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 ELEVENTH
CIRCUIT

BRIEF OF VOATZ, INC., AS *AMICUS CURIAE* IN SUPPORT OF RESPONDENT IN AFFIRMANCE OF THE DECISION BELOW

JARED L. HUBBARD
(*Counsel of Record)*
FITCH LAW PARTNERS LLP
One Beacon Street
Boston, MA 02108
(617) 542-5542
jlh@fitchlp.com

Counsel for Amicus Curiae
Voatz, Inc.

Dated: September 3, 2020

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

CASES

STATUTES

OTHER AUTHORITIES

boosts-its-payouts/d/d-id/1335322 (last accessed last accessed August 26, 2020)..............................5

Bugcrowd Pays Out a Half Millions Dollars to Whitehat Hackers in One Week! (November 8, 2019), https://www.bugcrowd.com/blog/bugcrowd-pays-out-a-half-million-dollars-to-whitehat-hackers-in-one-week/ (last accessed August 26, 2020)..5

Crowdsourced Security and Bug Bounty Adoption is Spreading (May 20, 2019), https://appdevelopermagazine.com/crowdsourced-security-and-bug-bounty-adoption-is-spreading/ (last accessed August 26, 2020)..............................5

HackerOne Customer Terms And Conditions https://www.hackerone.com/terms (last accessed Sept 1, 2020) 4-5

How Google handles security vulnerabilities, https://www.google.com/about/appsecurity/ (last accessed September 2, 2020))............................14

Ng, Alfred, *US officials hope hackers at Defcon find more voting machine problems*, CNET (August 10, 2018), https://www.cnet.com/news/us-officials-hope-hackers-at-defcon-find-more-voting-machine-problems/ (last accessed August 26, 2020)... 7-8

Specter, Michael A., et al., *The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used In U.S. Federal Elections* (2020), https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf (last accessed September 2, 2020) 9

The #WeHeartHackers Initiative https://wehearthackers.org (last accessed August 26, 2020) 8

United States Attorney Mike Stuart Issues Statement on Election Security (October 1, 2019), https://www.justice.gov/usao-sdwv/pr/united-states-attorney-mike-stuart-issues-statement-election-security (last accessed September 1, 2020). 11

U.S. Department of Defense Concludes Third "Hack the Air Force" Bug Bounty Challenge with HackerOne to Improve Cybersecurity (Dec. 20, 2018), https://www.hackerone.com/blog/100-million-paid-one-billion-sight-hackers (last accessed August 26, 2020) 6

Voatz Response to Flawed Report (February 13, 2020), https://blog.voatz.com/?p=1209 (last accessed August 26, 2020). 9

Voatz Security Issue Disclosure Policy, https://blog.voatz.com/?p=1278 (last accessed August 26, 2020) 4

Warner, Andrew "Mac," *WV Secretary of State to Deter Threats Against Election Systems and Processes* (October 2, 2019), https://sos.wv.gov/news/Pages/10-2-2019-A.aspx (last accessed September 1, 2020)................ 10-11

INTEREST OF AMICUS CURIAE[1]

Amicus Curiae is Voatz, Inc. ("Voatz"), a for-profit company running a mobile election voting application using blockchain technology. Voatz's platform has been designated as critical infrastructure by the United States Department of Homeland Security,[2] and the Voatz application has been successfully used in 70 elections, including 11 state and municipal elections. Voatz's mission is to make voting not only more accessible and secure, but also more transparent, auditable and accountable. Voatz's technology makes voting easier for persons with disabilities, and for overseas voters such as military personnel stationed abroad.

As a company responsible for designing and operating critical infrastructure for our democracy, Voatz has a significant interest in maintaining the security of its application and software, which it does through techniques involving controlling authorized access to its systems, and prohibiting unauthorized access.

