No. 19-783

In the Supreme Court of the United States

NATHAN VAN BUREN, PETITIONER

v.

UNITED STATES

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

BRIEF FOR THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS ET AL. AS AMICI CURIAE SUPPORTING PETITIONER

BRUCE D. BROWN
KATIE TOWNSEND
GABRIEL ROTTMAN
REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS
1156 15th Street, N.W., Suite 1020
Washington, DC 20005

KANNON K. SHANMUGAM
Counsel of Record
JOEL S. JOHNSON
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
2001 K Street, N.W.
Washington, DC 20006
(202) 223-7300
kshanmugam@paulweiss.com

AMANDA C. WEINGARTEN
PAUL, WEISS, RIFKIND, WHARTON & GARRISON LLP
1285 Avenue of the Americas
New York, NY 10019

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page

Cases—continued:

Statutes:

Miscellaneous:

Page

Miscellaneous—continued:

Page

Miscellaneous—continued:

In the Supreme Court of the United States

No. 19-783

NATHAN VAN BUREN, PETITIONER

v.

UNITED STATES

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

BRIEF FOR THE REPORTERS COMMITTEE FOR FREEDOM OF THE PRESS ET AL. AS AMICI CURIAE SUPPORTING PETITIONER

INTEREST OF AMICI CURIAE

Amici curiae[1] are Reporters Committee for Freedom of the Press; Advance Publications, Inc.; ALM Media, LLC; The Associated Press; Boston Globe Media Partners, LLC; BuzzFeed; The Center for Investigative Reporting (d/b/a Reveal); The Center for Public Integrity; The Daily Beast Company LLC; Dow Jones & Company,

[1] Pursuant to Rule 37.6, amici affirm that no counsel for a party authored this brief in whole or in part, and that no person other than amici, their members, or their counsel made a monetary contribution to fund its preparation or submission. Counsel of record for both parties have consented to the filing of this brief.

Inc.; The E.W. Scripps Company; First Amendment Coalition; Freedom of the Press Foundation; Gannett Co., Inc.; Hearst Corporation; Injustice Watch; International Documentary Association; Investigative Reporting Workshop at American University; Investigative Studios; Los Angeles Times Communications LLC; The Media Institute; MediaNews Group Inc.; MPA – The Association of Magazine Media; National Freedom of Information Coalition; National Press Photographers Association; The New York Times Company; The News Leaders Association; Newsday LLC; Online News Association; POLITICO LLC; Quartz Media, Inc.; Radio Television Digital News Association; Reuters News & Media, Inc.; The Seattle Times Company; Society of Environmental Journalists; Society of Professional Journalists; TIME USA, LLC; Tribune Publishing Company; Tully Center for Free Speech; Univision Communications Inc.; Vice Media Group; and The Washington Post.

Amici are media organizations with an interest in ensuring that federal criminal laws such as the Computer Fraud and Abuse Act are not construed so broadly that they impede newsgathering by dissuading sources from disclosing information that is important for an informed electorate or by deterring journalists from engaging in essential journalistic activity, thereby chilling speech and press activity protected by the First Amendment.

SUMMARY OF ARGUMENT

Amici agree with petitioner's interpretation of Section 1030(a)(2) of the Computer Fraud and Abuse Act. Amici submit this brief to highlight the serious constitutional concerns posed by the more expansive interpretation adopted by the court of appeals. That interpretation is unconstitutionally vague and significantly chills speech and press activity protected by the First Amendment.

The Court should adopt the narrower interpretation advanced by petitioner because it avoids those constitutional infirmities.

Impermissibly vague laws violate due process and the separation of powers. A law is unconstitutionally vague if it fails to give fair notice, invites arbitrary enforcement, or impermissibly delegates the task of defining criminal conduct to someone other than the legislature. Application of the vagueness doctrine is especially stringent when overly broad laws threaten to infringe First Amendment freedoms.

