Response to Voatz's Supreme Court Amicus Brief

September 14, 2020

On September 3, 2020, Voatz — a blockchain voting company with a publicly documented track record of hostility towards security research[1] — filed an amicus brief with the U.S. Supreme Court in *Van Buren v. United States* arguing in favor of a broad interpretation of the Computer Fraud and Abuse Act (CFAA), the federal anti-hacking law enacted in 1986.[2,3] Voatz's amicus brief repeatedly refers to independent good-faith security research as a threat to cybersecurity and glosses over harmful effects to security research that would result from an overbroad CFAA.

As representatives of the security community, including pioneers of coordinated vulnerability disclosure, bug bounties, and election security, it is our opinion that Voatz's brief to the Court fundamentally misrepresents widely accepted practices in security research and vulnerability disclosure, and that the broad interpretation of the CFAA threatens security research activities at a national level. We stand in support of the petitioner, reiterating arguments made by the Computer Security Researchers, Electronic Frontier Foundation, et al.,[4] Orin S. Kerr,[5] Technology Companies,[6] and many others advocating a narrow interpretation of the CFAA in which contractual violations do not constitute CFAA violations.

Security research is vital to the public interest.

We benefit from security research in nearly every aspect of our lives. From crucial work exposing vulnerabilities in technologies ranging from election systems[7] to medical devices[8] and automobiles,[9] it is clear security research has tangibly improved the safety and security of systems we depend upon. It is not a given that this vital security work will continue. A broad interpretation of the CFAA would magnify existing chilling effects, even when there exists a societal obligation to perform such research.

Coordinated vulnerability disclosure (CVD) is a standard, widely adopted practice in which the public may engage in the process of security research and safely report vulnerabilities to organizations. Under CVD, researchers give organizations a reasonable set timeframe to fix a vulnerability before disclosing it publicly; organizations in turn agree to consider such activities authorized and not take legal action against such research. Hundreds of private sector entities,[10,11] including leading technology companies and election vendors,[12] as well as government organizations including the U.S. Department of Defense[13] and the U.S. Securities and Exchange Commission,[14] operate vulnerability disclosure programs to provide a channel for receiving vulnerability reports from security researchers and authorize such testing. A recent directive from the Cybersecurity and Infrastructure Security Agency (CISA) has adopted these best practices, requiring every federal civilian executive branch agency to establish a vulnerability disclosure program authorizing security research against their live internet-accessible systems.[15]

Vulnerability disclosure policies and bug bounties help mitigate, but do not solve, the broader chilling effects of the law toward security research. As we explore below, a company claiming to offer safe harbor through a vulnerability disclosure policy may still take legal action against security researchers. Likewise, under a broad interpretation of the CFAA, a failure to comply with any component of a vulnerability disclosure policy would itself constitute a contractual violation, and hence a CFAA violation, even if the policy specifically authorizes testing. Even when a company abides by its vulnerability disclosure policy's safe harbor, that promise only binds the company itself.[16] The reach of that protection is insufficient since security research can often involve a company's vendors or third-party services. The fact that the Department of Justice has provided guidance on establishing vulnerability disclosure programs[17] and acknowledged that the CFAA remains an issue for conducting good-faith security research on systems[18] (research that is otherwise authorized under the Digital Millennium Copyright Act, or DMCA[19]) only further exemplifies the difficult reality of navigating the CFAA. Individual companies should not need to address these intricacies when seeking to authorize testing on their systems.

Voatz acts in bad faith towards coordinated vulnerability disclosure.

There is great irony in the fact that Voatz's own interactions with researchers highlight the need for CFAA reform; Voatz's actions demonstrate how firms are not necessarily incentivized to behave well. A firm acting in bad faith should not subject a good-faith researcher to legal action.

In coordinated vulnerability disclosure, both parties agree to play by established rules in order to improve the state of security, and Voatz has not followed the rules of its own policies. In 2019, as acknowledged by the company in its court brief, Voatz referred a student security researcher to state authorities for what its CEO alleged was "unauthorized activity."[20] Voatz took this action despite purporting to offer a safe harbor as part of its bug bounty program, which stated at the time of the student's testing that "[a]ny activities conducted in a manner consistent with this policy will be considered authorized conduct and we will not initiate legal action against you."[21] Shortly after news of this incident became public, Voatz retroactively updated its safe harbor to disallow the student's activity.[22]

In Voatz's amicus brief, the company states that it reported the student to state authorities because they "did not seek any prior authorization privately or through Voatz's public bug bounty program."[23] In truth, Voatz's public bug bounty program authorized any member of the public to report vulnerabilities to Voatz without needing to seek prior authorization.

