No. 19-783

In the Supreme Court of the United States

NATHAN VAN BUREN

v.

UNITED STATES OF AMERICA

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

BRIEF FOR THE UNITED STATES IN OPPOSITION

NOEL J. FRANCISCO
Solicitor General
Counsel of Record
BRIAN A. BENCZKOWSKI
Assistant Attorney 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

TABLE OF AUTHORITIES

Cases:

Cases—Continued: Page

Statutes and rule:

Miscellaneous: Page

In the Supreme Court of the United States

No. 19-783

NATHAN VAN BUREN

v.

UNITED STATES OF AMERICA

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

BRIEF FOR THE UNITED STATES IN OPPOSITION

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. The jurisdiction of this Court is invoked under 28 U.S.C. 1254(1).

STATEMENT

Following a jury trial in the United States District Court for the Northern District of Georgia, petitioner was convicted on one count of honest-services wire fraud, in violation of 18 U.S.C. 1343, 1346, and 1349; and one count of exceeding authorized access to a protected computer, in violation of 18 U.S.C. 1030(a)(2)(C) and (c)(2)(B)(i). Judgment 1. He was sentenced 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 but vacated petitioner's conviction for wire fraud and remanded for a new trial on that count. Pet. App. 32a; see *id.* at 1a-32a. Petitioner's new trial on the wire-fraud count is currently scheduled for June 22, 2020. D. Ct. Doc. 157, at 1 (Feb. 13, 2020).

1. Petitioner was a police sergeant in Cumming, Georgia. Pet. App. 3a. In that capacity, petitioner came to know Andrew Albo, a local man who allegedly paid prostitutes to spend time with him and then often accused the women of stealing the money he gave them. *Id.* at 3a-4a. Petitioner first met Albo when he helped arrest Albo for providing alcohol to a minor, and he often handled disputes between Albo and various women. *Id.* at 4a.

Because petitioner had financial difficulties, he decided to ask Albo for a loan, falsely claiming that he needed approximately $15,000 to pay his son's medical bills. Pet. App. 4a. Unbeknownst to petitioner, Albo recorded their conversations and presented the recording to a detective in the Forsyth County Sheriff's Office. *Ibid.* The Federal Bureau of Investigation (FBI) was informed of petitioner's loan solicitation, and it planned a sting operation in which Albo would offer petitioner cash in exchange for law-enforcement information. *Ibid.* In furtherance of the FBI's plan, Albo 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 but needed to know whether she was an undercover police officer before pursuing her further. *Ibid.* Petitioner agreed to

help, and he and Albo discussed checking the woman's license-plate number against a police database. *Ibid.*

In a later conversation, Albo asked petitioner whether he had conducted the search yet, and petitioner responded that he did not think he had gotten the correct license-plate number from Albo. Pet. App. 5a. Petitioner told Albo to text him the number, and Albo responded by sending petitioner a fake license-plate number that the FBI had created. *Ibid.* 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 that he did not have the $2000 they had discussed. *Ibid.* Petitioner asked Albo for the woman's name, explaining that the car might not be registered to her, and after Albo provided the name, petitioner promised to conduct the search soon. *Id.* at 5a-6a. Albo replied that "then I will have all the money for you." *Id.* at 6a.

A few days later, petitioner searched for the fake license-plate number in the Georgia Crime Information Center (GCIC) database. Pet. App. 6a. The GCIC database is an official government database maintained by the Georgia Bureau of Investigation and connected to the National Crime Information Center database maintained by the FBI. *Ibid.* Petitioner had received training on the proper uses of the GCIC database, and that training explained that law-enforcement officers are authorized to run searches in the GCIC database only for law-enforcement purposes and that Georgia law also imposes criminal penalties on officers who access information in the database for personal use. D. Ct. Doc. 127, at 14-15, 44-45, 51 (July 10, 2018). When petitioner searched the GCIC database for the fake license-plate

number the FBI had created, he accessed information associated with the fake number that FBI investigators had entered into the system. *Id.* at 79; see *id.* at 41-43. After running the search, petitioner texted Albo to tell him that he had information for him. Pet. App. 6a.