The expansive interpretation of Section 1030(a)(2) adopted by the court of appeals is unconstitutionally vague and significantly chills protected First Amendment activity. That interpretation implicates the due process and separation-of-powers concerns protected by the vagueness doctrine because it criminalizes a virtually limitless range of ordinary computer and Internet conduct by means of incorporating private terms of service, which often impose restrictions based on a user's purpose. That interpretation invites arbitrary enforcement, fails to give sufficient notice of what conduct is criminal, and impermissibly delegates the decidedly legislative task of defining criminal conduct to third parties—especially because employers and website owners can easily change their terms of service at any time.

The court of appeals' interpretation also chills ordinary journalistic activity protected by the First Amendment. It thwarts traditional source-journalism activity because it deters would-be government sources and corporate whistleblowers from coming forward with newsworthy information. And when sources are not deterred, that interpretation opens the door to criminal liability for journalists themselves under broad theories of conspiracy

or other inchoate crimes. It could also apply to web scraping, an increasingly common data-journalism technique that relies on automation to pull large amounts of information from websites, with the perverse result that investigative activity that is perfectly acceptable in the analog world is criminal when conducted more efficiently online. A looming threat of criminal liability would significantly deter the use of web-scraping techniques and deprive the public of the valuable information that can be gleaned from it.

Given the constitutional infirmities plaguing the court of appeals' interpretation of Section 1030(a)(2), the Court should embrace the narrower interpretation advanced by petitioner, consistent with the Court's practice of adopting narrower constructions of criminal statutes when overly broad alternatives pose constitutional concerns. The judgment of the court of appeals should be reversed.

ARGUMENT

THE COMPUTER FRAUD AND ABUSE ACT'S PROHIBITION ON EXCEEDING UNAUTHORIZED ACCESS SHOULD BE CONSTRUED NARROWLY TO AVOID SERIOUS CONSTITUTIONAL CONCERNS

Section 1030(a)(2) of the Computer Fraud and Abuse Act provides that whoever "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains * * * information from any protected computer," commits a federal crime. 18 U.S.C. 1030(a)(2)(C). To "exceed[] authorized access" means "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." 18 U.S.C. 1030(e)(6). In this case, the court of appeals broadly construed the phrase "exceeds authorized access" in Section 1030(a)(2) to encompass a person who has permission to

access certain information but uses that information for a purpose that is improper under the terms of use imposed by a third party.

While amici agree with petitioner that the court of appeals' expansive interpretation contravenes the plain text and history of the CFAA, see Pet. Br. 17-26, amici submit this brief to highlight the serious constitutional concerns posed by that interpretation. Because the court of appeals' interpretation is unconstitutionally vague and would significantly chill speech and press activity protected by the First Amendment, the Court should reject it and instead adopt the narrower interpretation advanced by petitioner.

A. Overly Broad Criminal Statutes Implicating The First Amendment Are Subject To Particularly Stringent Application Of The Vagueness Doctrine

1. It is a familiar principle that a statute is void for vagueness if it "is so vague that it fails to give ordinary people fair notice of the conduct it punishes, or so standardless that it invites arbitrary enforcement." *Johnson* v. *United States*, 135 S. Ct. 2551, 2556 (2015) (citation omitted).

With its concern for fair notice, the vagueness principle is a "basic principle of due process." *Grayned* v. *City of Rockford*, 408 U.S. 104, 108 (1972). But vague laws also "undermine the Constitution's separation of powers and the democratic self-governance it aims to protect" by "hand[ing] responsibility for defining crimes" to someone other than the legislature, thereby "eroding the people's ability to oversee the creation of the laws they are expected to abide." *United States* v. *Davis*, 139 S. Ct. 2319, 2325 (2019); see Peter W. Low & Joel S. Johnson, *Changing the Vocabulary of the Vagueness Doctrine*, 101 Va. L. Rev. 2051, 2053 (2015) (identifying an "antidelegation" principle in the Court's vagueness decisions).

2. This Court has made clear that a "more stringent vagueness test" applies when overly broad laws "threaten[] to inhibit the exercise of constitutionally protected rights," such as "the right of free speech." *Village of Hoffman Estates* v. *Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 499 (1982); see, *e.g.*, *Kolender* v. *Lawson*, 461 U.S. 352, 358 (1983). As commentators have long recognized, the vagueness doctrine serves as an "insulating buffer zone of added protection at the peripheries" of First Amendment freedoms. Anthony G. Amsterdam, *The Void-for-Vagueness Doctrine in the Supreme Court*, 109 U. Pa. L. Rev. 67, 75 (1960); see *id.* at 75 n.40 (collecting cases).

