No. 19-783

In the Supreme Court of the United States

NATHAN VAN BUREN

v.

UNITED STATES OF AMERICA

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

BRIEF FOR THE UNITED STATES

JEFFREY B. WALL
Acting Solicitor General
Counsel of Record
BRIAN C. RABBITT
Acting Assistant Attorney General
ERIC J. FEIGIN
Deputy Solicitor General
MORGAN L. RATNER
Assistant to the Solicitor General
JENNY C. ELLICKSON
Attorney

Department of Justice
Washington, D.C. 20530-0001
SupremeCtBriefs@usdoj.gov
(202) 514-2217

QUESTION PRESENTED

Whether the evidence was sufficient to establish that petitioner, a police sergeant, exceeded his authorized access to a protected computer to obtain information for financial gain, in violation of 18 U.S.C. 1030(a)(2)(C) and (c)(2)(B)(i), when in exchange for a cash payment, he searched a confidential law-enforcement database for information about whether a particular person was an undercover police officer.

TABLE OF CONTENTS

Page

Table of Contents—Continued: Page

TABLE OF AUTHORITIES

Cases:

Cases—Continued: Page

Cases—Continued: Page

Constitution and statutes:

Statutes—Continued: Page

Miscellaneous—Continued: Page

Miscellaneous—Continued: Page

In the Supreme Court of the United States

No. 19-783

NATHAN VAN BUREN

v.

UNITED STATES OF AMERICA

ON WRIT OF CERTIORARI
TO THE UNITED STATES COURT OF APPEALS
FOR THE ELEVENTH CIRCUIT

BRIEF FOR THE UNITED STATES

OPINION BELOW

The opinion of the court of appeals (Pet. App. 1a-32a) is reported at 940 F.3d 1192.

JURISDICTION

The judgment of the court of appeals was entered on October 10, 2019. The petition for a writ of certiorari was filed on December 18, 2019, and was granted on April 20, 2020. The jurisdiction of this Court rests on 28 U.S.C. 1254(1).

STATUTORY PROVISIONS INVOLVED

Pertinent statutory provisions are reproduced in the appendix to this brief. App., *infra*, 1a-13a.

STATEMENT

Following a jury trial in the United States District Court for the Northern District of Georgia, petitioner

was convicted on one count of exceeding authorized access to a protected computer to obtain information for financial gain, in violation of 18 U.S.C. 1030(a)(2)(C) and (c)(2)(B)(i), and one count of honest-services wire fraud, in violation of 18 U.S.C. 1343, 1346, and 1349. Judgment 1. The district court sentenced petitioner to 18 months of imprisonment, to be followed by two years of supervised release. Judgment 2-3. The court of appeals affirmed petitioner's Section 1030 conviction, vacated petitioner's wire-fraud conviction, and remanded for a new trial on the wire-fraud count. Pet. App. 1a-32a.

A. Legal Background

1. By the early 1980s, "the subject of computer-related crimes" had captured the public's attention. H.R. Rep. No. 894, 98th Cong., 2d Sess. 8 (1984) (1984 House Report); see S. Rep. No. 432, 99th Cong., 2d Sess. 2 (1986) (1986 Senate Report). At the time, no federal statute specifically addressed "the area of computer crime," and other federal criminal statutes, such as the wire-fraud statute, 18 U.S.C. 1343, were proving to be an imperfect fit for some "computer-related crimes." 1984 House Report 6.

Congress took an interest in the problem, and in late 1983 and early 1984 the House Judiciary Committee's Subcommittee on Crime held several hearings on "computer fraud and abuse." 1984 House Report 4, 12; see generally *Counterfeit Access Device and Computer Fraud and Abuse Act: Hearings Before the Subcomm. on Crime of the House Comm. on the Judiciary*, 98th Cong., 1st & 2d Sess. (1983-1984) (1983-1984 Hearings). The congressional inquiry addressed not just the "hackers" that had garnered significant public attention, but also the increasing threats from corrupt "insiders." For example, a state prosecutor urged in the hearings that

Congress "should focus on corrupt 'insiders,'" even though that focus "may jar with recent headlines concerning pre-teen and teen-age 'hackers.'" 1983-1984 Hearings 231 (statement of James F. Falco); see *id.* at 225, 232. And another witness shared a recent front-page New York Times article, which had opened with an anecdote about how an "auxiliary policeman" in Connecticut had "us[ed] the Police Department computer to check records for his full-time employer," but "was never charged with a crime." *Id.* at 86; see *id.* at 84 (statement of Robert A. Hoadley).

In contemporaneous congressional inquiries, a staff report explained that "[a]lthough media attention consistently focuses on the threats from 'computer hackers' and other outside intruders, the greatest threat to computerized resources remains personnel who are authorized to access them." Staff of the Subcomm. on Transportation, Aviation and Materials of the House Comm. on Science and Technology, 98th Cong., 2d Sess., *Computer and Communications Security and Privacy* 4 (Comm. Print 1984). And a Representative testified that "even though the hackers got a lot of publicity, I am more worried about the employee in the social security system or the teller at a bank * * * who is playing around with the computer system to which he already has access." *Computer Crime: Hearing Before the Subcomm. on Civil and Constitutional Rights of the House Comm. on the Judiciary*, 98th Cong., 1st Sess. 7-8 (1983) (testimony of Rep. Dan Glickman).

Following the 1983 and 1984 hearings, Congress enacted the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, Tit. II, §§ 2101-2102, 98 Stat. 2190-2192, which included a new computer-crime prohibition codified in 18 U.S.C.

1030. Section 1030(a) made it a crime to obtain national-security information or financial records, or to use, modify, destroy, or disclose information on federal-government computers, by "knowingly access[ing] a computer without authorization, or having accessed a computer with authorization, us[ing] the opportunity such access provides for purposes to which such authorization does not extend." 18 U.S.C. 1030(a) (Supp. II 1984). Section 1030 thus applied not only to outside hackers who accessed computers without authorization, but also to insiders who were "authorized to use a computer" but "access[ed] it knowing that the access [was] for a purpose not contemplated by the authorization." 1984 House Report 21.

2. In 1986, Congress enacted the Computer Fraud and Abuse Act of 1986, Pub. L. No. 99-474, 100 Stat. 1213, which made several modifications to Section 1030. The accompanying House Report explained that the amendments addressed "gaps" in the original statute and "clarif[ied] the existing law." H.R. Rep. No. 612, 99th Cong., 2d Sess. 4 (1986) (1986 House Report).

One refinement that the Senate Report described as "intend[ed] * * * to simplify the language" was to "substitute[] the phrase 'exceeds authorized access' for the more cumbersome phrase * * * 'or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend.'" 1986 Senate Report 9 (citation omitted). Pursuant to the 1986 Act, the phrase "exceeds authorized access" was—and still is—defined, in 18 U.S.C. 1030(e)(6), 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." Computer Fraud and Abuse

Act of 1986, § 2(g)(4), 100 Stat. 1215. The House Report, similar to the Senate Report, explained that "[t]he purpose of this change [wa]s merely to clarify the language in existing law." 1986 House Report 11.

3. In 1994, Congress broadened the statute, including by expanding the coverage of Section 1030(a)(5)—a provision covering unauthorized access that causes damage—and adding a new provision, Section 1030(g), that allows a person who suffers damage or loss from a Section 1030 violation to bring a civil action against the violator. Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, Tit. XXIX, § 290001(b) and (d), 108 Stat. 2097-2098.

Two years later, the Economic Espionage Act of 1996, Pub. L. No. 104-294, 110 Stat. 3488, created the first federal criminal laws punishing the theft and misappropriation of trade secrets, see § 101, 110 Stat. 3488-3491, and simultaneously amended Section 1030, see § 201, 110 Stat. 3491-3494. The accompanying Senate Report stated that the amendments would "strengthen" the statute "by closing gaps in the law to protect better the confidentiality, integrity, and security of computer data and networks." S. Rep. No. 357, 104th Cong., 2d Sess. 3 (1996) (1996 Senate Report). It identified particular concerns about "Government employees who abuse their computer access privileges to obtain Government information that may be sensitive and confidential," and about ensuring protection for "information on any civilian or State and local government computers." *Id.* at 4.

Congress accordingly amended Section 1030 to cover anyone who intentionally accesses a computer without authorization or "exceeds authorized access" and

thereby obtains information from any federal department or agency. 18 U.S.C. 1030(a)(2)(B) (Supp. II 1996); see Economic Espionage Act of 1996, § 201(1)(B)(ii), 110 Stat. 3492. And it added a provision, 18 U.S.C. 1030(a)(2)(C) (Supp. II 1996), that addresses the same issue with respect to civilian and State computers with an interstate nexus. See § 201(1)(B)(ii), 110 Stat. 3492. Following an additional broadening amendment in 2008, Section 1030(a)(2)(C) criminalizes intentionally accessing a computer without authorization, or "exceed[ing] authorized access," and thereby obtaining information from any "protected computer," defined to include any computer used in or affecting interstate or foreign commerce or communication. 18 U.S.C. 1030(a)(2)(C); see 18 U.S.C. 1030(e)(2); Economic Espionage Act of 1996, § 201(1)(B)(i), 110 Stat. 3492; Identity Theft Enforcement and Restitution Act of 2008, Pub. L. No. 110-326, Tit. II, § 203, 122 Stat. 3561.