[1] Pursuant to Supreme Court Rule 37.6, counsel for *amicus* states that no counsel for a party authored this brief in whole or in part, and that no person other than *amicus* or their counsel made a monetary contribution to the preparation or submission of this brief. Pursuant to Supreme Court Rule 37.2, both parties have consented to the filing of this *amicus* brief.

[2] *Statement by Secretary Jeh Johnson on the Designation of Election Infrastructure as a Critical Infrastructure Subsector* (January 6, 2017), https://www.dhs.gov/news/2017/01/06/statement-secretary-johnson-designation-election-infrastructure-critical (last visited August 26, 2020).

CORPORATE DISCLOSURE STATEMENT

Voatz, Inc., is a for-profit organization based in Boston, Massachusetts. A publicly held company, Overstock.com, Inc., owns more than 10% of its stock through a wholly-owned subsidiary. Voatz has no parent company, and no other publicly held company owns 10% or more of its stock.

INTRODUCTION

Voatz writes in support of the Respondent in opposing the Petitioner's effort to narrow the meaning of the Computer Fraud and Abuse Act (CFAA). Contrary to the argument of some *amici*, particularly the Computer Security Researchers, Electronic Frontier Foundation, et al. ("the Computer Researchers"), no narrowing of the CFAA is necessary in order to ensure the security of computer applications and systems by permitting unauthorized "independent research." Rather, the necessary research and testing can be performed by *authorized* parties. These include private consulting firms and participants in organized "bug bounty" programs. Voatz's own security experience provides a helpful illustration of the benefits of authorized security research, and also shows how unauthorized research and public dissemination of unvalidated or theoretical security vulnerabilities can actually cause harmful effects. The Court should therefore affirm the decision below and uphold the plain meaning of the CFAA.

ARGUMENT

I. A BROAD READING OF "EXCEEDS AUTHORIZED ACCESS" IN THE CFAA WILL NOT HAVE A DELETERIOUS EFFECT ON COMPUTER SECURITY.

Voatz agrees fully with the Computer Researchers that security research is vital, especially for entities like Voatz that create and provide services that are in the public interest. Indeed, as noted above, the Voatz application along with other election systems has been designated as critical infrastructure by the US government. Other entities with this designation include banks, electricity grids, and dam operators. All such entities require their systems to be completely secure.

Voatz meets the applicable subset of requirements for United States voting systems, according to Pro V&V, an independent, federally-certified Voting System Test Laboratory (VSTL). Pro V&V recently completed comprehensive testing of the Voatz system. In a lengthy report, Pro V&V concluded that the Voatz platform "meets the applicable requirements set forth for voting systems" in the U.S. Election Assistance Commission (EAC) 2015 Voluntary Voting System Guidelines (VVSG), Version 1.1, subject to recommendations contained in the report.

Voatz's security program, which is typical of programs run by many other critical infrastructure operators, employs three principal methods.

First, Voatz takes account of extensive feedback given to it by its testing laboratories (such as Pro V&V), and uses that feedback to address potential vulnerabilities.

Second, Voatz retains two reputable internet security firms as consultants, and follows the recommendations of those firms. As is common in the internet security field, the consultants' services include conducting simulated "attacks" on the Voatz platform, informing Voatz about any vulnerabilities that may have been discovered, and making recommendations about how to fix those vulnerabilities.

Third, Voatz conducts "bug bounty" programs, in which registered participants are incentivized, and given permission, to explore vulnerabilities in its platform and report them. Voatz was, in fact, the first elections company to conduct such a program in 2018. Currently these programs are organized by Voatz itself, but in the past some were conducted through a vendor such as HackerOne Inc.