B. The Expansive Interpretation Adopted By The Court Of Appeals Is Unconstitutionally Vague And Would Significantly Chill First Amendment Activity

The court of appeals' expansive interpretation of Section 1030(a)(2) of the CFAA implicates the vagueness doctrine on multiple levels. It does not provide fair notice of what conduct is criminal, invites arbitrary enforcement, and delegates to third parties the decidedly legislative task of defining criminal conduct. And because that interpretation covers such a wide range of conduct, it threatens to criminalize a significant amount of ordinary journalistic activity, thereby chilling essential speech and press activity protected by the First Amendment.

1. The Court Of Appeals' Interpretation Implicates The Due Process and Separation-of-Powers Concerns Protected By The Vagueness Doctrine

The overly broad interpretation of Section 1030(a)(2) adopted by the court of appeals effectively delegates the task of defining criminal conduct to employers, website owners, and other third parties—incorporating their computer-use policies and terms of service into the federal

criminal code. In so doing, the court of appeals' interpretation does not provide fair notice of what conduct is criminal and invites arbitrary enforcement.

a. The court of appeals' interpretation would render a virtually limitless swath of ordinary computer and Internet conduct criminal, depending on what happens to be covered by the particular terms of private policies.

In the workplace, for example, the court of appeals' interpretation would criminalize even employees' "minor dalliances," such as "[]chatting [online] with friends, playing games, shopping[,] or watching sports highlights," because those and other non-business activities are routinely prohibited by employers' computer-use policies. *United States* v. *Nosal*, 676 F.3d 854, 860 (9th Cir. 2012) (en banc). And because those policies often draw lines on the basis of an employee's purpose—rather than conduct itself—employees could risk criminal liability when they use work computers for non-business purposes, such as sending a personal note from a work e-mail account or searching for a birthday gift on a work Internet browser. That renders virtually every employee who uses a work computer a criminal, given that even the best of employees use their computers for personal reasons "dozens or even hundreds of times" per day. Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 Minn. L. Rev. 1561, 1585 (2010) (Kerr).

While prosecutions for such conduct may be unlikely, the threat of criminal prosecution nonetheless gives employers significant power. Those that want to rid themselves of bothersome employees need only identify a violation of the computer-use policy and then "threaten to report them to the FBI unless they quit." *Nosal*, 676 F.3d at 860.

Outside the workplace, the court of appeals' expansive interpretation creates the potential for criminal liability

for any Internet user who violates a website's written terms of service—as the government has argued on multiple occasions. See, *e.g.*, Dkt. 2, *United States* v. *Swartz*, Crim. No. 11-10260 (D. Mass. July 14, 2011); *United States* v. *Lowson*, Crim. No. 10-144, 2010 WL 9552416, at *7 (D. N.J. Oct. 12, 2010); *United States* v. *Drew*, 259 F.R.D. 449, 467 (C.D. Cal. 2009). That is especially troubling because websites' terms of service often use broad and indefinite language to forbid a wide range of ordinary activity, such as the blanket prohibition on posting "bad stuff" that was at one point included in YouTube's terms. See David A. Puckett, *Terms of Service and the Computer Fraud and Abuse Act: A Trap for the Unwary?*, 7 Okla. J. L. & Tech. 53, at 20 (2011).

b. A construction of the CFAA so broad as to incorporate private terms of service or computer-use policies implicates the due process and separation-of-powers concerns that the vagueness doctrine protects. It invites arbitrary enforcement by effectively "giv[ing] the government the ability to arrest anyone who regularly uses the Internet," since there is no textual basis in the CFAA for intelligibly criminalizing only certain violations of terms of service but not others. Kerr 1582. And because private companies can change their website's terms of service at any time and for any reason, behavior that was not criminal at the time Congress enacted Section 1030(a)(2) can be made criminal by private policy—without any action by Congress. That not only fails to provide sufficient notice of criminal conduct, but also impermissibly delegates the distinctly legislative task of defining criminal conduct to third parties such as private employers and website owners. See *Davis*, 139 S. Ct. at 2326; see also Low & Johnson 2053; Note, *The Vagaries of Vagueness: Rethinking the CFAA as a Problem of Private Nondelegation*, 127 Harv. L. Rev. 751, 768-771 (2013).