Many signatories of this letter have operated and participated in public bug bounty programs, in both the private sector and government. We can attest that requiring researchers to obtain prior authorization for a public bug bounty program is non-standard and discourages participation. In March, HackerOne (a signatory of this letter) removed Voatz from its bug bounty platform, citing Voatz's failure to act in "good faith" towards researchers.[24] This marked the first time in the platform's history that a company was removed.[25]

A security assessment of Voatz published by MIT researchers in February is a model example of coordinated vulnerability disclosure.[26] The researchers took care not to enter legal gray areas, only reverse engineering the client of the Voatz app. After discovering a slew of worrying vulnerabilities, the researchers followed standard coordinated disclosure procedures, working with CISA to disclose and then giving Voatz adequate time to fix the vulnerabilities identified before publicly releasing the research. Despite a report by the independent security firm Trail of Bits (a signatory of this letter), commissioned by Voatz, that confirmed the MIT researchers' findings as valid vulnerabilities,[27] Voatz would later dispute both the MIT assessment and the confirmation by Trail of Bits.[28]

Despite the MIT researchers' extensive efforts to perform and disclose their work in good faith, Voatz claims in its brief that the research was conducted "on an unauthorized basis" and that such "unauthorized research and public dissemination of unvalidated or theoretical security vulnerabilities can actually cause harmful effects." To be clear, the MIT team did not need authorization to perform or publish their work, as the research was protected by the 2018 DMCA security research exemption and did not violate the CFAA as no systems owned or operated by Voatz were ever accessed in the course of security testing.[29] In this case, the MIT researchers upheld the principles of coordinated vulnerability disclosure by first disclosing the vulnerability to Voatz. Voatz responded to this act of good-faith coordinated vulnerability disclosure by claiming that the MIT researchers' activities were conducted on an "unauthorized basis," implying that they "knowingly exceed[ed] their authorized access to a computer system."

Voatz's insinuation that the researchers broke the law despite having taken all precautions to act in good faith and respect legal boundaries shows why authorization for this research should not hinge on companies themselves acting in good faith. To companies like Voatz, coordinated vulnerability disclosure is a mechanism that shields the company from public scrutiny by allowing it to control the process of security research. The fact that the MIT researchers discovered vulnerabilities that reflect poorly on Voatz's security only underscores the need for public scrutiny — what is simply a hassle to Voatz is a crucial warning flare to the public.

We support efforts to strengthen security research.

We reiterate our support for the petitioner and the amicus briefs of EFF et al., Orin S. Kerr, Technology Companies, and many others. The work of security researchers is vital to the public interest, and a broad interpretation of the CFAA chills such security research. Voatz's self-interested amicus brief should not be persuasive to this important case; it ignores the overwhelmingly positive and necessary role played by security researchers. If anything, Voatz's role as an elections startup, aiming to support the most crucial function of our democracy, should only further signify the need for public security research of these critical systems.

We must not let Voatz's distorted arguments overshadow many recent advancements in this space. In addition to its directive mandating federal agencies to authorize security research against their systems with a vulnerability disclosure policy, CISA released guidance for election administrators to implement vulnerability disclosure policies.[30] Furthermore, six major voting vendors recently committed to launching vulnerability disclosure policies, signaling their

intentions to repair previously strained relationships with the security community in order to serve the greater public interest in secure elections.[31] The launches in recent weeks of the first-ever vulnerability disclosure policies by a state for election systems[32] and by a voting machine vendor[33] illustrate the rapid pace at which security research and coordinated vulnerability disclosure are becoming normalized.

A broad interpretation of the CFAA risks undoing many of these positive advancements. Voatz's actions threatening good-faith security research are indicative of what may come should the Court decide that a breach of contractual terms constitutes a criminal CFAA violation. We cannot afford to lose the benefits of security research on our digital and physical safety, and our democracy as a whole. Thus, we urge the Court to adopt a narrow interpretation of the CFAA in support of the petitioner.

Signed,

Jack Cable, Independent Security Researcher

Casey Ellis, Chairman/Founder/CTO, Bugcrowd*

Alex Rice, Founder & CTO, HackerOne*

Daniel Guido, Chief Executive Officer, Trail of Bits*

Eric Mill

Riana Pfefferkorn, Stanford Center for Internet and Society

Ben Adida, Executive Director, VotingWorks*

Sergey Alekhnovich, Security Engineer, Latacora

Steven M. Bellovin, Percy K. and Vida L.W. Hudson Professor of Computer Science, Columbia University; affiliate faculty, Columbia Law School

Matthew Bernhard, Research Engineer, VotingWorks*

Matt Bishop, Professor, Department of Computer Science, University of California at Davis

Matt Blaze, McDevitt Professor of Computer Science and Law, Georgetown University

Georgia Bullen, Executive Director, Simply Secure*

Jon Callas, Director of Technology Projects, Electronic Frontier Foundation

Lorrie Cranor, Director and Bosch Distinguished Professor in Security and Privacy Technologies, CyLab Security and Privacy Institute and FORE Systems Professor, Computer Science and Engineering & Public Policy, Carnegie Mellon University

