

Van Buren now appeals his convictions. He argues the jury instructions the district court gave were incorrect, insufficient evidence exists to support his convictions, and the district court denied him his Sixth Amendment right to confront an adverse witness during the trial.

We agree that the jury instructions on the honest-services count were fatally flawed. But we nevertheless conclude the government presented sufficient evidence to support a conviction on that count, so we remand that charge for a new trial. On the other hand, we find no deficiencies with either the jury instructions for or the evidence supporting the computer-fraud charge. Finally, we also reject Van Buren's claim that he was denied his Sixth Amendment right to confront an adverse witness at trial.

II.

We conduct a *de novo* review of the legal correctness of a jury instruction, but we review for abuse of discretion questions concerning the phrasing of an instruction. *United States v. Prather*, 205 F.3d 1265, 1270 (11th Cir. 2000). We likewise review for abuse of discretion a district court's refusal to give a requested jury instruction. *United States v. Carrasco*, 381 F.3d 1237, 1242 (11th Cir. 2004).

As for the sufficiency of evidence to support a conviction, we review that *de novo*, considering the evidence "in the light most favorable to the government and drawing all reasonable inferences and credibility choices in favor of the jury's verdict." *United States v. Taylor*, 480 F.3d 1025, 1026 (11th Cir. 2007). Under this standard, we have explained that the jury's verdict survives "unless no trier of fact could have

found guilt beyond a reasonable doubt." *United States v. Lyons*, 53 F.3d 1198, 1202 (11th Cir. 1995).

Finally, we review *de novo* a Confrontation Clause claim. *United States v. Curbelo*, 726 F.3d 1260, 1271–72 (11th Cir. 2013).

III.

We divide our discussion into three parts. In Section A, we address Van Buren's objections as they pertain to his honest-services-fraud conviction. Section B considers Van Buren's objections to his computer-fraud conviction. And finally, we examine Van Buren's remaining arguments in Section C.

A.

We begin with honest-services fraud. The government theorized that Van Buren deprived the public of his honest services by accepting a bribe, as that act is defined by the federal bribery statute, 18 U.S.C. § 201. Under § 201, a public official may not seek or receive anything of value in return for "being influenced in the performance of any official act." 18 U.S.C. § 201(b)(2). The statute defines an "official act," in turn, as "any decision or action on any question, matter, cause, suit, proceeding or controversy, which may at any time be pending, or which may by law be brought before any public official, in such official's official capacity, or in such official's place of trust or profit." *Id.* § 201 (a)(3).

The controversy here centers on how a jury should be instructed regarding what constitutes an "official act." As relevant on appeal, the district court instructed the jury as follows on the honest-services-fraud count:

With respect to Count 2, you are instructed that it is a federal crime to use interstate wire, radio or television communications to carry out a scheme to defraud someone else of a right to honest services. The Defendant can be found guilty of this crime only if all of the following facts are proven beyond a reasonable doubt:

First, that the Defendant knowingly devised or participated in a scheme to fraudulently deprive the public of the right to honest services of the Defendant through bribery or kickbacks. Second, that the Defendant did so with an intent to defraud the public of the right to the Defendant's honest services; and, third, that the Defendant transmitted or caused to be transmitted by wire, radio or television some communication in interstate commerce to help carry out the scheme to defraud.

. . .

Bribery and kickbacks involve the exchanges of a thing or things of value for ***official action*** by a public official. Bribery and kickbacks also include solicitation of things of value in exchange for official action, even if the thing of value is not accepted or the ***official action*** is not performed, that is, bribery and kickbacks include the public official's solicitation or agreement to accept something of value, whether tangible or intangible, in exchange for an ***official act***, whether or not the payor actually provides the thing of value, and whether or not the public official ultimately performs the requested ***official action***.

> *To qualify as an official act, the public official must have made a decision or taken an action on a question or matter. The question or matter must involve the formal exercise of governmental power. It must also be something specific which requires particular attention to the question or matter by the public official.*

(emphasis added).

