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 AMICI CURIAE COMPUTER SECURITY RESEARCHERS, ELECTRONIC FRONTIER FOUNDATION, CENTER FOR DEMOCRACY & TECHNOLOGY, BUGCROWD, RAPID7, SCYTHE, AND TENABLE IN SUPPORT OF PETITIONER

ANDREW CROCKER
Counsel of Record
NAOMI GILENS
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
andrew@eff.org

Counsel for Amici Curiae

296514

COUNSEL PRESS
(800) 274-3321 • (800) 359-6859

TABLE OF CONTENTS

TABLE OF CITED AUTHORITIES

STATUTES

OTHER AUTHORITIES

Page

Ashley Carman, *Nissan Leaf's App Could Let Hackers Run Down Batteries and See Trip Logs*, The Verge (Feb. 24, 2016) 13

Ben Grubb, *Stephane Chazelas: The Man Who Found the Web's 'Most Dangerous' Internet Security Bug*, Sydney Morning Herald (Sept. 27, 2014) 15

Bill Budington, *Ring Doorbell App Packed with Third-Party Trackers*, EFF (Jan. 27, 2020) 22

Brian Krebs, *Hacked Cameras, DVRs Powered Today's Massive Internet Outage*, Krebs on Security (Oct. 21, 2016) 6

Catherine Stupp, *Hackers Change Ransomware Tactics to Exploit Coronavirus Crisis*, Wall St. J. (May 14, 2020). 5-6

CERT Coordination Center, Wikipedia 6

Coders' Rights Project, EFF 25

Commerce Dep't, *International Cybersecurity Priorities: Fostering Cybersecurity Innovation Globally* (June 26, 2017) 8

Computer Security, Wikipedia 1

Dan Goodin, *More than 11 million HTTPS websites imperiled by new decryption attack*, Ars Technica (Mar. 1, 2016) .15

Page

Darren Pauli, *Talk revealing p0wnable surveillance cams pulled after legal threat*, The Register (Oct. 8, 2015) 24

David E. Sanger, *et al.*, *Amid Pandemic and Upheaval, New Cyberthreats to the Presidential Election*, N.Y. Times (June 7, 2020) 6

DHS Public-Private Analytic Exchange Program, *Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar* (2019). 34

DHS, CISA, *ICS Alert (ICS-ALERT-10-301-01) Control System Internet Accessibility* (Oct. 28, 2010) 16

DirBuster, SecTools 19

DOJ, Computer Crimes and Intellectual Property Section, *A Framework for a Vulnerability Disclosure Program for Online Systems* (July 2017) 33

DOJ, *Report of the Attorney General's Cyber-Digital Task Force* (July 2, 2018). 7-8, 25

The DROWN Attack (July 1, 2016) 15

Elizabeth Weise, *Nissan Leaf App Deactivated Because It's Hackable*, USA Today (Feb. 26, 2016). 13

Page

Marcia Hofmann, *Legal Considerations for Widespread Scanning*, Rapid7 (Oct. 30, 2013) 21

Markup of H.R. 6620, H.R.6735, H.R. 6740, H.R. 6742, and S.1281, 115th Cong. (Sept. 13, 2018) 30

Michael A. Specter & J. Alex Halderman, *Security Analysis of the Democracy Live Online Voting System* (June 7, 2020) 28, 29, 33

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* (Feb. 13, 2020) 11

Mike Hoskins, *Diabetes Device 'Hacker' Joins Forces with FDA*, Healthline (June 27, 2019). 12

Natalie Pittore & Liam Davitt, *Ghidra—the Software Reverse Engineering Tool You've Been Waiting for—is Here!*, NSA Central Security Service (Mar. 5, 2019) 21

Nicole Perlroth, *Security Experts Expect 'Shellshock' Software Bug in Bash to Be Significant*, N.Y. Times (Sept. 25, 2014) 15

NIST, *Cybersecurity Framework Version 1.1* (Apr. 16, 2018) 29

Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596 (2003) 17

Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143 (2016) 17, 18

Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. Davis L. Rev. 1327 (2008) 25, 26

Press Release, Voting Village at DEF CON Promotes Election Security and Integrity (Aug. 12, 2018). 23