A first-time violation of Section 1030(a)(2) is a misdemeanor with a maximum penalty of one year of imprisonment. 18 U.S.C. 1030(c)(2)(A). That penalty increases to five years 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 state or federal law; or (iii) "the value of the information obtained exceeds $5,000." 18 U.S.C. 1030(c)(2)(B).

B. Factual Background

1. Petitioner was a police sergeant in Cumming, Georgia. Pet. App. 3a. In that capacity, he was entrusted with a username and password for a data-communications network managed and maintained by

the Georgia Crime Information Center (GCIC), a division of the Georgia Bureau of Investigation. J.A. 8-9, 19-25; see Pet. App. 6a.

The GCIC computer system gives law-enforcement agencies access to a number of official government computer databases, including the National Crime Information Center (NCIC) database maintained by the Federal Bureau of Investigation (FBI). J.A. 22-24; see Pet. App. 6a. The NCIC database, in turn, contains many sensitive law-enforcement files, including information about known suspected terrorists, fugitives, wanted persons, gangs, protective orders, and stolen vehicles. J.A. 24.

In order to receive a username and password, petitioner had to complete training on the limits of his authorization to access the GCIC computer system and the associated law-enforcement databases. J.A. 10-11, 19-20, 24-25. The training explained that law-enforcement officers are authorized to run searches on the GCIC system only for law-enforcement purposes and that state law imposes criminal penalties on officers who access such information for personal use. J.A. 11-14, 16-17, 28-31.

2. Petitioner nevertheless used his access to the GCIC system for personal financial gain by accepting a cash payment from Andrew Albo, a frequent subject of police action, to determine whether someone was an undercover officer. Pet. App. 3a-6a. The deputy chief of petitioner's police department considered Albo—who allegedly accused young women whom he paid to spend time with him of harassment or theft—to be "very volatile" and warned officers in the department to "be careful" with him. *Id.* at 4a. Petitioner did not heed that advice and instead fostered a relationship with Albo,

culminating in his accepting money to obtain computerized law-enforcement information for Albo. See *id.* at 3a-6a.

Petitioner first met Albo when he helped to arrest Albo for providing alcohol to a minor. Pet. App. 4a. As petitioner continued to frequently handle disputes between Albo and various women, he apparently came to view Albo as a potential solution for his financial difficulties. *Ibid.* Petitioner asked Albo for a loan, falsely claiming that he needed around $15,000 to pay his son's medical bills. *Ibid.* When Albo responded that he was "trying to stay out of trouble," petitioner replied that "there's no law against you helping a friend out," D. Ct. Doc. 87-4, at 13 (Oct. 30, 2017), and assured Albo that no one would have to know about the loan, *id.* at 14.

Unbeknownst to petitioner, Albo recorded that conversation and confided in his priest about petitioner's loan request. Pet. App. 4a; D. Ct. Doc. 126, at 122, 143 (July 10, 2018). The priest put Albo in touch with a detective in the Forsyth County Sheriff's Office, and Albo told the detective that petitioner had begun to "shake him down for his money." D. Ct. Doc. 126, at 123. The FBI was informed of petitioner's loan solicitation, and it planned a sting operation in which Albo would offer petitioner cash in exchange for confidential law-enforcement information. Pet. App. 4a. As part of that plan, Albo had lunch with petitioner and gave petitioner an envelope containing $5000. *Id.* at 5a. Petitioner offered to pay Albo back, but Albo responded that money was "not the issue." *Ibid.*

Albo told petitioner that he had met a woman he liked at a strip club and needed to know whether she was an undercover police officer before pursuing her further. Pet. App. 5a. Albo asked petitioner to find out

whether the woman was an undercover officer, and petitioner agreed to help. *Ibid.* In a subsequent conversation, also orchestrated by the FBI, Albo asked petitioner whether he would be willing to help Albo's friends transport drugs in the area in exchange for "big money." D. Ct. Doc. 87-7, at 37 (Oct. 30, 2017). Petitioner told him, "I'll see what I can come up with," *id.* at 39, and volunteered that "I've got contacts everywhere," *id.* at 42.

Several days later, Albo asked petitioner whether he had run a search for the woman's license-plate number, and petitioner responded that he did not think that he had received the correct license-plate number from Albo. Pet. App. 5a; see Gov't Trial Ex. 8A, at 2-3. Petitioner instructed Albo to text him the number, and Albo responded by sending petitioner a fake license-plate number that the FBI had created. Pet. App. 5a. Petitioner told Albo that he would look into the matter but needed the "item" first. *Ibid.* Albo responded that he had "2," and the pair arranged to meet for lunch. *Ibid.* At lunch, Albo gave petitioner an envelope containing $1000 and apologized for not having the $2000 that they had discussed. *Ibid.* Petitioner asked Albo for the woman's name and promised to conduct the search soon. *Id.* at 5a-6a. Albo replied that once petitioner had run the search, "I will have all the money for you." *Id.* at 6a.

3. A few days later, petitioner used a computer terminal in his patrol car, and his username and password, to access the GCIC system in order to carry out his deal with Albo. Pet. App. 6a; see J.A. 8-9. Petitioner searched the GCIC system for the registration information associated with the (fake) license-plate number that Albo had provided. *Ibid.* The search enabled petitioner to obtain information relating to the fake number

from a database of vehicle-registration information maintained by the Georgia Department of Revenue. J.A. 26-27; see Pet. App. 6a. That information, which FBI investigators had entered into the database in connection with this investigation, included the name and address of the purported owner of the car associated with the fake license-plate number. J.A. 32. Through the same GCIC search, petitioner also obtained information from the NCIC database indicating that the license-plate number was not associated with a stolen vehicle. J.A. 28. Petitioner then texted Albo to tell him that he had information for him. Pet. App. 6a.

After petitioner ran the license-plate search, the FBI agents investigating his conduct decided to take immediate action because they "didn't want him on the streets any more as a police officer." D. Ct. Doc. 127, at 93 (July 10, 2018). The FBI thus stopped investigating whether petitioner might also be willing to assist a drug-transportation scheme. *Ibid.* Instead, agents from the Georgia Bureau of Investigation and the FBI visited petitioner's home and interviewed him. Pet. App. 6a. During the interview, petitioner admitted that Albo "gave me $1,000" to run the license-plate search and that he knew that running the search for Albo was "wrong." *Ibid.*

C. Proceedings Below

1. Following indictment by a federal grand jury, petitioner went to trial on one count of exceeding authorized access to a protected computer to obtain information for private financial gain, in violation of 18 U.S.C. 1030(a)(2)(C) and (c)(2)(B)(i), and one count of honest-services wire fraud, in violation of 18 U.S.C. 1343, 1346, and 1349. Superseding Indictment 1-5; see Pet. App. 6a. Both at the close of the government's case and at the

close of all evidence, petitioner moved for a judgment of acquittal, arguing, among other things, that a person cannot "exceed authorized access" under Section 1030 by "accessing information that [he has] access to * * * for an improper or impermissible purpose." J.A. 35-36. The district court denied petitioner's motion. J.A. 37; D. Ct. Doc. 128, at 123-125 (July 10, 2018).

In accord with petitioner's own proposal, however, the jury was instructed that the Section 1030 count required the government to prove that petitioner used his "authorized access" to a computer "to get or []change information that [he was] not permitted to get or change." D. Ct. Doc. 129, at 51 (July 10, 2018); see D. Ct. Doc. 70, at 21 (Oct. 23, 2017). During closing arguments, petitioner's counsel argued that petitioner had not exceeded his authority to access the GCIC computer system because petitioner "had a password" and "was certified for GCIC searches." J.A. 40. The government, in contrast, contended that petitioner had exceeded his authorized access to the GCIC computer system when he searched for the fake license-plate number for his "own private gain" and for a "non[-]law[-]enforcement purpose." J.A. 39.

The jury found petitioner guilty on both the Section 1030 and honest-services wire-fraud counts. Pet. App. 6a. The district court sentenced petitioner to 18 months of imprisonment, to be followed by two years of supervised release. Judgment 2-3.

2. The court of appeals affirmed petitioner's Section 1030 conviction but vacated his conviction for honest-services fraud and remanded for a new trial on that count. Pet. App. 3a, 32a; see *id.* at 1a-32a.

As relevant here, the court of appeals rejected petitioner's contention that insufficient evidence supported

his Section 1030 conviction. Pet. App. 26a-28a. The court observed that petitioner's sufficiency claim amounted to a request that the court overrule its earlier decision in *United States* v. *Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), cert. denied, 563 U.S. 966 (2011), which had explained that an individual can "exceed authorized access[]" to a protected computer when he accesses the computer for a prohibited purpose or use. Pet. App. 26a-27a. And the court found "no question that the record contained enough evidence for a jury to convict" petitioner on the Section 1030 count. *Id.* at 27a-28a. It emphasized that petitioner had "accepted $6,000 and agreed to" perform the requested search; that the GCIC database "is supposed to be used for law-enforcement purposes only"; and that petitioner admitted that he "knew it was 'wrong' to run the tag search." *Id.* at 28a.