Contrary to the government's suggestion, moreover, the current Department of Justice charging policy does not "ameliorate[]" those concerns. Br. in Opp. 16-17. That policy merely states that a federal prosecution under the CFAA "may not be warranted" if certain atextual "factors" are not present. See Memorandum from the Attorney General to United States Attorneys and Assistant Attorneys General for the Criminal and National Security Divisions, Intake and Charging Policy for Computer Crime Matters 1, 4-5 (Sept. 11, 2014). Such discretionary language—which the government could unilaterally modify at any point—does not meaningfully restrain prosecutorial authority. Even if it did, it would not solve the vagueness problem inherent in the court of appeals' interpretation of Section 1030(a)(2): because the statute itself "prescribes the rule to govern conduct and warns against transgression," *Lanzetta* v. *New Jersey*, 306 U.S. 451, 453 (1939), an overly broad statutory interpretation cannot be saved "on the assumption that the Government will 'use it responsibly.'" *Marinello* v. *United States*, 138 S. Ct. 1101, 1109 (2018) (quoting *McDonnell* v. *United States*, 136 S. Ct. 2355, 2372-2373 (2016)).

2. The Court Of Appeals' Interpretation Chills First Amendment Activity

The court of appeals' interpretation is so broad that it could sweep in ordinary journalistic activity that is essential to the newsgathering process. If that interpretation is permitted to stand, it would significantly chill the exercise of speech and press rights protected by the First Amendment, dramatically altering the way in which government officials and corporate whistleblowers relate to the press, the means by which the press gathers and reports the news, and the degree of newsworthy information ultimately made available to the public.

a. The Court Of Appeals' Interpretation Criminalizes Traditional Newsgathering Activity

The court of appeals' interpretation would significantly chill First Amendment activity by criminalizing traditional source-journalism activity.

i. Journalists have long depended on their relationships with government sources and corporate whistleblowers in order to obtain information in the public interest. See William E. Lee, *Deep Background: Journalists, Sources, and the Perils of Leaking*, 57 Am. U. L. Rev. 1453, 1518 (2008) (Lee); Michael J. Borden, *The Role of Financial Journalists in Corporate Governance*, 12 Fordham J. Corp. & Fin. L. 311, 329-331 (2007) (Borden). The most successful political journalists are "master[s]" at building relationships with government officials and employees. Lee 1518. And corporate whistleblowers "play an important role in funneling journalists toward appropriate targets of investigation." Borden 331.

Consistent with that reality, Congress has never thought it necessary or appropriate to enact a criminal statute aimed at ensuring official or corporate secrecy or to punish press leaks. That is because our democratic system—in which the "people are sovereign," *Buckley* v. *Valeo*, 424 U.S. 1, 14 (1976)—places limits on the government's power to enforce a system of official secrecy. As this Court has stated, "[t]ruth may not be the subject of either civil or criminal sanctions where discussion of public affairs is concerned," because such speech is "the essence of self-government." *Garrison* v. *Louisiana*, 379 U.S. 64, 74-75 (1964). And the mere fact that a source may have obtained information illegally is insufficient to impose criminal liability on the journalist who shares such information with the public. See, *e.g.*, *Bartnicki* v. *Vopper*, 532 U.S. 514, 535 (2001).

ii. Because Congress never intended the CFAA to limit the dissemination of information to the press—much less the publication of such information by the press—it is not worded to reflect the First Amendment concerns that must be addressed to impose criminal liability in that area. As a result, the court of appeals' interpretation of Section 1030(a)(2) would significantly chill speech by threatening to criminalize a substantial amount of ordinary journalistic behavior without offering any guidance to those who wish to exercise their First Amendment rights.