Van Buren objected, arguing that the district court should have instead instructed the jury this way:

> To qualify as an official act, the public official must have [made a decision or taken an action] . . . on a question, matter, **cause, suit, proceeding, or controversy**. Further, the question, matter, **cause, suit, proceeding, or controversy** must involve the formal exercise of governmental power. **It must be similar in nature to a lawsuit before a court, a determination before an agency, or a hearing before a committee**. It must also be something specific which requires particular attention by a public official.
>
> **The public official's [decision or action] . . . on that question, matter, cause, suit, proceeding, or controversy may include using his official position to exert pressure on another official to perform an official act, or to advise another official, knowing or intending that such advice will form the basis for an official act by another official. But setting up a meeting, talking to another**

> **official, or organizing an event (or agreeing to do so)—without more—is not an official act.**

(emphases added).[3]

A district court's refusal to provide a requested instruction constitutes reversible error if (1) the requested instruction was legally correct, (2) the content of the requested instruction was not otherwise covered, and (3) the omitted instruction was so vital that its absence seriously impaired the defense. *United States v. Opdahl*, 930 F.2d 1530, 1533 (11th Cir. 1991). After careful review, we conclude that all these conditions are present here, and the district court committed reversible error in declining to instruct the jury that an "official act" "must be similar in nature to a lawsuit before a court, a determination before an agency, or a hearing before a committee." To explain why, we start with *McDonnell v. United States*, 136 S. Ct. 2355 (2016), the case on which Van Buren relied in requesting the refused instruction.

i.

Like Van Buren's case, *McDonnell* also involved a prosecution for honest-services fraud where the government defined the crime by reference to the bribery statute. *McDonnell*, 136 S. Ct. at 2365. There, the government indicted former Virginia Governor Robert McDonnell and his wife, Maureen McDonnell, for bribery. *Id.* at 2361. The couple had accepted about $175,000 in loans, gifts, and other benefits from "the

---

[3] For convenience, we have underlined and bolded the parts of Van Buren's requested instruction that do not appear in the corresponding italicized and bolded instructions the district court gave the jury.

CEO of Star Scientific, a Virginia-based company that developed and marketed Anatabloc, a nutritional supplement made from anatabine, a compound found in tobacco." *Id.* at 2361–62. In exchange, the government alleged, McDonnell had committed at least five "official acts" for Star Scientific and its CEO:

(1) he had arranged meetings between Star Scientific's CEO and Virginia government officials to discuss and promote Star Scientific's interests;

(2) he had hosted and attended events at the Governor's Mansion designed to encourage Virginia university researchers to study and promote Star Scientific's products;

(3) he had contacted other government officials to encourage Virginia state research universities to initiate studies favorable to Star Scientific;

(4) he had promoted Star Scientific by allowing its CEO to invite people to exclusive events at the Governor's Mansion; and

(5) he had recommended that senior government officials in the Governor's office meet with executives from Star Scientific.

Id. at 2365–66.

The district court there instructed the jury that "official acts" are those that "a public official customarily performs," including acts "that have been clearly established by settled practice as part of a public official's position" and acts that further long term goals or contribute to "a series of steps to exercise influence or achieve an end." *Id.* at 2366, 2373. So charged, the jury convicted McDonnell of honest-

services fraud, and the Fourth Circuit affirmed. The Supreme Court, though, vacated that conviction because the instructions incorrectly described an "official act." *Id.* at 2375.

In explaining why, the Court observed that the words "cause, suit, proceeding or controversy" in § 201(a)(3) "connote a formal exercise of governmental power, such as a lawsuit, hearing, or administrative determination." *Id.* at 2368. With that in mind, the Supreme Court applied the interpretive canon *noscitur a sociis* ("a word is known by the company it keeps") to conclude that a "question or matter"—words that appear in the same series of items as "cause, suit, proceeding or controversy" in the definition of "official act"—must likewise "be similar in nature to a cause, suit, proceeding or controversy." *Id.* at 2368-69 (citation and internal quotation marks omitted). Confining the plain meaning of "question" or "matter" in this way makes sense, explained the Court, since otherwise, "the terms 'cause, suit, proceeding or controversy' would serve no role in the statute—every 'cause, suit, proceeding or controversy' would also be a 'question' or 'matter.'" *Id.* at 2369. The Supreme Court also cautioned against considering the question, matter, cause, suit, proceeding or controversy at too high a level of generality; rather, the Court reasoned, any qualifying question, matter, cause, suit, proceeding, or controversy must be "focused and concrete." *Id.*

And to give further color to the phrase "question, matter, cause, suit, proceeding or controversy," *McDonnell* looked to the surrounding text. "Pending" and "may by law be brought," *McDonnell* explained, "suggest something that is relatively circumscribed—

the kind of thing that can be put on an agenda, tracked for progress, and then checked off as complete." *Id.* As for "may *by law* be brought," that implies "something within the specific duties of an official's position." *Id.* And the word "any" indicates that "the matter may be pending either before the public official who is performing the official act, or before another public official." *Id.*

Putting it all together, "question, matter, cause, suit, proceeding or controversy" must be a formal government action analogous to a lawsuit, hearing, or administrative determination that can be pending before any public official. It must be specific and concrete, fall within the duties of an official's position, and be relatively circumscribed, capable of being put on an agenda, tracked for progress, and checked off as complete.

