No. 19-783

In the Supreme Court of the United States

NATHAN VAN BUREN,

Petitioner,

v.

UNITED STATES,

Respondent.

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

BRIEF OF TECHNOLOGY COMPANIES AS AMICI CURIAE IN SUPPORT OF PETITIONER

Mark A. Lemley
Counsel of Record
Aditya V. Kamdar
Annie A. Lee
DURIE TANGRI LLP
217 Leidesdorff Street
San Francisco, CA 94111
(415) 362-6666
mlemley@durietangri.com

Counsel for Amici Curiae

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

Cases

Other Authorities

INTEREST OF AMICI CURIAE[1]

Amici are technology companies that are actual or potential targets of computer hacking and have a strong interest in effective cybersecurity. We have an interest in making sure that the law encourages effective computer security. We have no interest in the specific outcome of this case.

Atlassian's products help teams organize, discuss, and complete their work in a coordinate, efficient and modern fashion. Organizations use Atlassian's project tracking, content creation and sharing, and real-time communication and service management products to work better together and deliver quality results on time.

Mozilla Corporation is a global, mission-driven organization that works with a worldwide community to create open source products like its web browser Firefox. Its mission is guided by a set of principles that recognizes, among other things, that individuals' security and privacy on the Internet are fundamental and must not be treated as optional.

Shopify Inc. is a leading global commerce company, providing Internet-based software tools to help start, grow, and manage a retail business of any size. Shopify strongly believes in the value of an open and secure Internet, and businesses use Shopify's

---

[1] All parties have consented to the filing of this brief. Amici state that no counsel for a party authored this brief in whole or in part, and no person or entity, other than amici or their counsel, made a monetary contribution to the preparation or submission of this brief.

software in part because Shopify takes issues of security and privacy seriously.

SUMMARY OF THE ARGUMENT

Amici are technology companies that are actual or potential targets of computer hacking and have a strong interest in effective cybersecurity. We are the intended beneficiaries of a law like the Computer Fraud and Abuse Act (CFAA). But we are concerned that overbroad readings of the CFAA, like the one given by the Eleventh Circuit, hurt rather than help computer security.

Amici recognize that computer intrusion attempts are inevitable. Effective computer security thus entails creating systems that are resilient to computer hackers. That requires letting people, including members of the robust community of independent security researchers, probe and test our computer networks. Indeed, many companies, like amici, offer "bug bounty" programs where we offer financial rewards for external researchers who find vulnerabilities in our systems so we can improve them.

An overbroad reading of the CFAA, however, chills this critical security research. Security experts may not think it worth the risk to conduct their research without a clear definition of what it means to "exceed authorized access," especially when mere terms of service violations have been used to impose criminal penalties in the past. Under the Eleventh Circuit's interpretation, security experts, typically non-lawyers, fear they may access a computer system they thought they were permitted to access, but did so for a purpose that turns out to exceed the bounds of a company's terms of service.

Some companies, including amici, have taken steps to prevent this chilling effect, offering "safe harbors" to computer researchers who expose vulnerabilities in our systems. In so doing, amici authorize people to probe into our computer systems. But because the CFAA is a criminal statute, not just a civil tort, the fact that companies welcome security testing by experts does not prevent a zealous prosecutor from bringing a criminal case.

The CFAA should not be interpreted in a way that undermines rather than enhances computer security. Coupled with a real risk of criminal liability, an overbroad reading of the CFAA will drive—indeed, has driven—security researchers underground, discouraging them from testing and reporting vulnerabilities in computer systems at all.

ARGUMENT

I. Security research is becoming increasingly important, and it requires the participation of outside experts.

As every segment of our society becomes increasingly connected, all companies are becoming technology companies. Car manufacturers are now in the business of creating computers on wheels. Grocery stores collect troves of shopper data. Even household appliances are becoming voice-activated by default. With this shift comes a fast-growing need for robust consumer privacy, system integrity, and cybersecurity—especially at a time when data breaches have increasingly serious consequences. In the last few years alone, critical online systems—from credit agencies to hospital systems to social networks—have been exploited to devastating effect. As a result, today's businesses must devote significant attention and resources toward building and maintaining system security and consumer privacy. For many companies, including amici, security makes up a sizeable portion of their budgets.