The following day, agents from the Georgia Bureau of Investigation and FBI visited petitioner's home and interviewed him. Pet. App. 6a. During the interview, petitioner admitted that he had concocted a fake story to justify asking Albo for $15,000 and acknowledged that he had received $6000 from Albo. *Ibid.* Petitioner also admitted that he knew that running the license-plate search for Albo was "wrong." *Ibid.* Petitioner claimed that $5000 of the money he received from Albo was a "gift," but when asked if he received anything in exchange for the license-plate search, he responded, "I mean he gave me $1,000." *Ibid.*

2. A federal grand jury returned an indictment charging petitioner with two counts of honest-services wire fraud, in violation of 18 U.S.C. 1343, 1346, and 1349, and 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). Superseding Indictment 1-5; see Pet. App. 6a. Section 1030(a)(2)(C) prescribes criminal penalties for "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] * * * information from any protected computer." 18 U.S.C. 1030(a)(2)(C). The statute defines the phrase "'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). A computer is a "'protected computer'" for purposes of Section 1030 if it "is used in or affecting interstate or foreign commerce or communication." 18 U.S.C. 1030(e)(2)(B).

The district court dismissed one of the honest-services counts on the government's motion, and petitioner proceeded to trial on the remaining honest-services count and the Section 1030 count. D. Ct. Doc. 81, at 1 (Oct. 25, 2017); Pet. App. 6a. At the close of the government's case, petitioner moved for a judgment of acquittal on both counts. D. Ct. Doc. 128, at 31 (July 10, 2018). As relevant here, petitioner's counsel argued that because petitioner "had the proper password" to the GCIC database and "had the authority to conduct tag searches" in the course of his official duties, his conduct did not violate Section 1030 even if he used his password to acquire protected information in return for a bribe. *Id.* at 44. The court denied petitioner's motion for a judgment of acquittal, finding that the government had presented sufficient evidence to allow both counts to go to the jury. *Id.* at 50. Petitioner renewed the motion at the close of all evidence, relying on the same arguments, and the court again denied the motion. *Id.* at 123-125.

Petitioner asked the district court to instruct the jury that the Section 1030 count required the government to prove beyond a reasonable doubt that petitioner "intentionally accessed a computer in a way or to an extent beyond the permission given," in addition to other requirements. D. Ct. Doc. 70, at 21 (Oct. 23, 2017). Petitioner further asked the court to instruct the jury that "[t]o access a computer 'in a way or to an extent beyond the permission given'" means "to use authorized access to get or change information that the person is not permitted to get or change." *Ibid.* The government

proposed the same instructions, D. Ct. Doc. 69, at 21 (Oct. 22, 2017), and the court gave those instructions to the jury, D. Ct. Doc. 129, at 51 (July 10, 2018). See D. Ct. Doc. 128, at 140, 151 (discussion at jury-charge conference).

During closing arguments, the government contended that petitioner exceeded his authorized access to the GCIC database when he searched for the fake license-plate number for his "own private gain" and for a "non[-]law enforcement purpose." D. Ct. Doc. 129, at 6; see also *id.* at 10-11. In contrast, petitioner's counsel argued that petitioner had not exceeded his authority to access the GCIC database because petitioner "had a password" and "was certified for GCIC searches." *Id.* at 33.

The jury found petitioner guilty on both counts. D. Ct. Doc. 129, at 73. The district court sentenced petitioner to 18 months of imprisonment, to be followed by two years of supervised release. Judgment 2-3.

3. 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 rejected petitioner's contention that insufficient evidence supported his Section 1030 conviction. *Id.* at 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 explained that an individual can "exceed[] authorized access" to a protected computer when she accesses the computer for a prohibited purpose or use. Pet. App. 26a-27a. Although the court

"acknowledge[d] that other courts have rejected *Rodriguez*'s interpretation of 'exceeds authorized access,'" the court found "no question that the record contained enough evidence for a jury to convict" petitioner on the Section 1030 count under *Rodriguez*. *Id.* at 27a-28a. It explained that petitioner "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.

With respect to petitioner's conviction for honest-services fraud, the court of appeals determined that the jury instructions on that count were erroneous under this Court's decision in *McDonnell* v. *United States*, 136 S. Ct. 2355 (2016). Pet. App. 8a-22a. Because the court concluded that the error was not harmless, it vacated petitioner's conviction for honest-services fraud and remanded for a new trial on that count. *Id.* at 16a-22a, 32a.

4. After the court of appeals issued its decision, the case returned to the district court, and the district court scheduled a new trial. D. Ct. Doc. 149, at 1 (Dec. 11, 2019). The trial is currently set for June 22, 2020. D. Ct. Doc. 157, at 1.