SUMMARY OF ARGUMENT

When petitioner used his law-enforcement access to view confidential license-plate records in government databases for personal profit, he intentionally "exceed[ed] authorized access" to obtain protected computer information, in violation of 18 U.S.C. 1030(a)(2)(C). The statute defines "'exceeds authorized access'" to mean "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). That definition unambiguously includes petitioner's forbidden use of his law-enforcement credentials. The statute aims directly at "insider" conduct like petitioner's, and he identifies no textual, historical, or practical basis for excluding such conduct. The concerns of petitioner and his amici about hypothetical liability in commonplace scenarios can be addressed through *other* limiting features of Section 1030

that are not at issue here. Those concerns do not require atextually hollowing out the definition of "exceeds authorized access" to exempt heartland conduct like petitioner's.

A. The only dispute in this case is whether petitioner, when he used his official credentials to search a law-enforcement database in return for cash, obtained computer information that he was "not entitled so to obtain." 18 U.S.C. 1030(e)(6). He unambiguously did.

Someone is "entitled" to do something only when he has been granted a right to do it. And he is "entitled *so*" to do something only when he has been granted a right to do it in a particular manner or circumstance. As a result, the question under Section 1030's "exceeds authorized access" definition is whether petitioner was granted a right to access computer information in the circumstances in which he did. And because he was specifically forbidden from using his access outside his law-enforcement duties, he plainly was "not entitled so" to obtain confidential database information in that circumstance.

Petitioner's contrary construction would render Section 1030(e)(6)'s definition categorically inapplicable to anyone who could identify a *single* circumstance in which he could legitimately obtain computer information—no matter how remote or limited that circumstance might be. But if Congress meant to include only an individual who obtains computer information that he "has no right at all" (Pet. Br. 17) to obtain under any circumstances, then the phrase "entitled *so*" would be unnecessary. Congress could simply have said that a person is prohibited from obtaining computer information that he is "not entitled * * * to obtain." By expressly defining "exceeds authorized access" to encompass a person who

obtains information that he "is not entitled *so* to obtain," 18 U.S.C. 1030(e)(6) (emphasis added), Congress unambiguously covered insiders like petitioner who have some limited authority to access computer information but exceed those limits.

The history confirms that such coverage reflects deliberate congressional design. Petitioner does not dispute that the original version of Section 1030—which applied to using authorized access "for purposes to which such authorization does not extend," 18 U.S.C. 1030(a) (Supp. II 1984)—expressly covered uses of access like his own here. He is therefore forced to assert (Br. 6) that Congress later "cabin[ed]" its coverage of insiders, but the evidence refutes that assertion. Congress's substitution of the "exceeds authorized access" language in 1986 was to "clarify" (1986 House Report 11) (citation omitted) and "simplify" (1986 Senate Report 9) the preexisting law—not to make it a shell of its former self. Indeed, the dramatic limitation that petitioner posits would conflict with Congress's consistent understanding of Section 1030 as applying traditional property-protection principles to computer information. Both common-law and contemporary criminal prohibitions on theft have included takings of property that a defendant was entitled to use for *some* purposes, so long as the taking exceeded the scope of the owner's consent. Section 1030 analogously protects a computer owner from the actions of someone who exceeds the owner's consent to access sensitive computer information.

B. Rather than focusing on the text and history of Section 1030, petitioner (Br. 26-41) and his amici primarily assert that affirming his conviction will lead to a host of undesirable consequences in hypothetical future

cases. But their concerns rest on unwarranted assumptions that courts will necessarily adopt the broadest possible readings of other statutory terms—such as "with authorization," "use," and "intentionally," 18 U.S.C. 1030(a)(2) and (e)(6)—whose application petitioner has not challenged in this case.

In light of those additional limitations, applying the plain statutory text of "not entitled so to obtain" to petitioner's conduct will not endorse hypothetical liability for scenarios involving, *e.g.*, public websites, trivial web-surfing, or unclear conditions on access. If cases involving such scenarios were to arise, the other statutory terms are a more natural textual basis for limiting liability. The absence of any evidence of an actual parade of horribles in any circuit undermines petitioner's suggestion that the only way to avoid one is to carve his own core conduct out of the statute.

Petitioner's invocation of the constitutional-avoidance canon likewise rests on unfounded speculation about how the statute might apply in cases not before the Court. Nothing suggests that the statute, which applies to conduct, is a substantially overbroad restriction of speech or is facially vague.

C. Finally, the rule of lenity does not apply. That rule has force only if, after considering all of the traditional tools of statutory construction, "there remains a grievous ambiguity or uncertainty in the statute, such that the Court must simply guess as to what Congress intended." *United States* v. *Castleman*, 572 U.S. 157, 173 (2014) (citation omitted). Petitioner's hypothetical broad applications of Section 1030 do not create ambiguity in the text, let alone the grievous ambiguity required to trigger the rule of lenity.

ARGUMENT

PETITIONER "EXCEED[ED] AUTHORIZED ACCESS" BY SEARCHING A RESTRICTED LAW-ENFORCEMENT DATABASE IN RETURN FOR MONEY

As a police sergeant, petitioner had the authority to access the GCIC computer system and use that system to obtain confidential computer records from official government databases in the course of his law-enforcement duties. He intentionally "exceed[ed]" that "authorized access," 18 U.S.C. 1030(a)(2)(C), when he searched for and acquired such law-enforcement information for personal financial gain. The text of 18 U.S.C. 1030(a)(2)(C) and (e)(6) unambiguously covers that conduct, and the history and design of the statute illustrate that this sort of "insider" activity lies at the heart of those provisions. Petitioner's characterization of Section 1030 as solely a "hacking" statute, which permits an insider free rein so long as he has *any* access to the computer information, is textually untenable, historically inaccurate, and purposively unsound. The concerns of petitioner and his amici about the statute's theoretical application to various hypothetical scenarios far afield of this case can be (and in some courts have been) addressed through the statute's *other* limitations, which are not at issue here.

A. Petitioner's Forbidden Use Of His Computer Access To Obtain Confidential Database Information "Exceed[ed]" His "Authorized Access"

A person violates Section 1030(a)(2)(C) if he "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains * * * information from any protected computer." 18 U.S.C. 1030(a)(2)(C). As this Court has recognized, Section 1030(a)(2)(C) thus "provides two ways of committing

the crime of improperly accessing a protected computer: (1) obtaining access without authorization; and (2) obtaining access with authorization but then using that access improperly." *Musacchio* v. *United States*, 136 S. Ct. 709, 713 (2016). The latter—"using * * * access improperly," *ibid.*—is precisely what petitioner did here.

1. The statutory definition of "exceeds authorized access" unambiguously covers petitioner's search of a restricted law-enforcement database for personal profit

Congress defined the phrase "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). Petitioner's conduct—intentionally using his authorized access to a computer database to obtain confidential law-enforcement records in the unauthorized circumstance of a private bribe—unambiguously satisfies that definition.

a. Petitioner was not entitled to use access authorized solely for law-enforcement duties to obtain confidential records in return for cash

Under Section 1030(e)(6), a person "exceeds authorized access" if (1) he "access[es] a computer with authorization," (2) he "use[s] such access to obtain or alter information in the computer," and (3) the information that he obtains or alters is information that he "is not entitled so to obtain or alter." 18 U.S.C. 1030(e)(6). Petitioner does not dispute that his conduct satisfies the first two conditions—*i.e.*, that he "access[ed] a computer with authorization" and "use[d] such access to obtain or alter information in the computer," *ibid.*, when

he looked up the license plate in return for cash. See Pet. App. 28a; J.A. 39-40. The substance of petitioner's claim is instead that he was, in fact, "entitled so to obtain" that "information in the computer." See Pet. Br. 17-23. That claim is textually insupportable.

i. A person who "use[s]" his authorized computer access "to obtain or alter information in a computer" is "entitled *so* to obtain or alter" that information, 18 U.S.C. 1030(e)(6) (emphasis added), only when he is authorized to do so under the circumstances. Petitioner indisputably was not.

Someone is "entitled" to do something only when he has been granted a right to do it. See, *e.g.*, *Black's Law Dictionary* 477 (5th ed. 1979) (defining "[e]ntitle" as "to give a right or legal title to," or "[t]o qualify for; to furnish with proper grounds for seeking or claiming") (emphasis omitted); see also *Estate of Cowart* v. *Nicklos Drilling Co.*, 505 U.S. 469, 477 (1992) ("Both in legal and general usage, the normal meaning of entitlement includes a right or benefit for which a person qualifies."). A law that prohibits driving by anyone who is "not entitled to drive," for example, would allow licensed driving and prohibit unlicensed driving.

Someone is "entitled so" to do something only when he has been granted the right to do it in a particular manner or circumstance. See, *e.g.*, *Black's Law Dictionary* 1246 (defining "[s]o" as "[i]n the same manner as has been stated; under this circumstance; in this way, referring to something which is asserted") (emphasis omitted); 15 *The Oxford English Dictionary* 887 (2d ed. 1989) (defining "so" as "[i]n the way or manner described, indicated, or suggested; in that style or fashion"); *Webster's Third New International Dictionary* 2159 (1986) (defining "so" as "in a manner or way that

is indicated or suggested") (emphasis omitted). A law that prohibits driving by anyone who is "not entitled *so* to drive" would allow a 15-year-old with a learner's permit to drive with adult supervision, but prohibit her from driving alone.