The *McDonnell* Court then applied this definition to the facts of its case. "The first inquiry," the Court said, is whether the activity at issue—a meeting, call, or event—is itself a "question, matter, cause, suit, proceeding or controversy." *Id.* at 2368. Since the Court determined the activity was not, it moved on to the next inquiry: whether the meeting, call, or event could "qualify as a 'decision or action' *on* a different question or matter." *Id.* at 2369.

Answering that question, of course, required the Court to first identify the different question or matter being acted on. *Id.* The Court began by explaining that something like "Virginia business and economic development" could not constitute an underlying matter because it is defined at too high a level of generality and is not something that could be

"pending" before a public official, as the Court has construed "pending." *Id.*

Then the Court turned to the Fourth Circuit's formulation of the underlying questions:

(1) "whether researchers at any of Virginia's state universities would initiate a study of Anatabloc";

(2) "whether the state-created Tobacco Indemnification and Community Revitalization Commission would allocate grant money for the study of anatabine"; and

(3) "whether the health insurance plan for state employees in Virginia would include Anatabloc as a covered drug."

Id. at 2369–70 (citation and internal quotation marks omitted). The Court agreed with that formulation of the questions. Each of those questions, *McDonnell* explained, "is focused and concrete, and each involves a formal exercise of governmental power that is similar in nature to a lawsuit, administrative determination, or hearing." *Id.* at 2370. Still, merely setting up a meeting, hosting an event, or calling another official—while actions related to those questions—ultimately could not qualify as actions or decisions *on* those questions. Something more was needed: for example, a decision to actually initiate a research study or to provide advice to another official with the intent to cause the other official to perform an official act. *Id.*

Then the Supreme Court turned to the jury instructions the district court gave. Based on its interpretation of the "official act" language in § 201, *McDonnell* concluded that the jury instructions were

"significantly overinclusive." *Id.* at 2373–75. In particular, the district court had instructed the jury that an "official act" includes "actions that have been clearly established by settled practice as part of a public official's position" and could include acts designed to contribute to a long-term result. *Id.* at 2373. But that description did not inform the jury that an official act must be *on* a "question, matter, cause, suit, proceeding or controversy," nor did it explain how to identify such an underlying "question, matter, cause, suit, proceeding or controversy." *Id.* at 2374. So while the Fourth Circuit noted possible questions on which McDonnell had perhaps acted, nothing guaranteed that the jury found those questions on its own; instead, the Supreme Court was concerned that the jury may have "convicted Governor McDonnell without finding that he agreed to make a decision or take an action on a properly defined question, matter, cause, suit, proceeding or controversy." *Id.* at 2374–75 (internal quotation marks omitted). As a result, the Court concluded the error in the instructions was not harmless beyond a reasonable doubt. *Id.*

The Supreme Court left it to the Fourth Circuit to decide whether to dismiss the case or remand for a new trial. To make this determination, the Fourth Circuit was to ascertain whether enough evidence existed to convict McDonnell of honest-services fraud, given the Supreme Court's clarification of "official act." If so, the Fourth Circuit could remand for a new trial. Otherwise, it was to dismiss the charge. *Id.* at 2375.

ii.

McDonnell compels us to conclude that the instructions here were erroneous, the error was not

harmless, and a remand for a new trial on the honest-services charge is the appropriate remedy.

As we have noted, the district court instructed jurors that an "official act" involves a decision or action "on a question or matter" and that this question or matter "must involve the formal exercise of governmental power" and be "something specific which requires particular attention." But the court declined to give Van Buren's requested instruction that the question or matter "must be similar in nature to a lawsuit before a court, a determination before an agency, or a hearing before a committee," reasoning that that instruction was inapplicable to Van Buren's case and would only confuse the jury.