ARGUMENT

Petitioner contends (Pet. 6-22) that the evidence was insufficient to support his conviction for 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). Although some disagreement exists in the circuits about the meaning of the phrase "exceeds authorized access" in 18 U.S.C. 1030, this case would be a poor vehicle for resolving that issue because the decision below is interlocutory and because

the jury instructions at petitioner's trial were consistent with petitioner's narrower interpretation of "exceeds authorized access." Further review is therefore unwarranted.

1. As a threshold matter, this Court's review is unwarranted at this time because petitioner's case is in an interlocutory posture. Although the court of appeals affirmed petitioner's conviction on the Section 1030 count, it vacated his conviction for honest-services fraud and remanded the case to the district court for a new trial on that count. Pet. App. 3a, 32a. Petitioner's trial is currently scheduled for June 22, 2020. D. Ct. Doc. 157, at 1. The interlocutory posture of the case "of itself alone furnishe[s] sufficient ground for the denial" of the petition. *Hamilton-Brown Shoe Co.* v. *Wolf Bros. & Co.*, 240 U.S. 251, 258 (1916); accord *Abbott* v. *Veasey*, 137 S. Ct. 612, 613 (2017) (Roberts, C.J., respecting the denial of certiorari); *Virginia Military Inst.* v. *United States*, 508 U.S. 946, 946 (1993) (Scalia, J., respecting the denial of the petition for writ of certiorari); *Brotherhood of Locomotive Firemen & Enginemen* v. *Bangor & Aroostook R.R.*, 389 U.S. 327, 328 (1967) (per curiam); see generally Stephen M. Shapiro et al., *Supreme Court Practice* § 4.18, at 282-283 & n.72 (10th ed. 2013) (noting that the Court routinely denies interlocutory petitions in criminal cases).

Petitioner provides no sound reason to depart from the Court's usual practice of awaiting final judgment. In the district court, petitioner suggested that the government "may not retry" him on the honest-services count if the Court denies the petition. D. Ct. Doc. 151, at 1 (Dec. 18, 2019); D. Ct. Doc. 156, at 2 (Feb. 10, 2020). But even if the government were to make that choice,

the district court would need to enter a new final decision in the case if the honest-services count is dismissed. Cf. Fed. R. Crim. P. 32(k)(1). Petitioner could then raise his current claim—together with any additional claims arising from the remand proceedings—in a single petition for a writ of certiorari seeking review of the final judgment against him. See *Hamilton-Brown Shoe Co.*, 240 U.S. at 258; see also *Major League Baseball Players Ass'n* v. *Garvey*, 532 U.S. 504, 508 n.1 (2001) (per curiam) (noting that the Court "ha[s] authority to consider questions determined in earlier stages of the litigation where certiorari is sought from" the most recent judgment). And if petitioner is retried, convicted, and subject to a concurrent sentence on the wire-fraud count, the practical significance of his challenge to his Section 1030 conviction would be reduced. The interests of judicial economy are thus best served by permitting the proceedings in the lower courts to conclude.

2. The petition does not otherwise warrant this Court's review. Congress has prohibited "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing] * * * information from any protected computer." 18 U.S.C. 1030(a)(2)(C). And Congress has defined the phrase "'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). Petitioner contends (Pet. 6) that a person exceeds authorized access only when "he had no right at all to access the information" he obtained, and argues (Pet. 6-7, 16-22) that the Eleventh Circuit's contrary reading of "exceeds authorized access" is too broad. But

this case would be a poor vehicle for resolving any circuit disagreement about the scope of the statutory phrase "exceeds authorized access."

a. As petitioner observes, the circuits have disagreed about whether a person "exceeds authorized access" to a protected computer, in violation of 18 U.S.C. 1030, when she has access to a computer system for certain legitimate purposes but then accesses the system for a prohibited purpose. Petitioner, however, overstates (Pet. 11) the number of courts of appeals that have directly considered the question.

