No. 23-_____

In the
Supreme Court of the United States

Medghyne Calonge,

Petitioner,

v.

United States of America,

Respondent.

On Petition for a Writ of Certiorari to
The United States Court of Appeals
For the Second Circuit

PETITION FOR A WRIT OF CERTIORARI

Kendra L. Hutchinson
Federal Defenders of New York
Appeals Bureau
52 Duane Street, 10th Floor
New York, New York 10007
(212) 417–8731
Kendra_Hutchinson@fd.org

Counsel for Petitioner

QUESTION PRESENTED

Petitioner was convicted of two Computer Fraud and Abuse Act (CFAA) violations requiring "damage" to protected computers. At trial, the government's evidence showed that petitioner was in Florida when she deleted her former employer's data, and that this data physically resided in a database located in servers in Virginia and California. Nevertheless, the Second Circuit found that venue in the Southern District of New York was proper, because, due to petitioner's actions, users were unable to login remotely to the database to access the data on their computers in New York. It reached this result by construing the CFAA's definition of "damage," 18 U.S.C. § 1030(e)(8), as broadly as possible, to include a user's inability to virtually access data, no matter where the data physically resided.

Accordingly, the question presented is whether the Second Circuit correctly held that the evidence of venue was legally sufficient under the Venue and Vicinage Clauses of the United States Constitution?

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

RULES

CONSTITUTIONAL PROVISIONS

OTHER AUTHORITIES

OPINION BELOW

The opinion of the United States Court of Appeals for the Second Circuit is reported at 74 F.4th 31 and appears in Petitioner's Appendix at A.1-11.[1]

JURISDICTION

The district court had jurisdiction pursuant to 18 U.S.C. § 3231 and entered judgment on December 16, 2021. The Second Circuit had jurisdiction under 18 U.S.C. § 1291 and issued its opinion and judgment on July 14, 2023. This Court has jurisdiction under 18 U.S.C. § 1254(1).

RELEVANT CONSTITUTIONAL AND STATUTORY PROVISIONS

The Venue Clause of Article III, Section 2, of the United States Constitution provides, in relevant part: "The Trial of all Crimes . . . shall be held in the State where the said Crimes shall have been committed . . . ."

The Vicinage Clause of the Sixth Amendment to the United States Constitution provides, in relevant part: "the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed . . . ."

Subsection (a)(5)(A) of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, punishes one who:

> 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.

[1] Pages in Petitioner's Appendix are cited "A."

Subsection (a)(5)(B) of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, punishes one who:

> intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage.

Subsection (e)(8) of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030, defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information."

INTRODUCTION

Medghyne Calonge, a Florida resident, was charged with two violations of the Computer Fraud and Abuse Act (CFAA), 18 U.S.C. § 1030, for deleting the data of her former employer and thereby causing damage. The physical acts constituting the crime occurred in Florida. Moreover, the data that was deleted physically resided in cloud-based servers located in Virginia and California. Nevertheless, the Second Circuit held that venue was proper in the Southern District of New York. It did so by construing the CFAA's definition of "damage," 18 U.S.C. § 1030(e)(8), as broadly as possible, to include a user's inability to virtually access the data on the web browser of a computer located in the Southern District of New York .

In this modern, cloud-based, wired world, allowing the Second Circuit's holding to stand would vitiate the venue requirement in numerous CFAA cases and make a person subject to prosecution in any and every district throughout the country. This does not comport with the historical underpinnings of the Venue and Vicinage Clauses of the Constitution, and would risk unfairness for the accused and

forum-shopping by the government. Moreover, the Second Circuit's reading contravenes this Court's admonition in *United States v. Johnson*, 323 U.S. 273, 275 (1944), that venue must be construed narrowly. Given the importance and timeliness of the issue, this Court's review is necessary.

STATEMENT OF THE CASE

Ms. Calonge was tried before a jury for two violations of the Computer Fraud and Abuse Act (CFAA): one count of knowingly causing the transmission of a program, code, or command, and thereby intentionally causing damage without authorization to a protected computer, 18 U.S.C. § 1030(a)(5)(A); and one count of intentionally accessing a protected computer without authorization and thereby recklessly causing damage, 18 U.S.C. § 1030(a)(5)(B).