The "exceeds authorized access" definition in Section 1030 works similarly. The key question is whether someone who has used his authorized access to obtain or alter computer information—say, a psychiatrist's assistant who uses his own username and password to open a patient's computer records—was "entitled *so*" to do that. If that person uses his credentials to obtain or alter computer information in circumstances in which he is allowed to—say, to look up or enter information relating to patient care—he is "entitled so" to use his access. But if he uses those credentials to obtain or alter computer information in circumstances in which he is not allowed to—say, to obtain psychiatric notes on a famous patient to sell to a tabloid—then he is not "entitled so" to do that. Here, petitioner was specifically and explicitly foreclosed from using his access to a law-enforcement database to look up information for personal gain. He cannot plausibly claim that, when he nevertheless accessed the database in those forbidden circumstances, he was "entitled so" to act.

ii. As petitioner recognizes, a person can "'exceed[] authorized access'" by using his authorized computer access to obtain or alter information in the computer that he "has no right at all" to obtain or alter. Pet. Br. 17 (citation omitted). But if that were the *only* type of conduct that Congress wanted to cover, the word "entitled" alone would have done the job, and the word "so" would be unnecessary. A government contractor who

snoops through computer salary files that he is categorically forbidden ever from examining would be covered by a provision limited to obtaining computer information that he is "not entitled * * * to obtain." By expressly defining "'exceeds authorized access'" to encompass using authorized 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), Congress unambiguously included insiders who have *some* authority to access the computer information, but exceed the limitations of that authority.

It is a "cardinal principle of statutory construction that [courts] must give effect, if possible, to every clause and word of a statute." *Williams* v. *Taylor*, 529 U.S. 362, 404 (2000) (citation and internal quotation marks omitted); see, *e.g.*, *Nielsen* v. *Preap*, 139 S. Ct. 954, 969 (2019) (endorsing "the idea that 'every word and every provision is to be given effect and that none should needlessly be given an interpretation that causes it * * * to have no consequence'") (quoting Antonin Scalia & Bryan A. Garner, *Reading Law: The Interpretation of Legal Texts* 174 (2012)) (brackets omitted); *Loughrin* v. *United States*, 573 U.S. 351, 358 (2014). Application of that principle here necessarily means that the phrase "exceeds authorized access" applies to a computer user like petitioner, who was authorized to access confidential law-enforcement databases in his law-enforcement duties but who instead used that authorized access to obtain law-enforcement information for personal financial gain. See Pet. App. 6a.

iii. That interpretation also coheres with ordinary understandings of what it means to "exceed authorized access"—the defined phrase at issue. Cf. *Bond* v. *United States*, 572 U.S. 844, 861-862 (2014). In common

parlance, a police officer exceeds his authorized access to a law-enforcement database when he locates confidential information in that database to share with criminals. The same is true of a bank employee who rummages through a folder of credit reports, to which she has access for the purpose of approving loan applications, and steals Social Security numbers to sell online. And it is likewise true of a medical assistant who has access to medical records solely at a doctor's request, when he independently peruses the records of a former romantic partner.

In each circumstance, an ordinary speaker of English would comfortably describe the violator as having "exceed[ed] authorized access" to the sensitive computer information. Cf. *Musacchio*, 136 S. Ct. at 713 (describing the phrase as covering "obtaining access with authorization but then using that access improperly"). And the plain language of the statutory definition forecloses a contrary interpretation in the context of Section 1030.

b. Petitioner's conduct is not exempt from Section 1030 simply because he would be allowed to query the database in a different circumstance

Petitioner nevertheless urges the Court to adopt a contrary interpretation, under which an insider would not be covered by Section 1030 as long as he could identify at least *one* circumstance that would entitle him to obtain or alter the computer information, no matter how limited or remote that circumstance might be. On that view, the statute would fail to cover a car-company employee who accesses a customer's real-time GPS data in order to stalk her, simply because he is authorized to access that data when a customer reports a car stolen

or needs roadside assistance. Petitioner offers no plausible textual basis for that view.

i. Petitioner posits (Br. 19) that if Congress meant to cover insiders who are permitted to access information only for certain purposes, it would have included language about accessing a computer "for an unauthorized purpose" or would have defined "exceeds authorized access" to mean "obtaining or altering information 'for an unauthorized purpose.'" As an initial matter, Congress apparently designed the "exceeds authorized access" formulation to capture that very concept. See pp. 26-28, *infra*.

In any event, the current language, unlike petitioner's proposal, makes clear that the statute covers not only those insiders who abuse their authorized access by obtaining information for an unauthorized purpose; it also covers those insiders, such as the medical assistant who needs the doctor's permission to access patient records, who abuse their authorized access by obtaining information in violation of other types of restrictions. Petitioner's proposal for a differently worded provision is no reason to disregard the plain meaning of the text that Congress enacted.

ii. To the extent that petitioner tries to give meaning to Congress's use of the phrase "entitled so," rather than just the word "entitled," he offers an unsound reading that fails to avoid superfluity. Petitioner briefly suggests (Br. 18) that "so" is meant to illustrate that the statute covers someone who lacks the right to obtain or alter information "via computer," but has the right to obtain information "via some other method, such as by calling on the phone or procuring hard copies of records." But the statute would still cover such a person even if it only used the word "entitled." The statute's

coverage is limited to computer information—namely, "information in the computer," where "the computer" is "a computer" that the "accesser" has "accesse[d]." 18 U.S.C. 1030(e)(6). As a result, it cannot apply to information acquired through some other method.

The contractor who snoops through salary files that he is never allowed to examine (see pp. 19-20, *supra*) is "access[ing] a computer with authorization and * * * us[ing] such access to obtain or alter information in the computer"—namely, the computerized salary files—"that [he] is not entitled * * * to obtain or alter," 18 U.S.C. 1030(e)(6), irrespective of whether he could learn about salaries by asking someone on the phone. Information conveyed over the phone is not "information in the computer" merely because a computer contains the same information. Cf. *Kansas* v. *Garcia*, 140 S. Ct. 791, 802 (2020) (explaining that "an item of information * * * may be 'contained in' many different places, and it is not customary to say that a person uses information that is contained in a particular source unless the person makes use of that source"). Where Section 1030 refers in the abstract to "information" that was derived from or is separately stored in a computer, it uses a modifier other than "in the computer," or no modifier at all. See 18 U.S.C. 1030(a)(1), (a)(2)(A)-(C), (a)(5)(A), (a)(6)(B), (c)(2)(B)(iii), (e)(5), and (e)(8). Indeed, the modifier "in the computer" appears only in the definition of "exceeds authorized access," where it is used in the context of someone "access[ing] a computer." Because the definition's language already focuses exclusively on computerized access to computer data, the word "so" would be superfluous if all it did was to redundantly distinguish the brick-and-mortar world.

Petitioner's interpretation also makes no sense in "the broader context of the statute as a whole." *Robinson* v. *Shell Oil Co.*, 519 U.S. 337, 341 (1997). Under petitioner's theory, Congress specifically sought to prohibit the use of a computer to access information that a person *could* obtain through non-computerized means, yet simultaneously failed to prohibit the use of a computer to access confidential information in circumstances where the person is *completely* prohibited from obtaining it. That cannot be squared with Section 1030's plain focus on safeguarding sensitive computer information, such as national-security information, financial records, and information that can be used to commit fraud—all of which are protected from insiders who "exceed[] authorized access." 18 U.S.C. 1030(a)(1), (2)(A), and (4). A malicious insider who has been given strictly circumscribed access to such sensitive information can compromise the security of that information just as easily—if not more easily—than someone who lacks any authorized access to the same information. An insider with highly limited authority to access computerized national-security information, for example, surely "exceeds authorized access" to that information if he obtains it for the unauthorized purpose of selling its contents to a foreign government. See 18 U.S.C. 1030(a)(1).

iii. Petitioner cannot support his atextual and anomalous constriction of the statute by arguing (Br. 26) that conduct like his is already prohibited by other federal criminal statutes. The principal federal theft statute he identifies, 18 U.S.C. 1832, is limited to trade secrets and thus would not cover the theft of other sensitive and non-public information that does not qualify as a trade secret, such as confidential financial information or

criminal-history records. See 18 U.S.C. 1839(3) (defining "trade secret"); see also 142 Cong. Rec. 23,784 (1996) (statement of Sen. Leahy) (explaining that Section 1030 imposes criminal penalties on "[g]overnment employees who abuse their computer access privileges by snooping through confidential tax returns, or selling confidential criminal history information"). Conversely, Section 1030 does not encompass a theft of trade secrets that occurs without improper computer access. And Congress evidently viewed the two prohibitions as complementary because it enacted the trade-secrets statute and Section 1030(a)(2)(C) in the same 1996 Act. See Economic Espionage Act of 1996, §§ 101(a), 201(1)(B)(ii), 110 Stat. 3488-3491, 3492.

The other federal statutes that petitioner identifies likewise do not encompass all of the computer information protected by Section 1030(a)(2) and, notably, would not cover petitioner's own conduct. See 17 U.S.C. 506(a)(1) (copyright infringement); 42 U.S.C. 1320d-6(a) ("individually identifiable health information"). In any event, "substantial" "overlap * * * is not uncommon in criminal statutes." *Loughrin*, 573 U.S. at 358 n.4. And any overlap external to Section 1030 is far less salient than the textual superfluity within Section 1030 itself that petitioner's crabbed interpretation would create.