Modern computer systems are so complex that no company can hire enough security engineers to identify every possible vulnerability that might lie in its software—or in the interactions between its own software and third-party software, which is also constantly evolving. Just as a city must rely on motorists to report potholes because it cannot monitor every road every day, companies like amici must rely on external users to report bugs and vulnerabilities that their security staff may not catch. Companies

like amici, nonprofits, and even the government itself have thus turned to the robust independent security research community to probe and prod our systems.[2] We believe that collaborating openly with many experts and creating a mechanism for responsible disclosure of vulnerabilities will lead to more fruitful results—and, ultimately, more secure systems.

These external security researchers rely on common testing techniques—for example, automatically collecting (or "scraping") data, reverse engineering software, or creating fake accounts—in order to discover vulnerabilities (or "bugs") and investigate whether companies' systems work as intended. But because many company terms of service generally prohibit these commonly used techniques, security researchers may violate the literal terms of the CFAA unless they are otherwise authorized.[3]

---

[2] While this brief focuses on companies, we note that other organizations, including government agencies, have implemented bug bounty programs. For example, the Department of Defense has a highly successful bug bounty. *U.S. Dep't of Defense*, HackerOne, https://hackerone.com/deptofdefense (last updated Nov. 21, 2016).

[3] *See*, for example, Facebook's Terms of Service, which does not allow a researcher to "access or collect data from [Facebook] Products using automated means" and requires users to use "the same name that you use in everyday life" when setting up their one allowed account, ostensibly barring research accounts. *Terms of Service*, Facebook, https://www.facebook.com/terms.php (last updated July 31, 2019). Google "reserves the right to suspend or terminate your

II. Companies, including amici, use bug bounty programs to welcome external security research that would otherwise violate their terms of service.

Some companies, including the undersigned, have taken steps to actively welcome this independent security research. These companies have created "bug bounty" programs, offering financial rewards for researchers who discover and disclose flaws in their systems. One amicus, Shopify, implemented its bug bounty program in 2013. Hundreds of hackers have since participated, leading to the resolution of over 1,000 reported flaws and over $1 million in awarded bounties.[4] Indeed, much of Shopify's current security team started out as independent researchers who disclosed vulnerabilities to the company.

Many vulnerabilities disclosed through bug bounty programs are consequential. For instance, in 2018, amicus Shopify disclosed that it was able to fix a serious bug reported by an independent researcher

---

access" or "delete your Google Account" if they "reasonably believe your conduct causes harm . . . to a user, third party, or Google – for example, by hacking . . . misleading others, or scraping content that doesn't belong to you." *Terms of Service*, Google, https://policies.google.com/terms?hl=en-US (last updated March 31, 2020).

[4] Pete Yaworski, *What Shopify Has Learned From Five Years of Bug Bounty Programs*, Cyberscoop (May 5, 2020), https://www.cyberscoop.com/shopify-bug-bounty-five-years/.

through its bounty program.[5] Shopify operates an online ecommerce platform used by over a million businesses around the world. Security vulnerabilities on Shopify—like many other centralized platforms—therefore have the potential to have an outsized effect. In that one instance, the bug discovered could have enabled a malicious actor to take over a key aspect of Shopify's underlying infrastructure. What could have become a serious data breach, possibly exposing the private information of countless online businesses and consumers, was instead reported by an independent researcher and fixed within hours.

Today, hundreds of companies have bug bounty programs, reflecting widespread recognition that effective computer security requires some level of external testing.[6] *See generally* Andreas Kuehn & Milton Mueller, *Analyzing Bug Bounty Programs: An Institutional Perspective on the Economics of Software Vulnerabilities*, 42nd Telecomms. Policy Research Conf. (Sep. 13, 2014). As devices, personal information, and interactions become increasingly interconnected, this ability to crowdsource security

---

[5] Sean Michael Kerner, How Shopify Avoided a Data Breach, Thanks to a Bug Bounty, eWeek (Dec. 17, 2018), https://www.eweek.com/security/how-shopify-avoided-a-data-breach-thanks-to-a-bug-bounty.