The trial evidence showed that in January 2019, Ms. Calonge was hired as a human resources manager in the St. Petersburg, Florida, office of 1-800-Accountant, a virtual accounting firm that recruited and maintained lists of accountants who could be hired out to customers to perform remote work. To track recruitment and accountant historical data, 1-800-Accountant used an extensive database system maintained by an external third-party vendor, JazzHR. 1-800-Accountant employees accessed the JazzHR database by logging into it through web browsers on computers, laptops, smartphones, etc., wherever they were located. A.3.

Ms. Calonge ultimately was terminated from the position in June 2019 due to job performance issues. She was fired on a Friday afternoon; that weekend, nearly all of the recruitment and historical data in the JazzHR database was deleted by

Ms. Calonge's user account. 1-800-Accountant never was able to fully recover the deleted data. A.3-4.

Ms. Calonge was a resident of Florida. The office where she had worked was located in Florida. And a JazzHR internet technician testified that the deleted data had physically resided on servers in Virginia and California. Nevertheless, Ms. Calonge was charged and tried in the Southern District of New York. This was based on the testimony of Amy Gaspari, Ms. Calonge's supervisor, who worked in the company's Madison Avenue headquarters in Manhattan, New York. Ms. Gaspari testified that, after the weekend deletions, she was unable to access the JazzHR data from her office computer. Another New York employee told Ms. Gaspari that she, too, was unable to access the data. A.3-4.

Ms. Calonge moved for a judgment of acquittal under Federal Rule of Criminal Procedure 29, arguing that the evidence was insufficient to prove that venue was proper in the Southern District of New York because the deleted data did not physically reside in the district, and that allowing prosecution in such circumstances unconstitutionally expanded venue. The district court denied the motion, reasoning that venue was proper wherever damage to a protected computer occurred, and that the inability to access the deleted data from a computer in Manhattan, New York constituted "damage" to that computer. A.5. The final charge on venue was in accordance with the district court's ruling, and the jury subsequently convicted Ms. Calonge of both counts.

Ms. Calonge pressed the venue insufficiency argument on appeal. In particular, relying on the policy concerns expressed by the Third Circuit in the only other Court of Appeals case concerning CFAA venue, *United States v. Auernheimer*, 748 F.3d 525 (3d. Cir. 2014), she noted that, in an increasingly-cloud-based world, permitting CFAA venue in any district where someone's virtual access to data was impaired as a result of computer access or transmissions would vitiate the Constitutional venue requirement, and allow the government limitless freedom to choose its forum. *See* Brief for Defendant-Appellant 29-30, Jul. 8, 2022, ECF No. 36, *United States v. Calonge*, No. 21-3089 (2d Cir.).

The Second Circuit was not blind to the difficulties of ascertaining proper venue in the modern, cloud-based world:

> The proliferation of Internet-related crimes has further complicated the issue of appropriate venue. *See United States v. Auernheimer*, 748 F.3d 525, 541 (3d. Cir. 2014). In a world increasingly marked by remote work, it is not unusual that companies like 1-800-Accountant, based in New York, would manage employees who work in Florida or other states and handle data that is physically stored on cloud servers in various locations around the country, and that is potentially accessible to job applicants or other users in countless other jurisdictions. A.6.

However, it rejected the defense arguments and affirmed the judgment, essentially adopting the district court's reasoning. First, it held that each CFAA count of conviction included, as an "essential conduct element," damage to a protected computer, and, thus, that venue would be proper wherever such damage occurred. A.6-8 (citing *United States v. Rodriguez-Moreno*, 526 U.S. 275 (1999)).

Second, and most importantly, it adopted an expansive, wide-ranging view of the meaning of "damage":

> The text of the CFAA is clear that preventing a computer from accessing data that it regularly accesses constitutes "damage" under the statute. The statute defines damage as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). The jury was entitled to conclude that Calonge's actions impaired the availability of data on the JazzHR system on Gaspari's computer [in New York]. The fact that the deletion might also have damaged the Amazon servers located in Virginia and California makes no difference. A9-10.

The Second Circuit dismissed Ms. Calonge's reliance on the Third Circuit's *Auernheimer* decision, reasoning that that case concerned a different subsection of the CFAA, § 1030(a)(2)(c), which punishes one who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer." The Second Circuit opined that, because that subsection does not include a "damage" "essential conduct element," *Auernheimer*'s rationale was not persuasive. A.10-11.