This was error. As we have explained, *McDonnell* concluded that the words "cause," "suit," "proceeding," and "controversy" "connote a formal exercise of governmental power, such as a lawsuit, hearing, or administrative determination." *McDonnell*, 136 S. Ct. at 2368. So a "question" or "matter"—housed in the same statutory phrase as "cause," "suit," "proceeding," and "controversy"—similarly must involve a formal action of the same gravity as a lawsuit, hearing, or administrative determination. That analogy—"such as a lawsuit, hearing, or administrative determination"—is critical to understanding the meaning of "question" or "matter" as those terms are used in the federal bribery statute. And because the qualification that the "question or matter" be similar in nature to a "lawsuit, hearing, or administrative determination" is the product of statutory interpretation, not of *McDonnell*'s facts, this qualification applies with equal force to Van Buren's case.

This qualification also provides crucial context for what "formal exercise of governmental power" means, as that phrase is used in the district court's jury instruction. Without this analogy limiting the meaning of "question" or "matter," a "formal exercise of governmental power" could mean anything that a public official does that falls within the scope of the official's duties. Omitting the analogy unravels essential statutory limitations that the Supreme Court identified concerning the meaning of "official act."

Naturally, removing those protections opens the door to the same harmful effects that the Supreme Court described in *McDonnell*. Although the district court here informed the jury that the "question" or "matter" had to be a "formal exercise of governmental power," that phrase did not illuminate the scale or nature of the "question" or "matter" that would qualify, since it was not accompanied by an instruction that the exercise of governmental power must be comparable to a lawsuit, agency determination, or committee hearing. As in *McDonnell*, then, the instructions "provided no assurance that the jury reached its verdict after finding" a qualifying underlying question or matter. 136 S. Ct. at 2374.

And the government's arguments only reinforce our doubt that the jury identified a proper "question" or "matter" before convicting Van Buren. The government does not argue that the license-plate search is itself the question or matter, but rather that the search was an action *on* a question or matter. But the government's formulation of the "question" or "matter" at issue reveals its own misinterpretation of those terms as they are used in the federal bribery statute. Specifically, the government contends that the

underlying "question" is "whether to provide information to Albo about whether a woman was working as an undercover police officer."

That, of course, is not a "question" or "matter" comparable to a lawsuit, hearing, or administrative determination. Nor is it a "question" or "matter" like the ones the Supreme Court identified as similar in *McDonnell*. As we have noted, those questions asked whether to initiate a study at a state university, whether to allocate grant money for a particular study, and whether to include something as a covered drug. *McDonnell*, 136 S. Ct. at 2370. Each of these three "questions" is a formal exercise of governmental power that is similar in nature to, say, an administrative determination. Merely divulging information to a civilian is not. And if the government could not identify a proper question on which Van Buren acted, we can have no confidence that the jury did.

The government's incorrect formulation of the "question" or "matter" here also threatens to transform any improper disclosure by a public official into an "official act" under the bribery statute, regardless of whether the disclosure was meant to influence a formal exercise of governmental power that is analogous to a lawsuit, hearing, or administrative determination. But as *McDonnell* reminded us, "a statute in this field that can linguistically be interpreted to be either a meat axe or a scalpel should reasonably be taken to be the latter." 136 S. Ct. at 2373 (citing *United States v. Sun-Diamond Growers of Cal.*, 526 U.S. 398, 408, 412 (1999)).

Not only was the government's "question" incorrect, but the jury instructions also prevented Van

Buren from pointing out the government's mistake. Because the jury was not told that the "question" or "matter" must be similar in nature to a lawsuit before a court, a determination before an agency, or a hearing before a committee, Van Buren had no effective way to highlight the government's failure to identify an appropriate "question" on those grounds. Had the jury been properly instructed, Van Buren very well could have successfully made that argument. So we cannot say the error was harmless. *See United States v. Browne*, 505 F.3d 1229, 1267–68 (11th Cir. 2007) ("The correct focus of harmless-error analysis is whether it is clear beyond a reasonable doubt that a rational jury would have found the defendant guilty in the absence of the error.").

In sum, Van Buren's requested jury instruction that the question or matter "must be similar in nature to a lawsuit before a court, a determination before an agency, or a hearing before a committee" was correct and would have conveyed critical information that the instructions did not otherwise cover. Its omission deprived Van Buren of a potent argument and allowed the jury to convict him without identifying a qualifying "question" or "matter" on which he acted.