The Eleventh Circuit previously determined that an individual can "exceed authorized access" to a protected computer by employing his access to obtain or alter information in an unauthorized way. See *United States* v. *Rodriguez*, 628 F.3d 1258 (2010), cert. denied, 563 U.S. 966 (2011). In *Rodriguez*, a customer-service representative at the Social Security Administration (SSA) with access to databases containing sensitive personal information obtained such personal information about 17 individuals (his ex-wife, her sister, an ex-girlfriend, her father, and other acquaintances) for non-business purposes. *Id.* at 1260-1261. The employee's actions violated a written SSA policy that prohibited employees from obtaining information from SSA databases without a business reason, and SSA employees had been warned that "they faced criminal penalties if they violated [those] policies." *Id.* at 1260. The Eleventh Circuit affirmed the employee's conviction under 18 U.S.C. 1030(a)(2)(B), explaining that the employee's "access of the victims' personal information was not in furtherance of his duties as a [customer-service] representative" and he had "access[ed] things that were unauthorized." *Rodriguez*, 628 F.3d at 1263.

In the decision below, the court of appeals followed *Rodriguez*, Pet. App. 28a, and rejected petitioner's contention that a person can never have "exceeded authorized access" so long as "he accessed only databases that he was authorized to use" for some purposes, even when he uses that access for unauthorized purposes. *Id.* at 27a. Several other courts of appeals have issued decisions consistent with the Eleventh Circuit's construction in *Rodriguez*. But they have not definitively interpreted the statute in the manner petitioner suggests, and have instead more narrowly tailored their decisions to the particular circumstances at issue.

Contrary to petitioner's contention (Pet. 7), the First Circuit's factbound decision in the civil context in *EF Cultural Travel BV* v. *Explorica, Inc.*, 274 F.3d 577 (2001), has limited relevance here. In that case, the defendant company designed a program to retrieve large quantities of proprietary pricing information from the plaintiff company's public website. *Id.* at 579-581. Leading that effort was an employee who had previously worked for the plaintiff company and who shared the plaintiff's confidential information with the program's developers, in violation of his confidentiality agreement with the plaintiff. *Id.* at 579, 582-583. Based on those facts, the First Circuit affirmed the district court's issuance of a preliminary injunction, reasoning in part that the plaintiff would "likely" prove that the defendant had exceeded authorized access to the plaintiff's website. *Id.* at 582; see *id.* at 581-584. The court of appeals stated that the defendant's conduct violated the confidentiality agreement and therefore went "beyond any authorized use of" the plaintiff's website. *Id.* at 583. The court did not, however, provide a definitive view of the statute's reach and instead upheld the district court's

preliminary injunction as "not clearly erroneous" under the particular circumstances of the case. *Id.* at 583-584.

Petitioner also cites (Pet. 8) *International Airport Centers, L.L.C.* v. *Citrin*, 440 F.3d 418 (7th Cir. 2006). That civil case, however, concerned an allegation that an individual had accessed a computer "without authorization," not an allegation that he had done so "exceed[ing] authorized access." See *id.* at 420-421. Specifically, *Citrin* addressed whether an employee accessed his employer-issued laptop "'without authorization'" when, "having already engaged in misconduct and decided to quit * * * in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were also the property of his employer." *Id.* at 420 (citation omitted). The Seventh Circuit held that the employee's "breach of his duty of loyalty terminated his agency relationship * * * and with it his authority to access the laptop, because the only basis of his authority had been that relationship." *Id.* at 420-421. *Citrin* did not purport to define the range of circumstances in which an individual "exceeds authorized access."

Finally, the Fifth Circuit's decision in *United States* v. *John*, 597 F.3d 263 (2010), aff'g after remand, 466 Fed. Appx. 356 (2012), cert. denied, 568 U.S. 1163 (2013), did not adopt a comprehensive definition of Section 1030's reach. The defendant in *John* was an account manager at Citigroup with access to Citigroup's internal computer system, which contained customer account information. *Id.* at 269. The defendant surreptitiously accessed and printed confidential Citigroup records from at least 76 corporate customer accounts and provided them to her half-brother so that he and others could use the information to incur fraudulent charges. *Ibid.* A

jury found the defendant guilty on two counts of exceeding her authorization to a protected computer, in violation of 18 U.S.C. 1030(a)(2)(A) and (C), and the court of appeals affirmed the defendant's conviction on plain-error review. *John*, 597 F.3d at 269-272. In rejecting a challenge to those convictions, the court stated that, for purposes of Section 1030, an individual's "'authorized access'" to a computer "may encompass limits placed on the use of information obtained by permitted access * * * , at least when the user knows or reasonably should know that he or she is not authorized to access a computer and information obtainable from that access in furtherance of or to perpetrate a crime." *Id.* at 271 (emphasis omitted); see *id.* at 272 ("[T]he concept of 'exceeds authorized access' may include exceeding the purposes for which access is 'authorized.'").