REASONS FOR GRANTING THE WRIT

I. The venue requirement is essential to ensure a fair trial for the accused and curb government abuse; it must be construed narrowly.

The United States Constitution "twice safeguards the defendant's venue right." *United States v. Cabrales*, 524 U.S. 1, 6 (1998). The Venue Clause of Article III requires that "the Trial of all Crimes . . . shall be held in the State where the said Crimes shall have been committed." U.S. Const. art. III, § 2, cl. 3. And the Vicinage Clause of the Sixth Amendment further provides that "[i]n all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the State and district wherein the crime shall have been committed." *Id.* amend VI. *See also* Fed. R. Crim. Proc. 18 (requiring that "the government must prosecute an offense in a district where the offense was committed").

These clauses have lengthy historical provenance. They trace back to the Magna Carta, which declared that "[n]o free man shall be seized or imprisoned . . . except by the lawful judgment of his equals." Magna Carta cl. XXXIX (G.R.C. Davis trans., London British Museum 1963) (1215); *id.* cl. XX (declaring that punishment would not be "imposed except by the assessment on oath of reputable men of the neighborhood"). Deeply embedded in the common-law at the founding, "[t]here is no question that the founding generation enthusiastically embraced the vicinage right and wielded it as a political argument of the Revolution." *Smith v. United States*, 599 U.S. 236, 246 (2023) (internal citation and quotation omitted). In particular, revolutionary legislatures and colonists rallied around opposition to Parliament's

passage of laws to circumvent local trials by authorizing trials in England for British soldiers accused of murdering colonists, and colonists accused of treason. *Id.* Hence, the "right was highly prized by the founding generation, and this right undoubtedly inspired the Venue and Vicinage Clauses." *Id.* at 248; *Cabrales*, 524 U.S. at 6 ("[p]roper venue in criminal proceedings was a matter of concern to the Nation's founders").

Given its prominence in the Constitution, this Court has explained that the venue provisions are not "matters of mere procedure." *Travis v. United States*, 364 U.S. 631, 634 (1961). Instead, those provisions serve at least two salutary functions. They protect an accused from "the unfairness and hardship to which trial in an environment alien to the accused exposes him." *United States v. Johnson*, 323 U.S. 273, 275 (1944). In addition, they guard against prosecutorial abuse by limiting the government's ability to forum- and jury-shop. *Id.* at 275 (venue requirement prevents "the appearance of abuses, if not . . . abuses, in the selection of what may be deemed a tribunal favorable to the prosecution").

Accordingly, this Court has held that venue must be narrowly construed in order to effect these aims. *Id.* at 276 ("Questions of venue in criminal cases . . . are not merely matters of formal legal procedure. They raise deep issues of public policy in the light of which legislation must be construed."); *see also United States v. Cores*, 356 U.S. 405, 407 (1958) ("Provided its language permits, the Act in question should be given that construction which will respect [the] considerations [raised in *Johnson*].") Venue thus will only be proper where the acts constituting the offense –

the crime's "essential conduct elements" – took place. *Rodriguez-Moreno*, 526 U.S. at 280.

II. The Second Circuit's holding results in limitless venue in numerous CFAA prosecutions.

Ms. Calonge was convicted of 18 U.S.C. § 1030(a)(5)(A) and (a)(5)(B), both of which require that the person's acts – knowing transmission of a code or program, or intentional unauthorized access to a computer, respectively – cause "damage." Congress defined "damage" in the CFAA as "any impairment to the integrity or availability of data, a program, a system, or information." 18 U.S.C. § 1030(e)(8). The Second Circuit construed this definition of damage as broadly as possible. Rather than limiting it to the impairment or unavailability of data where it resides, as the defense argued, *i.e.,* the *physical* location of the servers or computers that house the actual digital data, it held that any computer, anywhere in the country, that is unable to *virtually* access the data suffers "damage" under the CFAA.

This holding results in venue without limit in CFAA prosecutions. In the modern world, countless cloud-based, internet applications and programs are used by millions of people nationwide. Applying the Second Circuit's logic, a person who accesses such a program's servers and impairs them in some fashion would be prosecutable in every single jurisdiction in which someone tried to use the program but was unable to. For example, someone who, say, hacks into the Texas-based server of a social media company, thereby causing its millions and millions of subscribers to lose access to their account profiles, could be prosecuted in every district court of all fifty states. All that would be required is for one user in the

district to be unable to login or view their profile, even temporarily. After all, under the Second Circuit's reasoning, there is no temporal or monetary qualification as to the "damage" that must be caused.