If this Court were to embrace that expansive interpretation, the number of government and corporate-whistleblower sources available to journalists would significantly drop. Because a violation of an employer's computer-use policy constitutes a crime under that interpretation and such a violation would occur virtually any time a potential source were to use a work computer to access information for a non-business reason—*i.e.*, any time a source is acting as a source—such an interpretation would strongly deter potential sources from coming forward with newsworthy information. See pp. 6-7, *supra*.

Even if it would not deter sources, moreover, a broad interpretation of Section 1030(a)(2) could significantly chill speech by opening the door to criminal liability for journalists themselves. Under broad theories of conspiracy or other inchoate crimes, journalists who have cultivated strong relationships with their sources could be prosecuted for any violations of the CFAA committed by their sources. Cf. Lee 1515-1520 (describing similar risk with broad interpretations of the Espionage Act).

Suppose, for example, that petitioner in this case—a state employee—had disclosed the results of his license-plate-number search not to a government informant, but instead to a journalist. Perhaps he and the journalist had

built a friendship centered around some issue of public concern, and he concluded that the seemingly harmless activity of running the search for the journalist would lead to an article in the public interest. Petitioner's conduct would nonetheless fall within the reach of a broadly construed CFAA. And if the journalist had engaged in conversations with petitioner that could be understood as encouraging him to conduct the search for that non-business purpose, the journalist would risk facing a conspiracy charge under a broadly construed CFAA.[2]

Under the court of appeals' interpretation, then, a CFAA conspiracy charge could lie against any journalist who received information from a source who obtained that information from a computer that the source was authorized to use on the ground that the source obtained the information with an improper purpose. In addition to chilling speech, that prospect opens the door to selective enforcement of members of the press. As petitioner notes, the fact that "federal law enforcement officials consider[ed] the CFAA fodder for devising sting operations" in this case illustrates that the court of appeals' overly broad construction invites selective enforcement. See Br. 38-39. That is especially concerning in the context of the press, where selective enforcement could be motivated by

[2] To be clear, amici take no position on whether the alleged conduct in this case—the misuse of a law enforcement database for personal reasons and alleged private gain—could be made criminal. As petitioner notes, however, laws prohibiting the use of government databases for an improper purpose will ordinarily articulate that improper purpose as the trigger for liability. Br. 19; see, *e.g.*, 10 U.S.C. 923(a)(1)-(2). The only question here is whether *this* law, as written, can be construed so broadly as to encompass a computer user who accesses information he is entitled to access but does so for an improper reason. Amici also do not dispute that the CFAA encompasses actual hacking, as appropriately defined.

a government official's disagreement or dislike of the substance of the journalism. Cf. *Nieves* v. *Bartlett*, 139 S. Ct. 1715, 1727 (2019) (expressing concerns about selective enforcement of those engaged in First Amendment activity in the context of arrests).

b. The Court Of Appeals' Interpretation Encompasses New Data-Journalism Techniques

The court of appeals' interpretation would also apply to increasingly used data-journalism techniques, with the perverse result that certain investigative conduct that is perfectly acceptable in the analog world would be criminal when done more efficiently online. That further risks chilling First Amendment activity, curbing the development of those data-journalism techniques and depriving the public of important information gained from their use.

i. Data journalists and researchers now frequently engage in various forms of web scraping—the automated pulling of large amounts of information from websites—or similar techniques. Web scraping typically does not reveal any information beyond what could be found through the manual use of the website; its chief advantage is that it "speeds up the tedious job of manually copying and pasting data into a spreadsheet, making large-scale data collection possible." Jacquellena Carrero, Note, *Access Granted: A First Amendment Theory of Reform of the CFAA Access Provision*, 120 Colum. L. Rev. 131, 137 (2020) (Carrero). As the amount of data available online has substantially increased, journalists are increasingly turning to these techniques. Indeed, data journalism is "now a driving force in newsrooms around the country." D. Victoria Baranetsky, *Data Journalism and the Law*, Tow Center for Digital Journalism (Sept. 19, 2018) <tinyurl.com/datajournalismandthelaw> (Baranetsky).