None of these methods – engagement of testing laboratories, employment of security consultants, and participating in bug bounty programs – requires a narrow construction of the CFAA in order to continue. This is because no matter what reading is given to the term "exceeds authorized access" as used in 18 USC §1030(a)2)(C), all of the methods are permitted. In the case of Voatz' testing laboratory and its consulting firms, this is by contract. In the case of bug bounty programs, participants' activities are specifically permitted by the bug bounty program terms.[3]

[3] *See Voatz Security Issue Disclosure Policy*, https://blog.voatz.com/?p=1278 (last accessed August 26, 2020);

Contrary to the arguments in the Computer Security Researchers' *amicus* brief, bug bounty programs are highly effective. They are extremely widespread in the technology industry, and even outside that industry, one survey in 2019 reported that 42 percent of companies outside of the technology industry were running a crowdsourced cybersecurity program, and another 24 percent were expecting to run one within the next year.[4] The rewards offered in bug bounty programs similarly increased by 83% in 2019 when compared to the past year, creating the environment for "more bug bounty programs launching" and "increased hacker engagement."[5]

see also HackeOne Customer Terms And Conditions, https://www.hackerone.com/terms (last accessed Sept 1, 2020).

[4] *Crowdsourced security and bug bounty adoption is spreading* (May 20, 2019), https://appdevelopermagazine.com/crowdsourced-security-and-bug-bounty-adoption-is-spreading/ (last accessed August 26, 2020).

[5] *Bug Bounties Continue to Rise as Google Boosts its Payouts* (July 23, 2019), https://www.darkreading.com/vulnerabilities---threats/bug-bounties-continue-to-rise-as-google-boosts-its-payouts/d/d-id/1335322 (last accessed August 26, 2020); *see also Bugcrowd Pays Out a Half Millions Dollars to Whitehat Hackers in One Week!* (November 8, 2019), https://www.bugcrowd.com/blog/bugcrowd-pays-out-a-half-million-dollars-to-whitehat-hackers-in-one-week/ (last accessed August 26, 2020).

Voatz notes that the recent growth of these programs makes the survey data reported by the Computer Researchers outdated. *See* Computer Researchers' *amicus* brief, p. 30 (citing 2018 data).

One of the companies that organize such programs, HackerOne, estimates that it has paid over $100 million as of May 2020 to participants in its programs.[6] To the extent such payments represent a rough proxy for the value to HackerOne's customers (such as Voatz in prior years), these programs are clearly valuable and effective.

Further illustrating the value of bug bounty programs, the United States Department of Defense (DoD) is a regular participant. The DoD first engaged HackerOne in the "Hack the Pentagon" program in 2016, and a series of such events followed. HackerOne states that over 5,000 vulnerabilities have been identified as part of these events.[7] In announcing Hack the Air Force 3.0 in 2018, a US Air Force official stated: "It's critical to allow these researchers to uncover vulnerabilities in Air Force websites and systems, which ultimately strengthens our cybersecurity posture and decreases our vulnerability surface area."[8]

[6] *$100 Million Paid – One Billion in Sight for Hackers* (May 27, 2020), https://www.hackerone.com/blog/100-million-paid-one-billion-sight-hackers (last accessed August 26, 2020).

[7] *118 Fascinating Facts From HackerOne's Hacker-Powered Security Report 2018* (Aug. 27, 2018), https://www.hackerone.com/blog/118-Fascinating-Facts-HackerOnes-Hacker-Powered-Security-Report-2018 (last accessed Sept. 1, 2020).

[8] *U.S. Department of Defense Concludes Third "Hack the Air Force" Bug Bounty Challenge with HackerOne to Improve Cybersecurity* (Dec. 20, 2018), https://www.businesswire.com/news/home/20181220005150/en/

Indeed, most of the incidents of helpful, independent research cited in the Computer Researchers' *amicus* brief constitute "authorized" activity, such that they will continue to take place no matter the outcome of this Court's construction of the CFAA. For example:

- In 2012, independent researchers tested the functionality and security of the Washington D.C. Board of Election and Ethics system in a mock election.[9] This event was by invitation, and authorized. (See Computer Researchers' *amicus* brief, p. 10)
- In 2018, officials from United States Department of Homeland Security asked hackers at the Defcon cybersecurity conference to take on voting machines and expose vulnerabilities, and further invited them to engage in conversations to discuss security.[10] (See Computer Researchers' *amicus* brief, p. 11).