Anil Dewan, Fellow, Aspen Institute's Tech Policy Hub

Cameron Dixon, Policy Technologist, Cybersecurity & Infrastructure Security Agency

Zakir Durumeric, Assistant Professor, Computer Science, Stanford University

Aleksander Essex, Associate Professor, Department of Electrical and Computer Engineering, Western University, Canada

Rik Farrow, Editor, USENIX ;login: magazine

Richard Forno, Senior Lecturer, UMBC & Assistant Director, UMBC Center for Cybersecurity

Alex Gaynor, Chief Information Security Officer, Alloy

Daniel Kahn Gillmor, Senior Staff Technologist, ACLU

Bron Gondwana, CEO, Fastmail Pty Ltd*

Joe Grand, Principal Engineer and Hardware Hacker, Grand Idea Studio, Inc.*

Matthew D. Green, Associate Professor, Computer Science, Johns Hopkins University

Jason Haddix, Head of Security and Risk Management, Ubisoft

J. Alex Halderman, Professor, Computer Science and Engineering, University of Michigan

Joseph Lorenzo Hall, Senior Vice President for a Strong Internet, Internet Society

Leigh Honeywell, CEO, Tall Poppy*

Laurens Van Houtven, Principal, Latacora*

John Hutchison, Security Engineer, Latacora

Philip James, Head of Engineering, Trim

David R. Jefferson, Lawrence Livermore National Laboratory (retired)

Frederic B. Jennings, Cybersecurity & Privacy Attorney

Douglas W. Jones, Associate Professor of Computer Science, University of Iowa

Paul Kehrer, Co-Founder, Fish in a Barrel*

Joseph R. Kiniry, Principal Scientist, Galois and CEO & Chief Scientist, Free & Fair*

Amélie E. Koran, Senior Technology Advocate, Splunk

Susan Landau, Bridge Professor in Cyber Security and Policy, Tufts University

Joshua Maddux, Security Engineer, Latacora

Vitaly McLain, Principal, Latacora

John Menerick, Chief Cyber Security Researcher, Research Something*

Katie Moussouris, Founder and CEO, Luta Security*, coauthor and coeditor of ISO 29147 and 30111 Vulnerability Disclosure and Vulnerability Handling Processes

Mudge, Director and Chairman, Cyber Independent Testing Lab*

Peter G. Neumann, Chief Scientist, SRI International Computer Science Lab

Patrick O'Doherty, Senior Security Engineer, Intercom

Daniela Oliveira, Associate Professor, IoT Term Professor, University of Florida

Lyell C. Read, Member, Oregon State University SSH Lab & Intern, Galois

Alexander (RoRo) Romero, Digital Service Expert & Public Interest Technologist

Jonathan Rudenberg, Chief Technology Officer, Flynn*

Joel Sandin, Principal, Latacora*

Stefan Savage, Professor, Computer Science and Engineering, University of California, San Diego

Andy Sayler, Senior Security Engineer, Twitter

Micah Sherr, Provost's Distinguished Associate Professor, Georgetown University

Barbara Simons, IBM Research (retired)

Michael Skelton, Global Head of Security Operations & Researcher Enablement, Bugcrowd

Kevin Skoglund, President and Chief Technologist, Citizens for Better Elections

Cris Thomas (Space Rogue), IBM X-Force Red Global Strategy Lead

Riad S. Wahby, Security Researcher and PhD Student, Stanford University

Dan S. Wallach, Professor, Computer Science, Rice University

Tarah Wheeler, Belfer Center Cyber Fellow, Harvard University Kennedy School & International Security Fellow, New America

Kenneth White, Security Principal, MongoDB

Chris Wolfe, Senior Security Software Engineer

Sarah Zatko, Chief Scientist, Cyber Independent Testing Lab*

Daniel Zappala, Professor, Brigham Young University

Daniel M. Zimmerman, Principal Researcher, Galois

Philip R. Zimmermann, Associate Professor Emeritus, Cyber Security Group, Delft University of Technology

**Signing on behalf of organization*

Affiliations provided for identification purposes only, except those indicated with an asterisk (*)

[1] “FBI investigating if attempted 2018 voting app hack was linked to Michigan college course”, https://www.cnn.com/2019/10/04/politics/fbi-voting-app-hack-investigation/index.html

[2] “Brief amicus curiae of Voatz, Inc.”, https://www.supremecourt.gov/DocketPDF/19/19-783/153062/20200903122434600_Voatz%20Amicus%20Brief.pdf

[3] “Van Buren v. United States”, https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/19-783.html

[4] “Brief amici curiae of Computer Security Researchers, et al.”, https://www.eff.org/files/2020/07/08/19-783_eff_security_researchers_amici_brief_.pdf