2. The statutory and legislative history confirm that Section 1030 covers petitioner's conduct

"[W]here, as here, the words of a statute are unambiguous, the judicial inquiry is complete." *Babb* v. *Wilkie*, 140 S. Ct. 1168, 1177 (2020) (brackets, citation, and internal quotation marks omitted). Because only one interpretation gives meaning to every word of the definition of "exceeds authorized access," the statutory text alone forecloses petitioner's contrary reading.

Nevertheless, the genesis and evolution of Section 1030 confirm that Congress understood and intended that a person "exceeds authorized access" by using his authorized computer access to obtain computer information in an unauthorized manner or circumstance.

a. Section 1030 has always been designed to cover insider misconduct like petitioner's

i. Since its initial enactment in 1984, Section 1030 has recognized two forms of improper computer access: access by outsiders acting "without authorization" and access by insiders who abuse their authorized access. 18 U.S.C. 1030(a) (Supp. II 1984). The original version covered conduct that could be committed by someone who knowingly accessed a computer without authorization, "or having accessed a computer with authorization, use[d] the opportunity such access provides for purposes to which such authorization does not extend." *Ibid.* As petitioner acknowledges (Br. 20), the statute thus unambiguously applied to an insider who—like petitioner—uses his authorized computer access to obtain information in an unauthorized circumstance, even though he might be permitted to obtain the same information in other circumstances.

Petitioner's acknowledgment of that point belies his contention that Congress enacted Section 1030 solely out of concern with so-called "'hackers'" who "exploit[] vulnerabilities in computer networking to access information stored in restricted computer files." Br. 23 (citation omitted). Instead, the plain text of the 1984 version of the statute imposed the same criminal penalties on both insiders and outsiders, so long as they improperly accessed computers and thereby obtained sensitive information, such as national-security information, 18 U.S.C. 1030(a)(1) (Supp. II 1984), or financial records

or consumer files, 18 U.S.C 1030(a)(2) (Supp. II 1984). The gravamen of those offenses was breaching the confidentiality of sensitive computer data, whether through "hacking" *or* insider misappropriation. Indeed, the 1984 House Report described "the advent of the activities of so-called 'hackers'" simply as a "[c]ompounding" factor of the more general problem of widespread losses from "computer crime." 1984 House Report 9-10. And the report accordingly emphasized that, with respect to covered computer records, the proposed legislation "would make it a criminal offense for anyone who has been authorized to use a computer to access it knowing that the access is for a purpose not contemplated by the authorization." *Id.* at 21; see *ibid.* (distinguishing "computer access that is for a legitimate business purpose").

ii. Because petitioner does not dispute that his conduct would have satisfied the improper-access element under the original version of Section 1030, his theory must necessarily be that subsequent amendments to Section 1030 withdrew or contracted the statute's coverage of insiders. The evidence, however, demonstrates the opposite. Congress has repeatedly expanded the statute's scope to cover even more insider conduct.

The 1986 amendments to Section 1030 substituted the phrase "exceeds authorized access" for the 1984 statute's longer description of improper computer access by an authorized insider. Computer Fraud and Abuse Act of 1986, § 2(c), 100 Stat. 1213; see 18 U.S.C. 1030(a) (Supp. II 1984). The accompanying Senate and House Reports both explained that the change did not narrow the statute's coverage. The Senate Report observed that "the phrase 'exceeds authorized access'" replaced "the more cumbersome phrase" in the 1984 version and that the Senate Judiciary Committee "intends

this change to simplify the language." 1986 Senate Report 9 (citation omitted). Similarly, the House Report observed that "[t]he purpose of this change is merely to clarify the language in existing law." 1986 House Report 11. Nothing suggests that any legislators thought the substitution would "cabin[]" (Pet. Br. 6) the scope of Section 1030.

Where Congress did, in fact, narrow the statute's coverage through the 1986 amendments, it did so deliberately and unambiguously. First, the amendments raised Section 1030(a)(2)'s mens rea requirement from "knowingly" to "intentionally." Computer Fraud and Abuse Act of 1986, § 2(a)(1), 100 Stat. 1213. The accompanying Senate and House Reports discussed that change at length. See 1986 Senate Report 5-6; 1986 House Report 9-10. Second, Congress replaced the original provision covering government computers with a new one that did not apply to insiders. § 2(b), 100 Stat. 1213. The Senate Report highlighted that aspect of the new provision, see 1986 Senate Report 8, and included "additional views" from Senators Mathias and Leahy about the government-specific concerns (relating to disclosures under the Freedom of Information Act) that supported excluding insiders from that provision. *Id.* at 20 (capitalization and emphasis omitted). But other provisions, old and new, included the "exceeds authorized access" language, and thus did cover insiders. § 2(c), 100 Stat. 1213; see *Russello* v. *United States*, 464 U.S. 16, 23 (1983) ("[I]t is generally presumed that Congress act[ed] intentionally and purposely in * * * disparate inclusion or exclusion.") (citation omitted).

The enactment of the Economic Espionage Act of 1996 similarly illustrated Congress's understanding that a person "exceeds authorized access" when he uses

his authorized computer access to obtain or alter information in an unauthorized manner or circumstance. Partly reversing course from ten years earlier, that Act added a provision applicable to government computers that encompassed not only access "without authorization," but also "exceed[ing] authorized access." 18 U.S.C. 1030(a)(2)(A) (Supp. II 1996); see § 201(1)(B)(ii), 110 Stat. 3492. The 1996 Senate Report specifically faulted the prior version of Section 1030 for failing to cover "Government employees who abuse their computer access privileges to obtain Government information that may be sensitive and confidential," and explained that Congress was closing that "gap." 1996 Senate Report 4. And right alongside the new government-computer provision, Congress enacted the new protection for "protected computer[s]" that petitioner was convicted of violating here, which employed the very same insider-covering language—"exceeds authorized access." 18 U.S.C. 1030(a)(2)(C) (Supp. II 1996); see § 201(1)(B)(ii), 110 Stat. 3492.

The comments of Senator Leahy, who co-sponsored the amendments, are particularly telling. He explained that the amended law would impose criminal penalties on "[g]overnment employees who abuse their computer access privileges by snooping through confidential tax returns, or selling confidential criminal history information" from the NCIC. 142 Cong. Rec. at 23,784. Senator Leahy observed that a recent General Accounting Office report had informed Congress that "individuals with authorized access" to the NCIC had abused that access, either by acquiring information to sell or by checking the criminal records of friends and family, and that "most abusers of NCIC were not criminally prosecuted." *Ibid.* Senator Leahy explained that the 1996

amendments "would criminalize these activities by amending the privacy protection provision in section 1030(a)(2)." *Ibid.*; see 142 Cong. Rec. 27,119 (1996) (statement of Sen. Leahy) (similar). Although "the views of a single legislator, even a bill's sponsor, are not controlling," *Mims* v. *Arrow Fin. Servs., LLC*, 565 U.S. 368, 385 (2012), Senator Leahy's evident understanding that the "exceeds authorized access" language would apply to conduct like petitioner's accords with the text, the purpose, and the rest of the statutory and legislative history of Section 1030.

b. Section 1030 applies traditional property-protection principles—which would cover insider misappropriation—to the electronic realm

The history also makes clear that Congress has consistently understood Section 1030 not solely as an anti-hacking statute, but as a statute that protects computer information as property. And petitioner's misappropriation of sensitive law-enforcement data would violate analogous protections for tangible property.

i. Congress first enacted Section 1030 because it considered existing criminal laws "ineffective" for addressing "computer abuse," in part because "much of the property involved does not fit well into categories of property subject to abuse or theft." 1984 House Report 9. The 1984 House Report found it "obvious that traditional theft/larceny statutes are not the proper vehicle to control the spate of computer abuse and computer assisted crimes." *Ibid.* The 1986 Senate Report accordingly described Section 1030 as an effort "to affirm the government's recognition of computerized information as property." 1986 Senate Report 14.

The 1986 Senate Report recognized that, because someone could deprive a computer owner of control

over information but leave the owner with a copy of the information itself, "[c]omputer technology simply does not fit some of the older, more traditional legal approaches to theft or abuse of property"—a disconnect that required law-enforcement officers to attempt to fit "'the square peg of computer fraud into the round hole of theft, embezzlement or even the illegal conversion of trade secrets.'" 1986 Senate Report 13-14 (citation omitted); see 1986 House Report 5 ("Under these circumstances, traditional theft or larceny statutes are difficult to apply."). It accordingly explained that Section 1030 was designed to impose penalties on all criminals who "use[] computers to steal, to defraud, and to abuse the property of others." 1986 Senate Report 2. And the 1986 House and Senate Reports both expressly described Section 1030's prohibition against improper computer access—including "exceed[ing] authorized access"—to further an intended fraud, 18 U.S.C. 1030(a)(4) (Supp. IV 1986), as "designed to penalize thefts of property via computer that occur as part of a scheme to defraud." 1986 Senate Report 9; see 1986 House Report 11.