U.S.-Department-Defense-Concludes-%E2%80%9CHack-Air-Force%E2%80%9D (last accessed Sept 1, 2020).

[9] Wolchok, Scott, et al., *Attacking the Washington, D.C. Internet Voting System at 1-2, Proc. 16th Conf. on Fin. Cryptography & Data Security* (February 2012), *available at* https://jhalderm.com/pub/papers/dcvoting-fc12.pdf (last accessed August 26, 2020).

[10] Ng, Alfred, *US officials hope hackers at Defcon find more voting machine problems*, CNET (August 10, 2018), https://www.cnet.com/news/us-officials-hope-hackers-at-defcon-

- In 2019, the United States Food and Drug Administration (FDA) launched the "We Heart Hackers" medical device challenge, whereby ten medical device makers pledge high-trust collaboration with the security researcher community, and these industry partners provided security researchers with more than thirty medical devices and shared information to learn adversary tactics and improve security approaches.[11] This challenge was organized by the FDA, and the research was authorized by the participating device makers. (See Computer Researchers' *amicus* brief, p. 12).

The instances of "independent research" involving Voatz discussed in the Computer Researchers' brief offer a perfect example of why authorized security research is preferable to research using unauthorized access to the nation's critical infrastructure.

The Computer Researchers cite a paper published by researchers at MIT as an example of beneficial research which revealed vulnerabilities in the Voatz application (Computer Researchers' *amicus* brief, p. 11). However, the researchers in question did not discover any practically exploitable security flaws in the actual Voatz application. Instead, the

find-more-voting-machine-problems/ (last accessed August 26, 2020).

[11] *The #WeHeartHackers Initiative*, https://wehearthackers.org (last accessed August 26, 2020).

researchers were analyzing a version of the Voatz voting application that was several versions out of date at the time, and that was never authorized for use in any election. Further, as the researchers admitted, they were never able to get access to the Voatz servers using this outdated application. This meant that the researchers were unable to register as a legitimate voter, unable to test or pass the layers of identity checks required to verify a legitimate voter, unable to receive a legitimate ballot, and unable to submit any votes or change any voter data. Instead, the researchers fabricated an imagined version of the Voatz servers, hypothesized how they would likely work, and then made assumptions about the interactions between the system components that turned out to be false.[12] In other words, by conducting their activities on an unauthorized basis rather than through Voatz authorized bug bounty program or direct collaboration with Voatz, the researchers rendered their own findings relatively useless. This stands in sharp contrast to *authorized* research on voting machines (for instance the 2018 Department of Homeland Security Event cited by the Computer Researchers), which results in helpful feedback to system operators.[13]

[12] Michael A. Specter, et al., *The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used In U.S. Federal Elections* (2020), https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf (last accessed September 2, 2020); *see also Voatz Response to Flawed Report* (February 13, 2020), https://blog.voatz.com/?p=1209 (last accessed August 26, 2020).

[13] *See supra*, note 10.

The Computer Researchers also cite a news account claiming that Voatz reported two college students to the Federal Bureau of Investigations. (Computer Researchers' *amicus* brief, p. 24). That account is at least partially inaccurate, in that Voatz made no report to the FBI or any other federal authority. Rather, Voatz reported the students' unauthorized attempts to access its systems to its customer, the State of West Virginia, because the students' ill-advised activity was indistinguishable from a hostile attack and the students did not seek any prior authorization privately or through Voatz's public bug bounty program. It is a standard practice for technology companies to report attack attempts to their clients and Voatz is contractually required to report such potential attacks during live elections – the same way an electric company would be required to report an attack on an electric grid to state and federal authorities, or a dam operator would be required to report an attack on software that monitors and operates dams to authorities such as the Army Corps of Engineers. Officials in West Virginia, in their discretion and independent of Voatz, then chose to refer the matter to the FBI.[14] To Voatz's knowledge, no one was prosecuted.