Privilege escalation, Wikipedia 19

Public Bug Bounty List, Bugcrowd 30, 33

Responsible Research and Disclosure Policy, Facebook (last updated Mar. 31, 2020) 31

Rolf Haenni, *Swiss Post Intrusion Test: Undetectable Attack Against Vote Integrity and Secrecy*, Bern Univ. of Applied Sciences 10-11

Sarah Jamie Lewis, *et al.*, *Trapdoor Commitments in the SwissPost E-Voting Shuffle Proof*, Univ. of Melbourne. 10

Page

Scott Wolchok, *et al.*, *Attacking the Washington, D.C. Internet Voting System*, Proc. 16th Conf. on Fin. Cryptography & Data Security (Feb. 2012) 10

Sean Gallagher, *How the KRACK attack destroys nearly all Wi-Fi security*, Ars Technica (Oct. 16, 2017) 14

Sean Gallagher, *Man gets threats—not bug bounty—after finding DJI customer data in public view*, Ars Technica (Nov. 17, 2017) 31

Sean Gallagher, *Oracle security chief to customers: Stop checking our code for vulnerabilities [Updated]*, Ars Technica (Aug. 11, 2015) 22

The #WeHeartHackers Initiative, #WeHeartHackers 12

Timothy B. Lee, *Here's what you find when you scan the entire Internet in an hour*, Wash. Post (Aug. 18, 2013) 20-21

Tod Beardsley, *R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump*, Rapid7 (Oct. 4, 2016) 12

What is a port scan?, Palo Alto Networks 20

Yael Grauer, *Safe Harbor or Thrown to the Sharks by Voatz?*, Cointelegraph (Feb. 7, 2020) 32

INTEREST OF AMICI CURIAE[1]

Amici are united in their concern that the government's broad interpretation of the Computer Fraud and Abuse Act ("CFAA") chills essential computer security[2] research by exposing computer security researchers to criminal and civil liability.

Amici include leading computer security researchers who have helped to advance the safety and integrity of information technology systems in the service of consumers, businesses, and governments worldwide. A complete list of individual amici is contained in the appendix.[3]

Amici also include organizations that support and employ security researchers:

The Electronic Frontier Foundation ("EFF") is a nonprofit civil liberties organization that has worked for nearly 30 years to protect innovation, free expression, and

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

[2] This brief uses the terms "computer security" and "cybersecurity" interchangeably. *See Computer Security*, Wikipedia, https://en.wikipedia.org/wiki/Computer_security.

[3] Short biographies for amici computer security researchers can be found at https://www.eff.org/cases/van-buren-v-united-states/security-researcher-amici.

civil liberties in the digital world. As part of its Coders' Rights Project, EFF offers pro bono legal services to researchers engaged in cutting-edge exploration of technology whose work in the public interest may be unjustly chilled by laws including the CFAA. EFF has served as counsel or amicus in nearly every appellate case involving the CFAA in the last decade.

The Center for Democracy & Technology ("CDT") is a nonprofit public interest organization that supports laws, corporate policies, and technical tools to protect the civil liberties of Internet users and represents the public's interest in maintaining an open Internet. CDT supports the clear and predictable application of cybercrime statutes including the CFAA. CDT has filed amicus briefs in several CFAA cases, including *United States v. Manning*, 78 M.J. 501 (A. Ct. Crim. App. 2018), *United States v. Valle*, 807 F.3d 508 (2d Cir. 2015), and *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009).

Bugcrowd is the leading crowdsourced cybersecurity platform, headquartered in San Francisco, CA with offices around the world. Bugcrowd connects a highly-skilled, global community of over 200,000 security researchers to governments, military, corporations, and not-for-profit organizations, helping identify and fix critical vulnerabilities before attackers exploit them. Bugcrowd pioneered the crowdsourced cybersecurity model and has actively advocated for more conducive legal frameworks for good-faith security research since its inception. This research is vital to the future resilience of the Internet, and over 1,000 Bugcrowd customers globally rely on it to help make the digitally connected world a safer place.