The history of the 1996 amendments demonstrates that the enacting Congress had a similar understanding of the new Section 1030(a)(2)(C)—the prohibition on improperly accessing a "protected computer" that petitioner violated here—as applying traditional property principles to computer information. The 1996 Senate Report described the new provision as "intended to protect against the interstate or foreign theft of information by computer," thereby "ensur[ing] that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way [as] theft of physical items." 1996 Senate Report 7. And it explained

that "proposed subsection 1030(a)(2)(C) addresses gaps in 18 U.S.C. 2314 (interstate transportation of stolen property)." *Id.* at 13.

ii. Traditional criminal prohibitions on property theft cover not only takings by people with no rights at all to the property, but also takings by people who are exceeding their limited property rights—akin to insiders like petitioner. The common law defined theft as a "taking" of property that occurs without "the consent of the owner." 4 William Blackstone, *Commentaries on the Laws of England* 230 (1769) (emphasis omitted). Accordingly, a person committed a felony if he "embezzl[ed]" goods that the owner entrusted to his "use" or to his "care and oversight." *Id.* at 231. Examples included a butler who stole the household's silver, a shepherd who stole sheep in his care, and a guest who "rob[bed] his inn or tavern of a piece of plate" that he was allowed to use for a meal. *Ibid.* And conduct of that sort would remain a crime, although a misdemeanor, even if the defendant intended only to borrow the property without permission, rather than to keep it permanently. See *id.* at 232. Such a misdemeanor would occur, for example, if "a servant takes his master's horse, without his knowledge, and brings him home again." *Ibid.*

Modern criminal law continues to define "[t]heft" as the "taking of property without the owner's consent," including by "[o]btaining or exerting unauthorized control over property." *Black's Law Dictionary* 1324 (emphasis omitted). As at common law, modern criminal law specifically recognizes that theft may "be committed by an agent, bailee, trustee, fiduciary, or other person entrusted with possession of the property." Model Penal Code, Pt. II, § 223.2 cmt. 1, at 163 (1980). Such a

theft occurs "at the moment the custodian of property begins to use it in a manner beyond his authority." *Id.* § 223.2 cmt. 2, at 166. A person therefore commits a theft by exercising unlawful control over the property of another "whenever consent or authority is exceeded." *Id.* § 223.2 cmt. 4, at 168; see *Gonzales* v. *Duenas-Alvarez*, 549 U.S. 183, 189 (2007) (defining generic theft to include the "taking of property or an exercise of control over property without consent with the criminal intent to deprive the owner of rights and benefits of ownership, even if such deprivation is less than total or permanent") (citation omitted).

iii. Congress's property-law paradigm reinforces even further that the "exceeds authorized access" offenses in Section 1030 apply to insider activity like petitioner's. Section 1030 sets forth a series of criminal offenses that apply many of the traditional principles of property law, including the scope of authorization, to computer information. The traditional property crimes like theft and trespass encompass someone who uses property in ways that the owner has not authorized, and the "exceeds authorized access" offenses in Section 1030 should be understood the same way. See 18 U.S.C. 1030(a)(1), (2), and (4). Just as the authorization to use or obtain property in some circumstances does not foreclose a theft prosecution when the property is taken in other circumstances, an insider's authorization to obtain or alter sensitive computer information in some circumstances should not foreclose a Section 1030 prosecution when the insider obtains or alters the information in other circumstances.

Petitioner fears that, in some such cases, determining the scope of an insider's authorization may require examination of "[e]mployer-employee and company-

consumer relationships." Pet. Br. 25 (citation omitted). But an inquiry into the scope of consent is familiar to traditional criminal law, as when an employee takes a company-assigned car on a personal vacation or a hotel guest takes the robe from his room. The potential need to examine the scope of consent is no reason to artificially narrow the conduct covered by Section 1030's text. To the contrary, it places Section 1030 on equal footing with traditional criminal property laws that seek to vindicate property abuses committed without the property owner's consent.

B. Petitioner's Policy And Constitutional Arguments Are Misplaced

Petitioner devotes the substantial majority of his argument (Br. 26-41)—and his amici devote nearly all of theirs—not to text or history, but to the assertion of policy and constitutional concerns with Section 1030. Those assertions do not provide any sound basis to overturn petitioner's conviction for accessing a law-enforcement database for money. The relevant part of the statutory definition of "exceeds authorized access" is unambiguous, and the genesis and evolution of that definition confirm that Congress intended the phrase to encompass conduct like petitioner's. Petitioner's assertions (Br. 26-35) about the breadth of Section 1030 rest on unwarranted assumptions about how courts will interpret *additional* statutory limitations on Section 1030 liability that are not at issue in this case. And he has failed to show (Br. 36-41) that the plain meaning of the language that *is* at issue presents any constitutional problems.

1. Affirming petitioner's conviction would not make routine or innocuous computer use a federal crime

The focus of petitioner and his amici is not on applying the statutory text, and Congress's manifest design, to petitioner's own conduct, but instead on a parade of horribles. They assert that affirming petitioner's conviction would "extend the statute's coverage to 'whole categories of otherwise innocuous behavior'" and would subject "most everyone who uses a computer" to federal misdemeanor liability. Pet. Br. 26-27 (citation omitted). But petitioner and his amici's myriad hypothetical scenarios depend on the assumption that courts will adopt the most expansive possible view of several *other* terms in Section 1030, resulting in criminal liability in improbable circumstances. The implication is that this case, which involves conduct at the core of Section 1030, presents the only guardrail against those hypothetical future decisions. Petitioner is wrong to suggest that reversal of his conviction is necessary to forestall convictions in other, less serious scenarios. If the Court applies the plain statutory text to affirm petitioner's conviction, lower courts may well decide that most or all of the proffered hypotheticals are outside the scope of Section 1030.

a. The policy concerns of petitioner and his amici are best addressed through separate statutory limitations that are not at issue here

As previously discussed (see pp. 17-18, *supra*), the dispute in this case is limited to only *one* of the conditions in the "exceeds authorized access" definition. Petitioner disputes only whether the information that he was bribed to obtain from the GCIC database was information that petitioner was "not entitled so to obtain."

18 U.S.C. 1030(e)(6). He does not dispute that his conduct satisfied the other conditions for exceeding authorized access—namely, that he accessed the GCIC system "with authorization" and that he "use[d] such access to obtain or alter information in the computer." *Ibid.*; see Pet. Br. 17-23. Nor has he challenged the jury's determination that he "intentionally" used his authorized access to the GCIC system improperly. 18 U.S.C. 1030(a)(2)(C). Those additional limitations, which are not at issue here, are a more natural home for addressing concerns that might arise if any of the hypothetical scenarios posited by petitioner and his amici were actually to come to court.

i. First, while petitioner has not disputed that his access to a highly restricted law-enforcement database was "with authorization," a user of a more public system or website could. Here, the trial evidence established that the GCIC system was password-protected and not available to the public, and that petitioner was required to undergo training on the proper uses of the system before he received the credentials that enabled him to access it. J.A. 11-14, 19-20, 24-25. But no similar circumstance exists in petitioner's hypotheticals about, *e.g.*, "inflating one's height on a dating website" (Br. 2), "posting an item on the wrong category on Craigslist" (Br. 15), or violating the terms of service of Zoom or eBay (Br. 28-29).

The concept of "authorization" does not necessarily apply to every access of a computer system. Although "the word 'authorize' sometimes means simply 'to permit,' it ordinarily denotes affirmative enabling action." *County of Washington* v. *Gunther*, 452 U.S. 161, 169 (1981); see, *e.g.*, *Black's Law Dictionary* 165 (11th ed. 2019) (defining "authorization" as "[o]fficial permission

to do something; sanction or warrant") (emphasis omitted); 1 *The Oxford English Dictionary* 798 (defining "authorization" as "[t]he conferment of legality; formal warrant, or sanction") (emphasis omitted). Many computer systems do not condition access on such "affirmative enabling action." When a system's owner does not establish meaningful restrictions on who has access, the authorization-based terms necessary to trigger Section 1030 ("with authorization" and "without authorization") may not logically apply.

For example, the Ninth Circuit has rejected the application of Section 1030 to website information generally available on the Internet, reasoning that Section 1030 "is premised on a distinction between information presumptively accessible to the general public" (which is not subject to Section 1030's access provisions) and "information for which authorization is generally required" (which is). *hiQ Labs, Inc.* v. *LinkedIn Corp.*, 938 F.3d 985, 1002 (2019), petition for cert. pending, No. 19-1116 (filed Mar. 9, 2020); see *id.* at 1000-1004. Other courts have adopted similar approaches. See *Sandvig* v. *Barr*, No. 16-1368, 2020 WL 1494065, at *8-*10 (D.D.C. Mar. 27, 2020), appeal pending, No. 20-5153 (D.C. Cir. filed May 28, 2020); *Cvent, Inc.* v. *Eventbrite, Inc.*, 739 F. Supp. 2d 927, 932-934 (E.D. Va. 2010). And although the Ninth Circuit suggested that a website that requires visitors to sign up for an account and perhaps pay a fee in order to gain access to some information might be a system that requires "authorization," see *hiQ Labs*, 938 F.3d at 1002, that need not be so. Offering access to the public on general terms, without imposing meaningful restrictions that would generate true "insiders," would not necessarily be the sort of "affirmative enabling action," *County of Washington*, 452 U.S.