[5] “Brief amicus curiae of Orin S. Kerr”, https://www.supremecourt.gov/DocketPDF/19/19-783/147235/20200708151655215_39887%20pdf%20Kerr.pdf

[6] “Brief amici curiae of Technology Companies”, https://www.supremecourt.gov/DocketPDF/19/19-783/147221/20200708131742277_19-783%20Amici%20Curiae.pdf

[7] “DEFCON 25 Voting Machine Hacking Village Report”, https://www.defcon.org/images/defcon-25/DEF%20CON%2025%20voting%20village%20report.pdf

[8] “FDA informs patients, providers and manufacturers about potential cybersecurity vulnerabilities for connected medical devices and health care networks that use certain communication software”, https://www.fda.gov/news-events/press-announcements/fda-informs-patients-providers-and-manufacturers-about-potential-cybersecurity-vulnerabilities

[9] “Comprehensive Experimental Analyses of Automotive Attack Surfaces”, http://www.autosec.org/pubs/cars-usenixsec2011.pdf

[10] “Public Bug Bounty List”, https://www.bugcrowd.com/bug-bounty-list/

[11] “Bug Bounty Programs”, https://hackerone.com/bug-bounty-programs

[12] “EI-SIG Members’ Vulnerability Disclosure Policies”, https://www.it-isac.org/ei-sig

[13] “DoD Vulnerability Disclosure Program (VDP)”, https://www.dc3.mil/Vulnerability-Disclosure/Vulnerability-Disclosure-Program-VDP/

[14] “SEC Vulnerability Disclosure Policy”, https://www.sec.gov/vulnerability-disclosure-policy

[15] “Binding Operational Directive 20-01”, https://cyber.dhs.gov/bod/20-01/

[16] “A Framework for a Vulnerability Disclosure Program for Online Systems”, https://www.justice.gov/criminal-ccips/page/file/983996/download

[17] Ibid.

[18] “U.S. Department of Justice Letter to U.S. Copyright Office”, https://www.copyright.gov/1201/2018/USCO-letters/USDOJ_Letter_to_USCO.pdf

[19] “Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies”, https://www.federalregister.gov/documents/2018/10/26/2018-23241/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control

[20] “FBI investigating alleged hacking attempt into mobile voting app during 2018 midterms”, https://www.cnn.com/2019/10/01/politics/fbi-hacking-attempt-alleged-mobile-voting-app-voatz/index.html

[21] “Safe Harbor, or Thrown to the Sharks by Voatz?”, https://cointelegraph.com/magazine/2020/02/07/safe-harbor-or-thrown-to-the-sharks-by-voatz

[22] “FBI investigating if attempted 2018 voting app hack was linked to Michigan college course”, https://www.cnn.com/2019/10/04/politics/fbi-voting-app-hack-investigation/index.html

[23] “Brief amicus curiae of Voatz, Inc.”, https://www.supremecourt.gov/DocketPDF/19/19-783/153062/20200903122434600_Voatz%20Amicus%20Brief.pdf. We note that while public reporting indicates that only one student was reported to authorities, Voatz’s brief states that two students were reported.

[24] “Voatz Bug Bounty Kicked Off of HackerOne Platform”, https://cointelegraph.com/news/voatz-bug-bounty-kicked-off-of-hackerone-platform

[25] “HackerOne cuts ties with mobile voting firm Voatz after it clashed with researchers”, https://www.cyberscoop.com/voatz-hackerone-bug-bounty-election-security/

[26] “The Ballot is Busted Before the Blockchain: A Security Analysis of Voatz, the First Internet Voting Application Used in U.S. Federal Elections”, https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf

[27] “Our Full Report on the Voatz Mobile Voting Platform”, https://blog.trailofbits.com/2020/03/13/our-full-report-on-the-voatz-mobile-voting-platform/

[28] “Why experts are overwhelmingly skeptical of online voting”, https://arstechnica.com/tech-policy/2020/09/why-experts-are-overwhelmingly-skeptical-of-online-voting/2/

[29] “Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies”, https://www.federalregister.gov/documents/2018/10/26/2018-23241/exemption-to-prohibition-on-circumvention-of-copyright-protection-systems-for-access-control

[30] “Guide to Vulnerability Reporting for America’s Election Administrators”, https://www.cisa.gov/sites/default/files/publications/guide-vulnerability-reporting-americas-election-admins_508.pdf

[31] “Elections Industry-Special Interest Group (EI-SIG) Two Years of Progress”, https://bit.ly/EISIGPROGRESS

[32] “Ohio becomes first state to release vulnerability policy for election-related websites”, https://www.cyberscoop.com/ohio-vulnerabiility-disclosure-2020-election/

[33] “Top voting vendor ES&S publishes vulnerability disclosure policy”, https://www.cyberscoop.com/ess-election-security-vulnerability-disclosure-black-hat/