[14] Warner, Andrew "Mac," *WV Secretary of State to Deter Threats Against Election Systems and Processes* (October 2, 2019), https://sos.wv.gov/news/Pages/10-2-2019-A.aspx (last accessed September 1, 2020) ("In last year's election, we detected activity that may have been an attempt to penetrate West Virginia's mobile voting process. No penetration occurred and the security protocols to protect our election process worked as designed. The IP addresses from which the attempts were made have been turned over to the FBI for investigation. The investigation will determine if crimes were committed."); *see also United States Attorney Mike Stuart Issues Statement on Election Security*

Regardless of the particulars, however, the West Virginia incident illustrates the harm caused by attacking, or "researching," critical infrastructure without proper access or authorization especially in the middle of an election. Because it is impossible for an organization to know in real-time the identity or motives of those attempting to exceed authorized access to their systems, they must treat every student "researcher" the same as they would a Russian hacker.[15] Even though the West Virginia incident demonstrates that the defenses built into the Voatz system worked as designed, this imposes significant additional costs on organizations operating our nation's critical infrastructure, who must monitor and report any improper attempts to access that infrastructure and now also try to distinguish between good-faith attempts versus malicious attempts. It also drains the resources of governmental authorities who receive reports of possibly hostile attacks and must spend valuable time and resources investigating them. The harm caused to public confidence in our electoral processes is immense.

The Petitioner and Computer Researchers wish to make such "research" attempts – where a user

(October 1, 2019), https://www.justice.gov/usao-sdwv/pr/united-states-attorney-mike-stuart-issues-statement-election-security (last accessed September 1, 2020).

[15] Zetter, K., *How Close Did Russia Really Come to Hacking the 2016 Election?*, Politico (December 26, 2019), https://www.politico.com/news/magazine/2019/12/26/did-russia-really-hack-2016-election-088171 (last accessed August 26, 2020).

knowingly exceeds their authorized access to a computer system – broadly legal. This would undoubtedly result in a significant increase in such unauthorized hacking. In the context of a live election, having both computer security experts and governmental authorities need to address numerous hacking attempts by "researchers" would distract from any actual threat. It would be far better to have legitimate researchers help to improve security as part of an authorized program as determined by the organization and its ultimate customers.

Moreover, violating terms and policies in order to conduct research upends reasoned expectations companies and organizations have when they create and publish such terms and policies. Setting conditions for access to computer systems created and maintained at great expense is just as reasonable as having conditions for entry onto physical premises. A nuclear power plant may offer tours to the public, but if a member of a tour group goes beyond that limited authorized access and attempts to sneak into the control room, they can be prosecuted for trespass. The same is true for virtually every other piece of physical critical infrastructure, whether it be banks, airports, or military bases. These physical locales frequently allow access to certain individuals either for limited purposes or to limited areas. Exceeding such limitations is a criminal offense. *See State ex rel. Qarmout v. Cavallo*, 774 A.2d 612, 614 (N.J. App. Div. 2001) ("[C]onduct in violation of the terms of a license to enter property can support a charge of criminal trespass even though the entry was initially permissible."); *see also Miller v. State*, 109 Ark. 362, 159 S.W. 1125, 1126 (1913) ("While they had the right of ingress and egress to the inclosure for the purposes specified in the reservation of the deeds, they had no right there for any other purpose, and therefore [when they exceeded the specified purposes,] they were guilty of the trespass and misdemeanor denounced by the statute."). As the Government points out in its briefing, in the similar context of property theft, it is well accepted that a theft can occur by exceeding one's consent or authority over the property (including as an agent, bailee, trustee, or fiduciary). See Respondent's Brief at 32-33.