Web scraping serves First Amendment values, at least when the information sought serves the public interest. For example, journalists have used web-scraping techniques to identify doctors nationwide that have continued to practice after being caught sexually abusing patients—a reporting feat that was not practically feasible through traditional means. See Carrie Teegardin, *Behind the Scenes: How the Doctors & Sex Abuse Project Came About*, Atlanta Journal-Constitution (Dec. 17, 2016) <tinyurl.com/sexabuseproject>. Web-scraping techniques have been used to evaluate prison conditions. See David Eads, *How (and Why) We're Collecting Cook County Jail Data*, ProPublica (July 24, 2017) <tinyurl.com/cookcountyjaildata>. Those techniques have also been employed to reveal to the public that the National Park Service had removed from its website "politically inconvenient environmental information related to efforts to reduce carbon emissions." Carrero 146. And an ongoing journalism project identifying new or changed missing-person cases relies on daily web scraping to keep it updated. See Baranetsky.

Perhaps most significantly, web scraping and other techniques have been used for civil-rights testing that has exposed unlawful discrimination on the Internet. See, *e.g.*, Noa Yachot, *Your Favorite Website Might Be Discriminating Against You*, ACLU (June 29, 2016) <tinyurl.com/favoritewebsitediscriminating>. There is growing evidence that websites are discriminating on the basis of race, sex, and other protected classes. See, *e.g.*, Executive Office of the President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights* 11-19 (May 2016) <tinyurl.com/reportonalgorithms>. In order to expose such discrimination, investigative journalists create test accounts that vary on the basis of race or sex

and aggregate data to compare the offers displayed to the various accounts.

Using those techniques, journalists have uncovered and reported on discrimination in a variety of contexts. For example, journalists have used web-scraping techniques to show that The Princeton Review, a test preparation-services company, imposed a "tiger mom tax" by listing higher prices for its services in geographic areas with large Asian populations. See Julia Angwin et al., *The Tiger Mom Tax: Asians Are Nearly Twice as Likely to Get a Higher Price from Princeton Review*, ProPublica (Sept. 1, 2015) <tinyurl.com/tigermomtax>. Similar techniques have revealed that Airbnb hosts are less likely to accept potential guests with "black-sounding names," as compared to those with distinctly "white-sounding names." See Komal S. Patel, Note, *Testing the Limits of the First Amendment: How Online Civil Rights Testing Is Protected Speech Activity*, 118 Colum. L. Rev. 1473, 1474-1475 (2018) (Patel). Web-scraping techniques have also exposed patterns of racial discrimination in a risk-assessment component of the prison-parole process used by many States. Jeff Larson et al., *How We Analyzed the COMPAS Recidivism Algorithm*, ProPublica (May 23, 2016) <tinyurl.com/compasrecidivism>.

ii. The broad interpretation of the CFAA adopted by the court of appeals would criminalize web scraping and similar techniques any time a website's terms of service include a blanket prohibition on web scraping, collecting data, or using the website for research purposes. Many terms of service do so. See Carrero 134; Patel 1475, 1494. And others could do so at any point in the future, leaving the task of deciding whether the use of increasingly commonplace data-journalism techniques constitutes a federal crime up to private website owners. See p. 8, *supra*.

As a result, the "looming threat" of criminal liability "deter[s]" web-scraping activity and "cause[s] journalists to withhold stories." Carrero 164-165. Indeed, "[s]everal independent journalists and newsrooms" have "declined to publish stories for fear of liability under the CFAA." Baranetsky.

The chilling effect is especially concerning when it comes to ensuring compliance with federal and state anti-discrimination laws. See, *e.g.*, *Havens Realty Corp.* v. *Coleman*, 455 U.S. 363, 373 (1982). The 1988 amendments to the Fair Housing Act, which empowered the Department of Housing and Urban Development to investigate and punish housing discrimination, directly resulted from a landmark journalism series that showed systematic redlining in the context of housing loans. See Bill Dedman, *The Color of Money*, Atlanta Journal-Constitution (May 1-4, 1988). If that series had instead run today, the journalists "would undoubtedly have thought about using [web] scraping" and dummy online accounts "to build [their] lending datasets." Gabe Rottman, *Knight Institute's Facebook 'Safe Harbor' Proposal Showcases Need for Comprehensive CFAA Reform*, Reporters Committee for Freedom of the Press (Aug. 6, 2018) <tinyurl.com/cfaasafeharbor>. Yet doing so would risk criminal liability under the court of appeals' expansive interpretation of Section 1030(a)(2), with the perverse result that journalistic conduct that was praised in the analog world is now criminal when done online.