We therefore vacate Van Buren's honest-services-fraud conviction. *Opdahl*, 930 F.2d at 1533 (explaining that failure to give a requested instruction is reversible if the instruction is correct, not otherwise covered, and important enough that its omission seriously impaired the defense). To the extent our prior precedent holds that an "official act" is simply "[e]very action that is within the range of official duty," *see United States v. Moore*, 525 F.3d 1033, 1041 (11th Cir. 2008) (quoting *United States v. Birdsall*, 233 U.S. 223, 230 (1914)),

without regard to whether that action is on a proper "question, matter, cause, suit, proceeding or controversy," it has clearly been abrogated by *McDonnell*. *See United States v. Archer*, 531 F.3d 1347, 1352 (11th Cir. 2008) (showing how an intervening decision by the Supreme Court abrogates clearly inconsistent precedent).

Nevertheless, our vacatur of Van Buren's honest-services-fraud conviction does not end our inquiry into that charge. Van Buren also argues the government failed to present sufficient evidence to convict him of bribery, raising the question of whether we should remand for retrial or dismiss the charge. *McDonnell*, 136 S. Ct. at 2375. After examining the evidence, we conclude a retrial is warranted.

Had the government identified a correct question or matter, the evidence, when viewed in the light most favorable to the government, was sufficient to allow a reasonable juror to conclude that Van Buren was guilty of bribery beyond a reasonable doubt. *Taylor*, 480 F.3d at 1026 (describing standard of review on a sufficiency-of-the-evidence challenge). Among other things, Van Buren confessed to the FBI and GBI that he ran the tag search for money. He also said that he knew the purpose of the search was to discover and reveal whether Carson, the woman Albo allegedly met at the club, was an undercover officer. If the government had identified the underlying matter as something like an investigation into illegal activity, such as prostitution, at the strip club, it may have been able to prove its case.

Such an investigation would have been a specific, formal government action, within the ambit of police

activity, that is comparable to a lawsuit, hearing, or administrative determination. It could have been put on an agenda, tracked for progress, and marked off as complete. And Van Buren could have acted *on* the underlying investigation because he could have influenced its findings had he identified an undercover agent in his tag search and revealed her cover to Albo. That Carson did not exist does not matter. The government presented evidence that Van Buren was fully prepared, and acted, to compromise a potential investigation, in exchange for money. His guilt or innocence cannot turn on whether he was lucky enough that the person he searched for fortuitously did not exist or that no investigation of the strip club was actually occurring.

For these reasons, we remand for a new trial on the honest-services-fraud count. *McDonnell*, 136 S. Ct. at 2375.

B.

Next, we turn to Van Buren's computer-fraud conviction. For searching Carson's tag in the GCIC system, Van Buren was convicted of violating the Computer Fraud and Abuse Act, which makes it a crime to obtain "information from any protected computer" by "intentionally access[ing] a computer without authorization or exceed[ing] authorized access." 18 U.S.C. § 1030(a)(2)(C). Van Buren contends that two problems specific to his computer-fraud charge undermine his conviction. He argues, first, that the district court should have instructed the jury on the lesser-included offense of misdemeanor computer fraud, and, second, that the government did not

present enough evidence to sustain his conviction. We are not persuaded.

i.

The computer-fraud crime of which Van Buren was convicted is a misdemeanor unless, among other things, it was committed for private financial gain, in which case it is a felony. 18 U.S.C. § 1030(c)(2). The district court instructed the jury on only felony computer fraud: it told the jury that to return a guilty verdict against Van Buren, it must conclude that Van Buren acted for private financial gain. But it did not raise the possibility that Van Buren could still be convicted of the lesser-included, misdemeanor version of the offense, should thejury conclude the financial element was missing. Van Buren argues that this omission of the misdemeanor instruction amounted to reversible error.

To succeed on his claim, Van Buren must meet a two-part test. First, he must satisfy the "elements test" by proving that the charged offense encompasses all the elements of the lesser offense. Here, that is not a problem. Indeed, the parties do not dispute that the "elements test" is satisfied: the sole difference between the felony and misdemeanor versions of crime, as relevant to Van Buren's case, is the private-financial-gain element. But Van Buren must also meet a second requirement: he must demonstrate that the evidence would have allowed a rational jury to acquit him of the greater offense while convicting him of the lesser. *United States v. Whitman*, 887 F.3d 1240, 1246–47 (11th Cir. 2018), *cert. denied,* 139 S. Ct. 1276, 203 (2019). This he cannot do.