[6] For a list of bug bounty programs, see Public Bug Bounty List, BugCrowd, https://www.bugcrowd.com/bug-bounty-list/ (including 23andme, Airbnb, Alibaba, AT&T, Coinbase, Facebook, Github, Goldman Sachs, Google, Ikea, Lyft, Massachusetts Institute of Technology, Medium, Nvidia, Pinterest, Starbucks, Tencent, Twitter, United Airlines, and Walmart, among many others) (last visited July 2, 2020).

efforts will only become more essential to ensuring the health of our online systems.

III. Under a broad reading of the CFAA, a company's authorization of security research does not eliminate the risk of criminal liability.

This ability for companies like amici to meaningfully engage with independent researchers, however, is at risk under the Eleventh Circuit's broad interpretation of "exceeds authorized access" in the CFAA—an interpretation that increases the risk of criminal liability for security researchers even where companies welcome external research.

Many companies with bug bounty programs include contractual language that offers a "safe harbor" for bona fide security investigations. For instance, amicus Mozilla includes a safe harbor in its bug bounty program that promises: "As long as you comply with this [bug bounty] policy, [w]e consider your security research to be 'authorized' under the Computer Fraud and Abuse Act."[7] Amici Atlassian and Shopify both have language similarly authorizing bug bounty participants to engage in security testing.[8] The growing list of companies with safe harbors shows that companies have recognized the potential for beneficial behavior to violate the broad

---

[7] *Security Bug Bounty Program*, Mozilla, https://www.mozilla.org/en-US/security/bug-bounty/ (last visited July 5, 2020).

[8] *Atlassian*, BugCrowd, https://bugcrowd.com/atlassian (last visited July 5, 2020); *Shopify*, HackerOne, https://hackerone.com/shopify (last updated May 8, 2020).

interpretation of the CFAA, and have taken important steps to prevent charges from being brought against the researchers they rely on.

But even where a company has made an affirmative effort to implement a bug bounty program with a safe harbor, there is still a real risk an outside security expert will face criminal liability. Indeed, the Department of Justice's own policy guidance setting out a framework for companies' bug bounty programs and safe harbors notes that these actions will "substantially reduc[e]"—but not eliminate—"the likelihood that such described activities will result in a civil or criminal violation" of the CFAA.[9]

This is not a hypothetical threat. The government has shown that it can and will bring criminal cases based on a mere terms of service violation, even if the company didn't ask it to. For instance, in *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009), prosecutors charged and a jury convicted a defendant of a CFAA misdemeanor based solely on the defendant's creation of a fake MySpace account in violation of MySpace's terms of service.[10]

---

[9] U.S. Dep't of Just., Computer Crime & Intellectual Property Section Criminal Div., *A Framework for a Vulnerability Disclosure Program for Online Systems* (July 2017), https://www.justice.gov/criminal-ccips/page/file/983996/download.

[10] Judge Wu ultimately granted the defendant's motion for judgment of acquittal, holding that a conviction under the CFAA based only on defendant's intentional violation of a terms of service would violate the void-for-vagueness doctrine. *See also United States v. Valle*, 807 F.3d 508, 528 (2d Cir. 2015) ("While

Similarly, in *United States v. Auernheimer*, 748 F.3d 525 (3d Cir. 2014), security researcher Andrew "Weev" Auernheimer was sentenced to 41 months in prison for exposing a security hole in AT&T's iPads. Auernheimer discovered that the devices would automatically provide a user's email address when connected to AT&T's website, thereby enabling anyone to obtain the pairing of a user's email address to their device. In that case, the government did not argue that Auernheimer's scraping of AT&T's website violated the company's terms, but instead alleged that Auernheimer's actions were unauthorized because AT&T would not have provided the information if asked, even though such information was publicly available.[11]

The unfortunate takeaway for researchers from cases like *Drew* and *Auernheimer* is that as long as the CFAA imposes criminal liability premised on violations of company policies, written or not, private companies cannot guarantee that researchers who test their systems will not be prosecuted. Further, what companies think is ordinary testing behavior may well look like malicious hacking to a prosecutor unversed in computer security. As one legal scholar explains, "a simple port scan, a basic operation used

---

the Government might promise that it would not prosecute an individual for checking Facebook at work, we are not at liberty to take prosecutors at their word in such matters.").