169, that would constitute "authorization" under Section 1030.

ii. Second, while petitioner has not disputed that he "use[d]" his authorized access to obtain law-enforcement information, someone whose authorized access was incidental to obtaining information could. Here, the trial evidence established that petitioner took advantage of his specialized access to the GCIC computer system to view confidential law-enforcement information. See Pet. App. 6a; J.A. 26-28. But an employee who, say, attends to personal matters on the Internet while logged into a work-only computer, has not necessarily "use[d]" her *authorized access*, 18 U.S.C. 1030(e)(6), to obtain the Internet information, which she could readily obtain in many other ways.

Section 1030(e)(6) requires that someone "access a computer with authorization" and then "*use such access* to obtain or alter information in the computer." 18 U.S.C. 1030(e)(6) (emphasis added). In context, the term "use" is best understood to require that the violator's authorized access be instrumental to acquiring the information—not merely the technical means by which he views such information. Although "use" often has a broader definition, it may also be limited to circumstances where the mechanism employed is particularly efficacious. See *Webster's Third New International Dictionary* 2523-2524 (defining "use" to mean "to carry out a purpose or action by means of: make instrumental to an end or process: apply to advantage"); see also 19 *The Oxford English Dictionary* 353 (defining "use" to mean "[t]o make use of (some immaterial thing) as a means or instrument") (emphasis omitted). That is the case when someone like petitioner relies on his username and password to obtain information from the restricted database

where information is stored. But it is not the case for simply checking sports scores or sending e-mail at work, see, *e.g.*, Pet. Br. 2, 15, 28, which could be done from numerous Internet-enabled devices, including a personal smartphone. Adopting that meaning of "use," rather than an untenable interpretation of "entitled so," would thus be the better way to address petitioner's concerns.

iii. Third, while petitioner has not contested that he "intentionally" exceeded his authorized access, someone without the same clear understanding of the limits of her authority could. Here, the trial evidence established that petitioner had been trained on the permissible uses of his access to the GCIC system and that he knew that accepting money to run a license plate for Albo was "wrong." Pet. App. 6a, 28a. But a person who violates a computer-use policy that she is "only dimly aware of," or has not understood, Pet. Br. 29 (citation omitted), would not have the requisite mens rea.

Every "exceeds authorized access" offense in Section 1030 requires proof that the computer user at least knew and understood that she was using her authorized access to obtain or alter information that she was not entitled so to obtain or alter. See 18 U.S.C. 1030(a)(1), (2), and (4); cf. 18 U.S.C. 1030(a)(7). And the "intent[]" mens rea requirement for offenses like petitioner's further ensures that the provision covers only "intentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones." 1986 Senate Report 5. A person thus may be prosecuted for such an offense only if her "conduct evinces a clear intent to enter, without proper authorization, computer files or data belonging to another." *Id.* at 6. That not only protects people with inadequate notice of—or who subjectively fail to

appreciate—the relevant restrictions, but also someone subject to vague or unclear restrictions that she merely worries might cover her conduct. See, *e.g.*, Karahalios et al. Amici Br. 14-17, 22; Technology Companies Amici Br. 12-13.

b. The Court should not hollow Section 1030 by excising core unlawful conduct like petitioner's

Petitioner's conduct here—intentionally abusing his individualized access privilege to misappropriate confidential computer data—is precisely the type of conduct at which Section 1030 is directed. The Court need not, and should not, accept his invitation to artificially constrict the one statutory requirement that he has put at issue—and thereby excise heartland cases like his—in order to guard against hypothetically broad applications of other statutory terms. That is especially true because the lower courts have had few occasions to grapple with those other terms, as neither the government nor private litigants have created the parade of horribles that petitioner and his amici envision. Possibly due in part to the high likelihood that courts would reject such cases for the reasons detailed above, the hypotheticals remain hypothetical, even though few circuits have embraced petitioner's atextual limiting construction of the language at issue here.

i. Historically, prosecutions against defendants who "exceed[] authorized access" have focused on the core conduct that Congress intended Section 1030 to cover. See, *e.g.*, *United States* v. *Valle*, 807 F.3d 508, 512-513 (2d Cir. 2015) (police officer who searched law-enforcement databases for information about a woman he had discussed kidnapping); *United States* v. *Teague*, 646 F.3d 1119, 1121-1123 (8th Cir. 2011) (Department of

Education contractor who accessed student-loan records of then-Presidential candidate Barack Obama); *United States* v. *John*, 597 F.3d 263 (5th Cir. 2010) (Citigroup account manager who accessed confidential customer records for purpose of making fraudulent charges), cert. denied, 568 U.S. 1163 (2013).

Petitioner identifies (Br. 32) only three actual prosecutions, none more recent than 2012, to support his claim that the government's interpretation of "exceeds authorized access" would invite prosecutions of "individuals who allegedly violated companies' terms of service agreements." But even those three cases do not establish that the government could or would successfully prosecute such conduct as an "exceeds authorized access" offense. In one, the government filed a superseding indictment that dropped the "exceeds authorized access" charges. See D. Ct. Doc. 53, at 12-13, *United States* v. *Swartz*, No. 11-cr-10260 (D. Mass. Sept. 12, 2012). In another, "[t]he indictment allege[d] a number of actions taken by defendants to defeat code-based security restrictions," and the resulting Section 1030 charges thus "involve[d] allegations of breaches of both contract- and code-based restrictions." *United States* v. *Lowson*, No. 10-114, 2010 WL 9552416, at *5-*6 (D.N.J. Oct. 12, 2010). And the third, *United States* v. *Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), is an outlier prosecution that a district court rejected. Although a jury found the defendant guilty of a misdemeanor based on evidence that she had conspired to create a profile for a fictitious teenager on the MySpace social network, in violation of MySpace's terms of service, *id.* at 452-453, 461, the district court granted a post-trial judgment of acquittal, *id.* at 468. The government did not

appeal that decision. See D. Ct. Doc. 165, *United States* v. *Drew*, No. 08-cr-582 (C.D. Cal. Dec. 7, 2009).

ii. Since the failed *Drew* prosecution, the Department of Justice has adopted a written computer-crime charging policy, in part to ensure that government attorneys apply Section 1030 "consistently." Memorandum from U.S. Att'y Gen. to U.S. Att'ys & Assistant Att'y Gens. for the Criminal & Nat'l Sec. Divs., *Intake and Charging Policy for Computer Crime Matters* 1 (Sept. 11, 2014), https://www.justice.gov/criminal-ccips/file/904941/download. Among other things, the policy cautions that "federal prosecution may not be warranted" if a defendant "exceeded authorized access solely by violating an access restriction contained in a contractual agreement or term of service with an Internet service provider." *Id.* at 5. Although petitioner faults (Br. 33) the government for not specifically disavowing his hypothetical prosecutions, he does not identify any real-world prosecution since issuance of the policy that involves violations of public websites' terms of service or employer restrictions on visiting publicly available websites.

Petitioner also suggests (Br. 35) that private civil suits could involve such conduct. But outside of specific statutory categories unlikely to apply to innocuous hypothetical conduct, Section 1030(g) authorizes civil suits only in cases involving losses of at least $5000. 18 U.S.C. 1030(g); see 18 U.S.C. 1030(c)(4)(A)(i)(I)-(V). And petitioner's one example of a civil suit involving improper Internet access at work was dismissed because the employer did not allege "that the [employee] accessed any of the [employer's] information (as distinguished from her personal email and facebook pages, to which she was entitled after business hours)." *Lee* v. *PMSI, Inc.*,

No. 10-cv-2904, 2011 WL 1742028, at *1 (M.D. Fla. May 6, 2011).

Although this Court "cannot construe a criminal statute on the assumption that the Government will use it responsibly," *Marinello* v. *United States*, 138 S. Ct. 1101, 1109 (2018) (citation and internal quotation marks omitted), neither should it adopt an atextual reading of the phrase "not entitled so to obtain or alter," 18 U.S.C. 1030(e)(6), based on unfounded conjecture about the inception or outcome of hypothetical litigation. To date, only three courts of appeals have adopted petitioner's atextual interpretation of "exceeds authorized access"—all relatively recently—yet petitioner and his amici have not identified even a single decision that has entered or affirmed a criminal or civil judgment under Section 1030 based on the kind of innocuous and routine computer use described in their hypotheticals. The evidence thus undermines petitioner's assertion that affirming his conviction will lead to a deluge of criminal prosecutions or civil suits involving such conduct.

iii. At bottom, petitioner's complaint that applying the plain meaning of the statutory language would lead to undesirable policy consequences is an impermissible effort to judicially amend Section 1030. Petitioner suggests (Br. 16) that because Congress enacted the definition of "exceeds authorized access" before the advent of Internet search engines and websites, this Court should narrow the statute to prompt a congressional examination of whether Section 1030 requires further "recalibration" in light of technological and societal changes. But it is not the proper role of the judiciary to disregard plain meaning in order to ask Congress if it really meant what it said. See *Connecticut Nat'l Bank* v. *Germain*, 503 U.S. 249, 253-254 (1992) ("[C]ourts

must presume that a legislature says in a statute what it means and means in a statute what it says there."). Nor is it the Court's role "to rewrite the statute so that it covers only what we think is necessary to achieve what we think Congress really intended." *Little Sisters of the Poor Saints Peter & Paul Home* v. *Pennsylvania*, 140 S. Ct. 2367, 2381 (2020) (citation omitted).