In essence, the Computer Researchers ask this Court to narrow the CFAA to protect everyone who attempts to attack applications and websites without authorization or exceeds their authorized use, in order to provide a safe harbor for those like themselves who do so with good intentions. But this is a request that should be addressed to Congress, not this Court. Congress certainly knows how to create safe harbors within statutory frameworks, including in statutes governing activities on the internet. For example, the Digital Millennium Copyright Act (DMCA) contains a safe harbor provision for internet service providers which protects them from liability if they meet certain specific requirements (e.g., establishing procedures for taking down infringing material on demand). *See* 17 USC §512. The CFAA might similarly be amended to protect independent researchers who meet certain requirements (e.g., reporting vulnerabilities directly to system operators so that they can address them within a reasonable timeframe, and refraining from interfering with live systems). Absent such an amendment to the statute, however, the Court should not create a giant loophole in the CFAA which protects not only "white hat" researchers, but malicious attackers as well.

Even well-intentioned unauthorized researchers may actually increase the practical threats to our nation's critical infrastructure if any identified vulnerabilities are not properly handled. If a security vulnerability is widely disseminated publicly and prematurely, it can expose software platforms and their users to malicious attacks, as ill-intentioned hackers can take advantage of such vulnerabilities prior to the development of any patch. That is why the technology industry has adopted standards that allow a software developer a 60-90 day window to adequately examine or validate security vulnerabilities and, if necessary, develop a patch.[16] Compliance with such standards, however, is voluntary, and researchers sometimes publicize potential security vulnerabilities before they can be validated or any fix can be developed, putting our nation's critical infrastructure at risk.[17]

[16] *See, e.g.*, *How Google handles security vulnerabilities*, https://www.google.com/about/appsecurity/ (last accessed September 2, 2020) (noting that Google has a 90-day disclosure policy for security vulnerabilities identified for its vendors).

[17] Voatz's experience with the MIT researchers, discussed above, shows the potential danger of simply relying on the good intentions of unauthorized researchers. Once they had identified potential vulnerabilities, the MIT researchers demanded contact information for all of Voatz customers under threat of going immediately to the press. Although Voatz cooperated and shared contact information for its clients, four days later the researchers' findings were published by the New York Times. The MIT researchers – due to the nature of their research on an earlier version of Voatz's application and without successfully accessing Voatz's servers – had not uncovered any practically exploitable security flaws in Voatz's system. But had they found any practically exploitable security vulnerabilities and published them in the midst of an ongoing election, such

The Computer Researchers are candid about the problems which would be created by their position. As they state, "Almost by its nature, discovering security vulnerabilities requires accessing computers in a manner unanticipated by computer owners, frequently in contravention of the owners' stated policies." Computer Researchers' *amicus* brief, pg. 19. But researchers who are sophisticated enough to conduct such activities are also sophisticated enough to know where to find and read the terms and policies that will govern those activities. While the Computer Researchers portray themselves as under threat of being victimized for inadvertently tripping over a restriction, the reality is different: they wish to be free to deliberately infiltrate a live system in violation of readily accessible terms, openly publish any results obtained, and be immune from being intercepted or reported for doing so. There is simply no rationale for such freedom where, as described above, security research can occur using processes already in place in coordination with organizations or their customers.

In the case of critical government infrastructure, companies such as Voatz are very willing to have researchers participate in improving the security of their systems, including through bug bounty programs and collaborative research incorporating coordinated vulnerability disclosure programs. Customers, including state and federal governments, can also get involved in such testing, as

unauthorized research and its premature public disclosure would have significantly increased the opportunity for malicious actors to interfere in our elections.

the Department of Homeland Security has done. Or Congress can provide a safe harbor to authorize and regulate such security research. But this Court need not artificially narrow the CFAA in order to accomplish this objective.

CONCLUSION

For all the foregoing reasons, Voatz respectfully requests that this Court affirm the decision below.

Respectfully submitted,

JARED L. HUBBARD
(*Counsel of Record)*
FITCH LAW PARTNERS LLP
One Beacon Street
Boston, MA 02108
(617) 542-5542
jlh@fitchlp.com

Counsel for *Amicus Curiae*
Voatz, Inc.

Dated: September 3, 2020