[11] After serving 41 months, Auernheimer's conviction was vacated for improper venue, though the court in a footnote expressed doubt that Auernheimer was ever guilty of accessing "without authorization, or in excess of authorization." *Id.* at 534 n.5.

to learn about services running on a computer and entryways into the system, could lead to prosecution under the CFAA. While this is clearly absurd in the eyes of security researchers, law enforcement authorities may not have the same perspective." Ido Kilovaty, *Freedom to Hack*, 80 Ohio St. L.J. 455, 510 (2019). Thus, even when companies like amici provide an exception in the form of a safe harbor, researchers may not think it is worth pursuing security research when terms of service violations have been used to impose criminal penalties in the past. This lower participation results in a less secure online ecosystem, putting private data and key infrastructure at risk.

The Eleventh Circuit's per-use, intent-based approach to the CFAA exacerbates this problem because it requires an inquiry into the defendant's motivation for *any* action, large or small, that is alleged to exceed authorized access. A single request for data could constitute an independent instance of access. At such a fine level of granularity, even the most dutiful researcher is likely to perform *some* action whose "purpose" could be interpreted as violating a terms of service—for example, researching Facebook under an alias rather than using "the same name that you use in everyday life." Indeed, the search for a vulnerability can stretch across multiple days, weeks, or even months, and many security researchers are full-time bug hunters. It is thus practically impossible to avoid all risk of inadvertently running afoul of some company's terms of service in the opinion of some prosecutor.

IV. The CFAA's uncertainty creates an untenable situation for security researchers.

This chilling effect from the risk of criminal liability is further compounded because security researchers (usually non-lawyers) typically decide whether to take on the legal risk that accompanies research without seeking legal counsel. Often, they rely on their own interpretations of a company's terms of service and safe harbor, and conflicting resources about the CFAA fail to provide clarity for researchers seeking a yes or no answer.[12] Security researchers are therefore left to interpret an area of law where lawyers, scholars, and courts themselves cannot agree on what constitutes authorized access, and where a broad interpretation creates a real risk of criminal liability. *See* Jonathan Mayer, *Cybercrime Litigation*, 164 U. Pa. L. Rev. 1453 (2016) (documenting the disagreements among the circuits about how to interpret the CFAA).

In such an area where the bounds of criminal law are uncertain, even bug bounty programs and safe harbors cannot soothe security researchers' fear of criminal prosecution. One cautionary tale is the

---

[12] *See, e.g.*, Kate Conger, *New Study Makes Clear Just How Risky It Is to Be a Security Researcher*, GIZMODO (Apr. 10, 2018, 8:30 AM), https://gizmodo.com/new-study-makes-clear-just-how-risky-it-is-to-be-a-secu-1825116053. *See also* Kim Zetter, *The Most Controversial Hacking Cases of the Past Decade*, Wired (Oct. 26, 2015), https://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/; Tim Wu, *Fixing the Worst Law in Technology*, New Yorker (Mar. 18, 2013), https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology.

case of Voatz, a mobile voting application that enables overseas and military voters to vote via smartphone. Late last year, the U.S. Attorney for the Southern District of West Virginia revealed that an FBI investigation was ongoing after a student from a University of Michigan election security course tried to investigate Voatz.[13] At the time that the student attempted to access the Voatz app, Voatz was part of a bug bounty program organized through San Francisco company HackerOne, and offered $2,000 for the discovery of critical vulnerabilities. Voatz included a safe harbor policy, which stated:

> Any activities conducted in a manner consistent with this policy will be considered authorized conduct and *we will not initiate legal action against you*. If legal action is initiated by a third party against you in connection with activities conducted under this policy, we will take steps to make it known that your actions were conducted in compliance with this policy.[14]

---

[13] Kevin Collier, *FBI investigating if attempted 2018 voting app hack was linked to Michigan college course*, CNN (Oct. 5, 2019), https://www.cnn.com/2019/10/04/politics/fbi-voting-app-hack-investigation/index.html.