Accordingly, "[i]f policy considerations suggest that the current scheme should be altered, Congress must be the one to do it." *Intel Corp. Inv. Policy Comm.* v. *Sulyma*, 140 S. Ct. 768, 778 (2020). Judicial intervention aimed at getting Congress's attention is not appropriate—or necessary here. See S. 1196, 113th Cong., 1st Sess. (2013) (unadopted bill that would limit Section 1030(e)(6) to circumventing technological restrictions); H.R. 2454, 113th Cong., 1st Sess. (2013) (same); S. 1030, 114th Cong., 1st Sess. (2015) (same); H.R. 1918, 114th Cong., 1st Sess. (2015) (same).

2. Petitioner's constitutional concerns are unfounded

Relying on the same sorts of hypotheticals that undergird his policy arguments, petitioner contends (Br. 36-40) that the canon of constitutional avoidance militates in favor of his narrow reading of "exceeds authorized access." Although he has never brought a constitutional challenge to the application of Section 1030, cf. *United States* v. *Sineneng-Smith*, 140 S. Ct. 1575 (2020), petitioner now theorizes (Br. 36) "both First Amendment and void-for vagueness problems" with construing Section 1030 to apply here. But the "canon of constitutional avoidance comes into play only when, after the application of ordinary textual analysis, the statute is found to be susceptible of more than one construction," at which point it supplies "a means of choosing between them." *Clark* v. *Martinez*, 543 U.S. 371,

385 (2005) (emphasis omitted). For all of the reasons explained above, petitioner's construction of "exceeds authorized access" is at odds with Section 1030's text, history, and purpose. As a result, "the meaning of the statute is sufficiently clear that [the Court] need not indulge [petitioner's] cursory nod to constitutional avoidance concerns." *United States* v. *Castleman*, 572 U.S. 157, 173 (2014). In any event, even if the text were susceptible to multiple constructions, petitioner's constitutional concerns are unfounded.

a. A statute is impermissibly overbroad under the First Amendment only if it prohibits "a substantial amount of protected speech." *United States* v. *Williams*, 553 U.S. 285, 292 (2008). To ensure that invalidation for overbreadth is not "casually employed," *Los Angeles Police Dep't* v. *United Reporting Publ'g Corp.*, 528 U.S. 32, 39 (1999), this Court has "vigorously enforced the requirement that a statute's overbreadth be *substantial*, not only in an absolute sense, but also relative to the statute's plainly legitimate sweep," *Williams*, 553 U.S. at 292. And laws that are "not specifically addressed to speech or to conduct necessarily associated with speech (such as picketing or demonstrating)" are far less likely to present such a danger. *Virginia* v. *Hicks*, 539 U.S. 113, 124 (2003); see *ibid.* (observing that "an overbreadth challenge" to such laws will "[r]arely, if ever, * * * succeed").

Section 1030's "exceeds authorized access" offenses proscribe conduct, not speech, and thus present no apparent First Amendment concerns. Nevertheless, petitioner contends (Br. 37) that construing Section 1030 to cover his conduct would make it a crime for other computer users to "conceal their identities online, in violation of websites' terms of service," which in turn could

chill those users' online "expression and consumption of speech." Petitioner further contends (Br. 37 n.7) that, in particular, construing Section 1030 to cover journalists' collection of data from public websites would "threaten[] the freedom of the press." As explained, however, affirming petitioner's conviction would not establish that Section 1030 actually criminalizes either category of conduct. See pp. 35-40, *supra*; see also *Members of the City Council* v. *Taxpayers for Vincent*, 466 U.S. 789, 801 (1984) (requiring overbreadth claimant to show "a realistic danger that the statute itself will significantly compromise recognized First Amendment protections"). And even if those hypotheticals both fell within the scope of Section 1030 and presented legitimate First Amendment concerns, they would amount to at most a small fraction of the conduct covered by the statute.

b. Petitioner's invocation of due-process vagueness principles is similarly misplaced. The Due Process Clause requires that a criminal statute be sufficiently clear to give "the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly." *Village of Hoffman Estates* v. *The Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 498 (1982) (citation omitted). The "touchstone" of that inquiry "is whether the statute, either standing alone or as construed, made it reasonably clear at the relevant time that the defendant's conduct was criminal." *United States* v. *Lanier*, 520 U.S. 259, 267 (1997). Here, the ordinary meaning of the language of Section 1030(a)(2)(C) and the definition of "exceeds authorized access" unambiguously encompassed petitioner's use of his authorized access to the GCIC system to obtain confidential law-enforcement records for personal financial

gain. See pp. 17-25, *supra*. And a party "who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others." *Holder* v. *Humanitarian Law Project*, 561 U.S. 1, 20 (2010) (citation omitted).

To the extent that the application of the statute might be less clear in certain other cases, this Court has definitively rejected the proposition that "the mere fact that close cases can be envisioned renders a statute vague." *Williams*, 553 U.S. at 305; see *Humanitarian Law Project*, 561 U.S. at 21. In addition, under this Court's precedents, "a scienter requirement in a statute 'alleviates vagueness concerns,' 'narrows the scope of its prohibition, and limits prosecutorial discretion.'" *McFadden* v. *United States*, 576 U.S. 186, 197 (2015) (brackets and citation omitted); see *Humanitarian Law Project*, 561 U.S. at 21. Here, every "exceeds authorized access" offense in Section 1030 requires, at a minimum, that the defendant knowingly exceed authorized access. See 18 U.S.C. 1030(a)(1) ("knowingly"); 18 U.S.C. 1030(a)(2) ("intentionally"); 18 U.S.C. 1030(a)(4) ("knowingly and with intent to defraud"). The statute thus imposes criminal penalties only on computer users who understand that they are acting outside the scope of their authorized access.

Petitioner's real complaint is that, in his view, the government's construction of "exceeds authorized access" would render Section 1030 so broad that many people will violate the statute, which petitioner believes would give prosecutors "free rein to prosecute virtually anyone" they dislike. Pet Br. 38. Again, petitioner lacks a substantial basis for his implicit attribution of far-reaching breadth to other provisions of Section 1030 that are not at issue here. See pp. 35-40, *supra*. But

even if the statute is broader than he thinks it should be, he cannot show that it "fails to give ordinary people fair notice of the conduct it punishes, or [is] so standardless that it invites arbitrary enforcement." *Beckles* v. *United States*, 137 S. Ct. 886, 892 (2017) (citation omitted); see, *e.g.*, *Coates* v. *City of Cincinnati*, 402 U.S. 611, 611, 614 (1971) (finding local ordinance vague where it proscribed conduct "annoying to persons passing by") (citation omitted). A vagueness challenge is not a license for policy-based narrowing of a sufficiently clear statute.

C. The Rule Of Lenity Does Not Apply

Finally, petitioner contends (Br. 40-41) that the rule of lenity requires interpreting Section 1030 to exclude his conduct. "But 'the rule of lenity only applies if, after considering text, structure, history, and purpose, there remains a grievous ambiguity or uncertainty in the statute, such that the Court must simply guess as to what Congress intended.'" *Castleman*, 572 U.S. at 172-173 (citation omitted). No such grievous ambiguity exists here. Rather, the text, history, and purpose of Section 1030 all illustrate that Congress intended to—and did—cover conduct like petitioner's. See pp. 16-34, *supra*.

Petitioner suggests (Br. 15-16, 29-32, 40-41) that this Court should default to the rule of lenity, even without a grievous ambiguity, when Congress drafts a federal statute that might impose criminal penalties on "everyday activities," unless Congress has provided "direct and unambiguous instructions" memorializing its contrary intent. Br. 15. As with his similar suggestion that this Court address his policy concerns by narrowing the statute to see how Congress responds, see pp. 43-44, *supra*, petitioner again misconceives the role of courts.

"[S]o long as Congress acts within its constitutional power in enacting a criminal statute, this Court must give effect to Congress' expressed intention concerning the scope of conduct prohibited." *United States* v. *Kozminski*, 487 U.S. 931, 939 (1988). Here, the language of Section 1030 unambiguously covers petitioner's conduct, and the statute's history confirms that the text embodies Congress's conscious design. Accordingly, even if petitioner were correct that Section 1030 could be applied, in other cases, "in situations not expressly anticipated by Congress," that possibility "does not demonstrate ambiguity." *Sedima, S. P. R. L.* v. *Imrex Co.*, 473 U.S. 479, 499 (1985) (citation omitted). Petitioner's conduct here was plainly within the scope of Section 1030, and this Court should affirm his conviction.

CONCLUSION

The judgment of the court of appeals should be affirmed.

Respectfully submitted.

JEFFREY B. WALL
Acting Solicitor General
Counsel of Record
BRIAN C. RABBITT
Acting Assistant Attorney General
ERIC J. FEIGIN
Deputy Solicitor General
MORGAN L. RATNER
Assistant to the Solicitor General
JENNY C. ELLICKSON
Attorney

AUGUST 2020

APPENDIX

18 U.S.C. 1030 provides:

Fraud and related activity in connection with computers

(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

---

[1] See References in Text note below.

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;

---

[2] So in original. The period probably should be a semicolon.

[3] So in original. Probably should be followed by "or".

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] So in original. The comma probably should not appear.

(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)[5] 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;

---

[5] See References in Text note below.

(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[6] (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

---

[6] So in original. Probably should be "subclause".

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[7]

---

[7] So in original. Probably should be followed by a period.