Van Buren's problem arises from the fact that the record contains no evidence that Van Buren engaged in computer access for any reason other than financial gain. As an initial matter, Van Buren's argument that there is evidence he ran the search as part of a good-faith effort to investigate Albo's other troubles with women does him no good: if Van Buren truly ran the PKP1568 tag as part of a legitimate good-faith investigation, that would absolve him of computer fraud entirely, since he would just be doing his job. As a result, even assuming a jury could find he acted in good faith, that would not support the inference that a rational jury could have convicted him of misdemeanor computer fraud. Plus, the record lacks any evidence that Van Buren ran the PKP1568 tag as part of a good-faith investigation.

Perhaps sensing the hole in this argument, Van Buren alternatively urges that the money he received was only a loan. Even if we call the money Van Buren received a "loan," though, a loan still confers financial benefit. As Van Buren admitted, he needed money to cover his bills but was having trouble securing a loan because of his poor credit. So receiving what appears to be an interest-free cash loan that he could use to cover any immediate needs counts as financial gain.

Van Buren next claims the record contains evidence that he ran the GCIC search before Albo offered him money to do so. This "evidence" appears to consist of the brief phone call between Van Buren and Albo on the morning of August 31, 2015, when Albo asked Van Buren if he had run the license plate yet, and Van Buren replied, "I don't—I don't think I got the right plate numbers from you." Van Buren suggests this conversation demonstrates that Van Buren had

already run a search on Carson's plate before receiving the $1,000 payment, so he had no financial motive for the unauthorized search.

But the rest of the record frustrates Van Buren's attempt to capitalize on his stray remark. First, on August 21—ten days before the August 31 conversation on which Van Buren relies—Van Buren had already received $5,000 from Albo and agreed in principle to investigate Carson. And second, even setting aside those facts, which independently establish financial gain, the record reflects that Albo did not provide Van Buren with Carson's purported plate number for the first time until *after* the August 31 conversation. In fact, Van Buren only ever tried to run Carson's alleged tag number once, and that occurred on September 2, 2015—again, after the August 31 conversation. So on this record, Van Buren's "I don't think I got the right plate numbers from you" comment can be understood to mean only that he had not yet received Carson's license-plate information from Albo.

Finally, Van Buren tries to show that a jury could have determined he wrongly accessed the computer for reasons other than financial gain: he highlights a comment he made to Albo during a recorded conversation on August 26, 2015. At that time, Van Buren stated, "I'm not charging for helping you out." In that convoluted exchange, though, Van Buren simultaneously claimed he was not looking into Carson for money, while he also probed whether Albo would continue to "help [him] out with the rest of the medical bills." Van Buren refers to the "rest" of the bills, of course, because he had already received $5,000 of the $15,368 he allegedly needed and had already agreed to

research Carson's identity by that point. And later, Van Buren texted Albo for more money as a condition of running the search and took another $1,000. But perhaps most significantly, Van Buren expressly confessed to the FBI and GBI that he ran the tag search for money.

In short, no jury could have rationally believed that if Van Buren searched Carson's tag in the GCIC system on September 2, 2015, he did it for some non-financial, unidentified reason. The district court therefore did not abuse its discretion in declining to give the misdemeanor-computer-fraud instruction.

ii.

We next consider Van Buren's contention that the evidence did not sufficiently support his conviction for computer fraud. Although styled as a sufficiency-of-the-evidence challenge, the animating force behind this argument is an appeal to overrule *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), where we held that even a person with authority to access a computer can be guilty of computer fraud if that person subsequently misuses the computer.

Rodriguez, the defendant in that case, was a Social Security Administration ("SSA") employee who, for personal reasons, used the SSA's computer database to research information such as birth dates and home addresses of 17 people. *Rodriguez*, 628 F.3d at 1260. This violated SSA policy, which prohibited employees from obtaining information from SSA databases without a legitimate business reason. *Id.* Rodriguez was convicted of computer fraud.

On appeal, though, he argued he was innocent because "he accessed only databases that he was

authorized to use," albeit for inappropriate reasons. *Id.* at 1263. We rejected that argument. We noted that the computer-fraud statute defines "exceeds authorized access," as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled [so] to obtain or alter." *Id.* at 1263 (quoting § 1030(e)(6)). Then we determined that the defendant had "exceeded his authorized access and violated the [computer-fraud statute] when he obtained [the victims'] personal information *for a nonbusiness reason*." *Id.* (emphasis added).