[14] Yael Grauer, *Safe Harbor, or Thrown to the Sharks by Voatz,* Magazine by CoinTelegraph (Feb. 7, 2020), https://cointelegraph.com/magazine/2020/02/07/safe-harbor-or-thrown-to-the-sharks-by-voatz (emphasis added).

Nevertheless Voatz reported the attempted "intrusion" to authorities and told journalists that the student's actions were "out of scope" for the bug bounty program because they were on Voatz's "live election system."[15] Public commentators later revealed, however, that Voatz had only updated its terms to prohibit attempts to disrupt a "live election system" *after* the criminal investigation had already begun.[16]

In 2018, the Center for Democracy & Technology published a study on security research in which they analyzed the chilling effects of the CFAA by interviewing 20 security researchers.[17] Aside from identifying several instances of actual chilling, the form of the study's conclusion is telling in itself. The authors explain that though they initially set out to

---

[15] Collier, *supra* note 13. Although no charges have been filed, even contemplating the potential for criminal charges can be a harrowing experience for potential defendants who might need to retain attorneys and respond to FBI warrants. Kendra Albert, a Lecturer on Law at Harvard Law School, has voiced concerns of deterrence from the Voatz incident: "An investigation, even if it ends positively without charges, is a life-altering, totally consuming experience. . . . Turning [students] over to the FBI when there's every indication that they're doing good-faith security research consistent with your bug bounty policy is just inappropriate." Grauer, *supra* note 14.

[16] Grauer, *supra* note 14.

[17] Joseph Lorenzo Hall & Stan Adams, *Taking the Pulse of Hacking: A Risk Basis for Security Research*, Ctr. for Democracy & Tech. (Mar. 2018), available at https://cdt.org/insights/taking-the-pulse-of-security-research/ (hereinafter CDT Study).

"better define what a code of conduct for security research might look like," as the project progressed, "it became clear that no unified code of conduct could easily apply" because the boundaries set by the CFAA "are constantly in flux, changing in response to the developing, accepted, and rejected practices."[18] Instead of laying out a code of conduct, the study provided a "risk basis" that identified lower- and higher-risk methods of performing common security research activities.[19] The study warned that because researchers could not eliminate all legal risk under the CFAA, researchers must rely on "a variety of signals to *manage* risk of legal threats."[20] Even where there were express policies governing access, the study also found that researchers could not "be certain how much legal weight those limits carry," meaning "the perceived degree of risk . . . varied from subject to subject."[21]

The CDT report confirmed that an overbroad reading of the CFAA will drive—and has driven—research further underground and toward anonymous or public disclosure. Indeed, many researchers already choose to disclose the vulnerabilities they discover through an intermediary to preserve their anonymity.[22] As Professor Kilovaty aptly put it, "[t]he CFAA's strict liability for access

---

[18] CDT Study, at 16–17.

[19] CDT Study, at 16-24.

[20] CDT Study, at 22 (emphasis added).

[21] CDT Study, at 10.

[22] CDT Study, at 12.

without authorization is certainly a major threat to security researchers [and] discourages talented researchers from engaging responsibly with [companies]."[23]

Amici, as beneficiaries of security research, believe a narrow and clear reading of the CFAA is necessary to encourage researchers to act responsibly and disclose to companies vulnerabilities they find so they can be fixed. The current law does not provide that certainty.

[23] Kilovaty, *supra* p. 13, at 509.

CONCLUSION

Companies like amici rely on external researchers to improve the security of their systems. But a lack of clarity around the CFAA's definition of "exceeds authorized access" chills security researchers from engaging in this critical work, especially when a broad reading of the statute creates criminal liability for mere violations of terms of service. For these reasons, the Court should reverse the Eleventh Circuit's interpretation of the CFAA and construe criminal liability for computer intrusion in a way that does not threaten legitimate security research.

Respectfully submitted,

Mark A. Lemley
Counsel of Record
Aditya V. Kamdar
Annie A. Lee
DURIE TANGRI LLP
217 Leidesdorff Street
San Francisco, CA 94111
(415) 362-6666
mlemley@durietangri.com

Counsel for Amici Curiae

Date: July 8, 2020