This construction of the CFAA comports with neither the historical tradition underpinning the Venue and Vicinage Clauses, nor the policy concerns animating their adoption by the founders. A person subject to prosecution anywhere would be subject to "the unfairness and hardship to which trial in an environment alien to the accused exposes him." *Johnson*, 323 U.S. 275. And nothing would cabin the government's ability to forum-shop for "a tribunal favorable to the prosecution." *Id.* Allowing the Second Circuit's decision to stand thus contravenes this Court's admonition that venue must be construed narrowly, to effectuate the "deep issues of public policy" involved. *Id.* at 276. Moreover, Congress could not possibly have intended this absurd and unfair result when it enacted the CFAA in 1986, at a time shortly after the birth of the internet, when nobody could have anticipated the immense advances in connectedness and computing that would ensue over the next four decades.

Only one other Court of Appeal has considered venue for CFAA purposes. In *Auernheimer*, 748 F.3d 525, the Third Circuit considered a different subsection of the CFAA, § 1030(a)(2)(C), punishing intentional unauthorized access resulting in obtaining information. The defendant, an Arkansas resident, was tried in the District of New Jersey based on allegations that he and a co-conspirator used a "brute force attack" program to collect tens of thousands of email addresses from the

AT&T website. *Id*. at 531. Auernheimer thereafter alerted a member of the media to the AT&T security flaw, and provided a list of email addresses to the reporter. *Id*. The government argued that venue in New Jersey was proper because, although the conduct did not take place in New Jersey, and the accessed servers were not in New Jersey, New Jersey residents were affected by the disclosure of their email addresses. *Id*.

The Third Circuit found that venue for the CFAA conspiracy count was improper because the "essential conduct elements" of the CFAA violation did not take place in New Jersey. *Id*. at 534-35. That court cautioned:

> Venue issues are animated in part by the danger of allowing the Government to choose its forum free from any external constraints. The ever-increasing ubiquity of the Internet only amplifies this concern. As we progress technologically, we must remain mindful that cybercrimes do not happen in some metaphysical location that justifies disregarding constitutional limits on venue. People and computers still exist in identifiable places in the physical world. When people commit crimes, we have the ability and obligation to ensure that they do not stand to account for those crimes in forums in which they performed no essential conduct element of the crimes charged.

Id. at 541 (internal quotations, citations, and brackets omitted).

It is true that, as the Second Circuit noted in its opinion, A.11, Ms. Calonge and the *Auernheimer* defendant were charged with different subsections of the CFAA, with different elements, and thus the venue analysis necessarily must be different. The problem, however, is that, unlike the Third Circuit, the Second Circuit made no attempt here to grapple with the inherent problems of determining venue in a wired, cloud-based world. Nothing about the Second Circuit's opinion in

Ms. Calonge's case acknowledges that "cybercrimes do not happen in some metaphysical location that justifies disregarding constitutional limits on venue." *Id.*

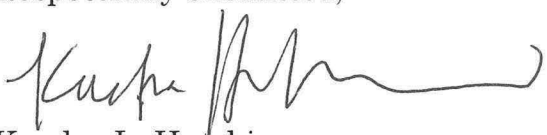
III. This case presents a suitable vehicle for resolving the question presented.

This case provides an appropriate certiorari vehicle. Petitioner raised the question presented in the district court, and specifically urged the Second Circuit to reverse the judgment on this ground. Moreover, the facts relating to venue are undisputed. The issue is purely legal, as it concerns the permissible, constitutional construction of 18 U.S.C. § 1030(e)(8)'s definition of "damage." The Second Circuit cleanly decided the question on the merits in a published decision that is likely to prove influential, given the paucity of caselaw on the issue, and which lower courts will be bound to follow. Finally, the decision on this issue was dispositive to the outcome of Ms. Calonge's appeal as to both counts of conviction.

CONCLUSION

For the foregoing reasons, the Court should grant this petition for a writ of certiorari.

Respectfully submitted,



Kendra L. Hutchinson
Federal Defenders of New York
Appeals Bureau
52 Duane Street, 10th Floor
New York, New York 10007
(212) 417–8731
Kendra_Hutchinson@fd.org

October 12, 2023

Counsel for Petitioner