Van Buren points out that our sister circuits have criticized *Rodriguez*'s interpretation of "exceeds authorized access," since it purportedly allows employers or other parties to legislate what counts as criminal behavior through their internal policies or their terms of use. Echoing the defendant's argument in *Rodriguez*, Van Buren alleges that he is innocent of computer fraud because he accessed only databases that he was authorized to use, even though he did so for an inappropriate reason.

We acknowledge that other courts have rejected *Rodriguez*'s interpretation of "exceeds authorized access." *See, e.g.*, *United States v. Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) (en banc) (noting that activities like "[Google]-chatting with friends, playing games, shopping or watching sports highlights" on a work computer are routinely prohibited by computer-use policies, and worrying that "under the broad interpretation of the [computer-fraud statute], such minor dalliances would become federal crimes"); *United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015) ("While the Government might promise that it would

not prosecute an individual for checking Facebook at work, we are not at liberty to take prosecutors at their word in such matters."). But under our prior-precedent rule, "a prior panel's holding is binding on all subsequent panels unless and until it is overruled or undermined to the point of abrogation by the Supreme Court or by this court sitting *en banc*." *Archer*, 531 F.3d at 1352. Since Van Buren has identified no Supreme Court or en banc decision of this Circuit that abrogates *Rodriguez*, we must continue to follow it.

And under *Rodriguez*, there is no question that the record contained enough evidence for a jury to convict Van Buren of computer fraud. The evidence showed that Van Buren accepted $6,000 and agreed to investigate Carson. It demonstrated that Van Buren searched what was supposed to be Carson's tag in the GCIC database. At trial, one of the assistant deputy directors of the GCIC testified that the database is supposed to be used for law-enforcement purposes only and that officers are trained on the proper and improper uses of the system. Van Buren also admitted to the FBI and GBI that he knew it was "wrong" to run the tag search and that he had done so for money. And as we have noted, *Rodriguez* previously rejected the contention that misusing databases a defendant lawfully can access does not constitute computer fraud. Taken in the light most favorable to the verdict, under our binding Circuit precedent, a jury could have found beyond a reasonable doubt that Van Buren committed computer fraud for financial gain.

C.

Van Buren raises two remaining arguments: one challenging the district court's decision to decline

giving good-faith instructions to the jury, and the other asserting that his Sixth Amendment right to confront Albo was violated at trial. We address each in turn.

i.

First, Van Buren contends the district court abused its discretion in refusing to give his requested good-faith instructions. Specifically, Van Buren asked for two good-faith instructions, one explaining that good faith is a complete defense to any charge that requires willfulness and one explaining that good faith is a complete defense to any charge that requires intent to defraud. The district court declined to give those instructions, reasoning that the record lacked any evidentiary basis to support them. That decision fell within the proper scope of the district court's discretion.

As we have explained, a district court's refusal to provide a requested instruction is reversible error if (1) the requested instruction was legally correct, (2) the content of the requested instruction was not otherwise covered, and (3) the omitted instruction was so vital that its absence seriously impaired the defense. *Opdahl*, 930 F.2d at 1533. A good-faith instruction is legally correct if *any* foundation in evidence supports it. *United States v. Martinelli*, 454 F.3d 1300, 1315 (11th Cir. 2006). But Van Buren has not met even this minimal evidentiary bar.

He points out that in the past, he and other officers had searched license plates Albo had provided, as part of legitimate investigations into Albo's issues with other women. That's true. What's missing, though, is *any* evidence that Van Buren searched the particular tag at issue this time—PKP1568—for a law-

enforcement purpose. So Van Buren's requested instruction is not "correct" because no evidentiary basis supports it.

Nor has Van Buren showed that omission of the good-faith instructions seriously impaired his defense, since even assuming that any trace of good faith could be squeezed from the record, it would have been negligible in the face of the overwhelming evidence of wrongdoing. *See Martinelli*, 454 F.3d at 1316 (holding that the absence of a good-faith instruction did not seriously impair the defense, since "the evidence of fraud . . . was overwhelming and the evidence of good faith was slight.").

ii.

Finally, Van Buren argues he was deprived of his Sixth Amendment right to confront adverse witnesses. Albo did not testify at Van Buren's trial because he allegedly had fled to Italy. In Albo's absence, the government played the recordings that the FBI had taped of the conversations between Albo and Van Buren. Van Buren contends that the admission of Albo's statements on the recordings violated his constitutional right to confront Albo. We find no merit to that argument.