That will not cut it from the perspective of the First Amendment. The court of appeals' interpretation of Section 1030(a)(2) threatens to criminalize a wide range of ordinary journalistic activity without offering any means of guarding journalists' First Amendment freedoms—raising the prospect that the "freedom of the press could be eviscerated." *Branzburg* v. *Hayes*, 408 U.S. 665, 681

(1972). And the chilling of journalistic activity will also have concomitant chilling effects on the public discourse resulting from that activity.

C. The Court Should Construe The Statute Narrowly To Avoid Constitutional Concerns

The Court could easily avoid the constitutional infirmities plaguing the court of appeals' expansive interpretation of Section 1030(a)(2) by adopting petitioner's proposed construction instead.

When one of two "plausible statutory constructions" of a federal statute "would raise * * * constitutional problems, the other should prevail." *Clark* v. *Martinez*, 543 U.S. 371, 380-381 (2005); see, *e.g.*, *Jennings* v. *Rodriguez*, 138 S. Ct. 830, 842 (2018). The Court need not resolve the constitutional question itself; it need only undertake a "narrow inquiry" into whether one reading "presents a significant risk" that a constitutional right "will be infringed." *NLRB* v. *Catholic Bishop of Chicago*, 440 U.S. 490, 502 (1979). That principle is even stronger when applied to ambiguous criminal statutes, because the rule of lenity "requires" such statutes "to be interpreted in favor of the defendants subjected to them." *United States* v. *Santos*, 553 U.S. 507, 514 (2008) (plurality opinion); see *Marinello*, 138 S. Ct. at 1106-1107.

Accordingly, when faced with potentially vague and overly broad federal criminal statutes, this Court has consistently construed them narrowly to avoid the constitutional issue. See, *e.g.*, *Skilling* v. *United States*, 561 U.S. 358, 405-406, 410-411 (2010); *United States* v. *Kozminski*, 487 U.S. 931, 949-950, 952 (1988); *Screws* v. *United States*, 325 U.S. 91, 102-103 (1945). Indeed, the "normal[] result" for "vagueness challenges to a federal law" in this Court is a "narrowing interpretation" that makes "the vague-

ness problem go away." Low & Johnson 2096. That comports with the historical roots of the vagueness doctrine, which developed from the "rule of construction" that "penal statutes are to be construed strictly in favor of the accused." Note, *Indefinite Criteria of Definiteness in Statutes*, 45 Harv. L. Rev. 160, 160 n.2 (1931).

The Court should therefore adopt the narrower interpretation of Section 1030(a)(2) advanced by petitioner. That interpretation is plainly plausible. And unlike the court of appeals' interpretation, it avoids "criminaliz[ing] a broad range of day-to-day activity," including a significant amount of First Amendment activity; posing a significant "risk of arbitrary or discriminatory prosecution and conviction"; and effectively "delegat[ing]" the "inherently legislative task of determining what type of * * * activities are so morally reprehensible that they should be punished as crimes." *Kozminski*, 487 U.S. at 949.

CONCLUSION

The judgment of the court of appeals should be reversed.

Respectfully submitted.

BRUCE D. BROWN
KATIE TOWNSEND
GABRIEL ROTTMAN
REPORTERS COMMITTEE FOR
FREEDOM OF THE PRESS
1156 15th Street, N.W.,
Suite 1020
Washington, DC 20005

KANNON K. SHANMUGAM
JOEL S. JOHNSON
PAUL, WEISS, RIFKIND,
WHARTON & GARRISON LLP
2001 K Street, N.W.
Washington, DC 20006
(202) 223-7300
kshanmugam@paulweiss.com

AMANDA C. WEINGARTEN
PAUL, WEISS, RIFKIND,
WHARTON & GARRISON LLP
1285 Avenue of the Americas
New York, NY 10019

JULY 2020