The Fifth Circuit in *John* did not decide whether an individual might exceed authorized access by obtaining information for other, non-criminal, prohibited purposes. See 597 F.3d at 270-273. Some district courts in that circuit have interpreted its statement that "[a]ccess to a computer and data that can be obtained from that access may be exceeded if the purposes for which access has been given are exceeded," *id.* at 272, to encompass some such cases. See, *e.g.*, *Associated Pump & Supply Co.* v. *Dupre*, No. 14-9, 2014 WL 1330196, at *6 (E.D. La. Apr. 3, 2014) (finding that company stated claim against former employee who accessed proprietary information to use in violation of confidentiality and non-compete agreement); *Beta Tech., Inc.* v. *Meyers*, No. 13-1282, 2013 WL 5602930, at *3 (S.D. Tex. Oct. 10, 2013) (similar); *Meats by Linz, Inc.* v. *Dear*, No. 10-CV-1511, 2011 WL 1515028, at *2-*3 (N.D. Tex. Apr.

20, 2011) (similar). But the Fifth Circuit itself has yet to directly address them.

b. As petitioner observes (Pet. 9-10), the Second, Fourth, and Ninth Circuits have adopted interpretations of "exceeds authorized access" that diverge from the Eleventh Circuit's view of the statute. See *United States* v. *Valle*, 807 F.3d 508, 511-513 (2d Cir. 2015) (concluding that a police officer had not exceeded authorized access under Section 1030 when he accessed law-enforcement databases in violation of department policies); *WEC Carolina Energy Solutions LLC* v. *Miller*, 687 F.3d 199, 206 (4th Cir. 2012), cert. dismissed, 568 U.S. 1079 (2013) (concluding that an individual "'exceeds authorized access'" only when he "obtains or alters information on a computer beyond that which he is authorized to access"); *United States* v. *Nosal*, 676 F.3d 854, 856-857, 863-864 (9th Cir. 2012) (en banc) (concluding that "'exceeds authorized access'" in Section 1030 "is limited to violations of restrictions on *access* to information, and not restrictions on its *use*"). But petitioner's case would be a poor vehicle for addressing the disagreement among the circuits because the jury at petitioner's trial found him guilty under jury instructions that were consistent with the narrower interpretation of the statute that petitioner asks this Court to adopt. Accordingly, further review of that statutory question would not change the outcome of petitioner's case. And to the extent petitioner's real complaint is that the jury incorrectly assessed the evidence in his particular case, that factbound issue does not warrant this Court's review.

Petitioner asserts that "[t]he most natural reading" of the definition of "'exceeds authorized access'" in Section 1030(e)(6) "is that a person 'obtain[s] information in the computer that [he] is not entitled so to obtain'

only if he had no right at all to access the information." Pet. 6 (citation omitted; brackets in original). Petitioner pressed the same construction of the statute during the proceedings below, see D. Ct. Doc. 128, at 42-44, and, as relevant here, asked the district court to instruct the jury 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. 70, at 21. The court gave that precise instruction to the jury at petitioner's trial. D. Ct. Doc. 129, at 51. And petitioner himself appeared to believe that the instruction accorded with his narrower construction of Section 1030, as petitioner's counsel argued to the jury in closing arguments that petitioner had not exceeded his authority to access the GCIC database because petitioner "had a password" and "was certified for GCIC searches." *Id.* at 33.

The district court's adoption of petitioner's instruction on the requirements of Section 1030 undermines any claim that the jury found petitioner guilty on the Section 1030 count based on a determination that petitioner had "permission to access" the information he obtained from the GCIC database but "accesse[d] that information for an improper purpose," Pet. 6. As this Court has recognized, "the crucial assumption underlying the system of trial by jury is that juries will follow the instructions given them by the trial judge." *Marshall* v. *Lonberger*, 459 U.S. 422, 438 n.6 (1983) (citation and internal quotation marks omitted); see *Kansas* v. *Carr*, 136 S. Ct. 633, 645 (2016); *Zafiro* v. *United States*, 506 U.S. 534, 540-541 (1993); *Richardson* v. *Marsh*, 481 U.S. 200, 206 (1987). In this case, that principle indicates that the jury found petitioner guilty because it

determined that he had used his access to the GCIC database to obtain or alter information that he was "not permitted to get or change." D. Ct. Doc. 70, at 21. That determination is consistent with the narrow reading of "exceeds authorized access" that petitioner asks this Court to adopt. And even if petitioner disagrees with the jury's finding that the evidence established that he used his access to the GCIC database to obtain or alter information that he was "not permitted to get or change," *ibid.*, that factbound, case-specific determination does not warrant this Court's review. See *United States* v. *Johnston*, 268 U.S. 220, 227 (1925).