The Sixth Amendment's Confrontation Clause guarantees a criminal defendant "the right . . . to be confronted with the witnesses against him." U.S. Const. amend. VI. This usually means that the defendant must have an opportunity to cross-examine an adverse witness at trial before that witness's statements may be admitted. *Crawford v. Washington*, 541 U.S. 36, 53-54 (2004). But significantly, the Confrontation Clause does not block statements that

are used "for purposes other than establishing the truth of the matter asserted." *Id.* at 59 n.9.

For instance, in *United States v. Price*, 792 F.2d 994 (11th Cir. 1986), the government relied on recordings between the defendant and another individual, since the person who made the recordings had passed away before trial. *Id.* at 996. The defendant asserted that admitting the other person's statements on the recording violated his Confrontation Clause right. We rejected that argument, finding that "[t]he single purpose for admitting the [other person's] statements was to make understandable to the jury the statements made by [the defendant] himself." *Id.* at 997. Put simply, the statements in question were not offered for their truth, so the defendant's "Sixth Amendment right of confrontation and to present a defense was not violated by the introduction of the tapes into evidence." *Id.*

The same is true here: Albo's statements were admitted only to provide context for Van Buren's statements and to show their effect on Van Buren. For example, whether Albo was actually interested in Carson or whether he actually wanted to learn her real identity was not at issue here; the truth or falsity of those claims did not tend to make it more or less likely that Van Buren had committed a charged crime. Rather, the government offered those statements solely to put into context Van Buren's remarks and actions. Because none of Albo's recorded statements was offered for its truth, none was subject to the Confrontation Clause.

IV.

For all the above reasons, we vacate Van Buren's honest-services-fraud conviction and remand for a new trial on that charge. We affirm his computer-fraud conviction.

VACATED AND REMANDED IN PART; AFFIRMED IN PART.

APPENDIX B

United States Code Title 18
Crimes and Criminal Procedure
Part I. Crimes
Chapter 47. Fraud and False Statements

18 U.S.C. § 1030. Fraud and related activity in connection with computers

Effective: January 7, 2011

(a) Whoever—

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

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

(A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) [1] of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.);

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

(C) information from any protected computer;

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

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

(5)

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

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

(C) intentionally accesses a protected computer without authorization, and as a result of such conduct, causes damage and loss.[2]

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

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

(B) such computer is used by or for the Government of the United States; [3]

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

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

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

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

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

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

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

(1)

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

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

(2)

(A) except as provided in subparagraph (B), a fine under this title or imprisonment for not more than one year, or both, in the case of an offense under subsection (a)(2), (a)(3), or (a)(6) of

this section which does not occur after a conviction for another offense under this section, or an attempt to commit an offense punishable under this subparagraph;

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

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

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

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

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

(3)

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

or an attempt to commit an offense punishable under this subparagraph; and

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

(4)

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

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

(I) loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;

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

(III) physical injury to any person;

(IV) a threat to public health or safety;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(d)

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

(2) The Federal Bureau of Investigation shall have primary authority to investigate offenses under subsection (a)(1) for any cases involving espionage,

foreign counterintelligence, information protected against unauthorized disclosure for reasons of national defense or foreign relations, or Restricted Data (as that term is defined in section 11y of the Atomic Energy Act of 1954 (42 U.S.C. 2014(y)), except for offenses affecting the duties of the United States Secret Service pursuant to section 3056(a) of this title.

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

(e) As used in this section—

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

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

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

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

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

(4) the term "financial institution" means—

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

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

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

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

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

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

(G) the Securities Investor Protection Corporation;

(H) a branch or agency of a foreign bank (as such terms are defined in paragraphs (1) and (3)

of section 1(b) of the International Banking Act of 1978); and

(I) an organization operating under section 25 or section 25(a) 1 of the Federal Reserve Act;

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

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

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

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

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

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

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

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

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

(g) Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses [5] (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages. No action may be brought under this subsection unless such action is begun within 2 years of the date of the act complained of or the date of the discovery of the damage. No action may be brought under this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware.

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

(i)

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

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

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

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

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

(1) Any personal property used or intended to be used to commit or to facilitate the commission of

any violation of this section, or a conspiracy to violate this section.

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