3. Finally, petitioner contends (Pet. 2, 12-13, 19-22) that this Court should grant review to ensure that "the Executive Branch" does not have "virtually unfettered prosecutorial discretion" to prosecute "commonplace activities of nearly all computer users." Pet. 20. Petitioner further contends (Pet. 13-15) that disagreement among the circuits over the meaning of "exceeds authorized access" leads to disparate outcomes in Section 1030 cases, "giv[ing] rise to a serious danger of forum shopping" and presenting potential issues regarding "fair notice." Pet. 15. Petitioner does not, however, identify any case in which a court of appeals has determined that the statute authorizes the prosecution of someone who engages in such "commonplace activities" involving the violation of private computer-use policies, Pet. 20, as opposed to misappropriating proprietary or confidential information for forbidden uses.

In addition, the Department of Justice's Intake and Charging Policy for Computer Crime Matters (Charging Policy), Memorandum from U.S. Att'y Gen. to U.S. Att'ys and Asst. Att'y Gens. for the Crim. and Nat'l Sec.

Divs. (Sept. 11, 2014),[*] ameliorates petitioner's theoretical concerns about the potential breadth of Section 1030. The Attorney General issued the Charging Policy in 2014 to ensure that government attorneys apply Section 1030 "consistently" and to improve the public's understanding of "how the Department applies the law." *Id.* at 1. As relevant here, the Charging Policy identifies numerous factors that Department of Justice attorneys consider when deciding whether to pursue a prosecution under Section 1030. See *id.* at 1-5. The policy explains that, when prosecuting an exceeded-authorized-access violation under Section 1030, the government "must be prepared to prove that the defendant knowingly violated restrictions on his authority to obtain or alter information stored on a computer, and not merely that the defendant subsequently misused information or services that he was authorized to obtain from the computer at the time he obtained it." *Id.* at 4. The Charging Policy also recognizes that "[t]he extent of the federal interest in exceeds-authorized-access prosecutions under section 1030(a)(2) varies based upon both the nature of the conduct and the nature of the information obtained during the offense." *Ibid.* It explains that factors weighing in favor of prosecution include "the abuse of a position of trust" and criminal conduct that "threatened national or economic interests, was in furtherance of a larger criminal endeavor, or posed a

---

[*] This policy is publicly available at https://www.justice.gov/criminal-ccips/file/904941/download. See U.S. Dep't of Justice, *Department Releases Intake and Charging Policy for Computer Crime Matters* (Oct. 25, 2016), https://www.justice.gov/archives/opa/blog/department-releases-intake-and-charging-policy-computer-crime-matters (announcement of the 2016 public release of the policy).

risk of bodily harm or threat to national security." *Ibid.* And 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 terms of service with an Internet service provider." *Id.* at 5.

Although petitioner asserts (Pet. 20) that the government has, in the past, "brought cases against individuals who have violated companies' terms of service agreements," all of the cases petitioner identifies predate the 2014 Charging Policy. See Pet. 20-21. Petitioner also fails to identify any case, either before or after the issuance of the Charging Policy, in which the government has attempted to apply the statute to "checking sports scores at work," "inflating one's height on a dating website," or engaging in the other hypothetical "trivial" conduct described in the petition. Pet. 2; see *id.* at 12-13. Nor does any significant possibility exist of a private civil suit in those circumstances, as Section 1030(g) authorizes such suits only for compensatory damages totaling at least $5000 (outside of certain categories unlikely to apply to the hypothetical conduct that petitioner envisions). 18 U.S.C. 1030(g); see 18 U.S.C. 1030(c)(4)(A)(i)(I). Courts have therefore had no occasion to determine whether such "commonplace activities" (Pet. 20) fall within the terms of the statute.

CONCLUSION

The petition for a writ of certiorari should be denied.

Respectfully submitted.

NOEL J. FRANCISCO
Solicitor General
BRIAN A. BENCZKOWSKI
Assistant Attorney General
JENNY C. ELLICKSON
Attorney

MARCH 2020