Rapid7 is a cybersecurity company headquartered in Boston. Rapid7 conducts independent research to advance security for all technology users, and to complement Rapid7's products and services. Rapid7's security research includes Internet-wide scanning of publicly accessible computer assets for vulnerabilities, and Rapid7 openly shares the results to help defenders reduce risks. Rapid7 performs independent research on numerous technologies and discloses vulnerabilities to the manufacturers. Rapid7 helps coordinate disclosures of vulnerabilities discovered by third party researchers to improve security outcomes. Rapid7's products and services manage cybersecurity risk, investigate attacks, and automate tasks. Over 9,000 customers rely on Rapid7 to securely advance their organizations.

SCYTHE, a Virginia-based cybersecurity company, provides an adversarial emulation platform based on available vulnerability and threat research to empower organizations to continuously assess and integrate remediations against the latest attack capabilities. Real-world threats are constantly evolving, the open sharing and reporting of research is a key element for organizations to analyze and achieve optimal security postures. SCYTHE's curated research enables defenders to reduce their attack exposure and minimize risks. SCYTHE's platform and customers worldwide rely on this exchange of vulnerability and capability research to continuously improve and advance organizational security.

Tenable, the cyber exposure company, helps over 30,000 organizations understand and reduce cyber risk. The Tenable research team takes a broad scope approach to understanding the vulnerability landscape, ultimately equipping customers and the industry at large with the tools, awareness, and intelligence needed to effectively reduce risk. The team's work includes writing plugins for vulnerability and asset detection; developing audit and compliance checks; and vulnerability and threat tracking and analysis. The team, which identified over 100 zero-days in 2019, also actively searches for vulnerabilities in common and critical products and works with vendors to fix vulnerabilities and alert end-users to the risks.

SUMMARY OF ARGUMENT

Congress passed the CFAA in recognition of growing security threats that malicious attackers could pose to computers and networks, especially computers used by the federal government and financial institutions. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 1001 (9th Cir. 2019). Over the following decades, however, the CFAA has been interpreted too broadly, with the perverse effect of slowing the development of computer security, undermining the very purpose of the law. That is because, in practice, secure computing and software[4] relies heavily on the work of independent researchers in academia, industry, public service, and independent practice to identify and fix flaws that malicious attackers could otherwise exploit. These researchers work to identify serious shortcomings in systems ranging from medical devices to voting machines to cloud services to critical national infrastructure. This research is especially urgent

[4] The CFAA prohibits unauthorized access to "protected computers," which encompass nearly any device with a microprocessor and thus the software and systems supported by these computers. *See United States v. Kramer*, 631 F.3d 900, 902 (8th Cir. 2011).

as we find ourselves integrating networked computers into our homes, vehicles, and even our bodies.

Despite widespread agreement about the importance of this work—including by the government itself—researchers face legal threat for engaging in socially beneficial security testing. Under the government's broad interpretation of the CFAA, standard security research practices—such as accessing publicly available data in a manner beneficial to the public yet prohibited by the owner of the data—can be highly risky.

Amici write to inform the Court of the vital role that security researchers play and to demonstrate how the CFAA has hindered their work. They urge the Court to adopt a narrow construction of the law consistent with Congress's intent and to clarify that contravening written prohibitions on means of access is not a violation of the CFAA.

ARGUMENT

I. The Work of the Computer Security Research Community Is Vital to the Public Interest.

A. Computer Security Benefits from the Involvement of Independent Researchers.

Failures of computer security threaten nearly every facet of our lives, from fighting COVID-19 to ensuring safe and fair elections to simply using Internet-connected devices in our homes.[5] But building trustworthy systems,

[5] *See, e.g.*, Catherine Stupp, *Hackers Change Ransomware Tactics to Exploit Coronavirus Crisis*, Wall St. J. (May 14, 2020),

products, and software is a challenging task. The complexity of modern computing and human fallibility make bugs inevitable. Many mistakes are benign, but others can have severe consequences if adversaries find and exploit them. As a result, the engineers who build and maintain essential systems and software—including for hospitals, banks, election commissions, power plants and other critical infrastructure—have the never-ending task of addressing flaws as they are discovered.

The modern computer security field emerged in the 1970s and 80s[6] and took on increased importance in the 1990s and early 2000s as the use of personal computers grew, and users connected corporate and personal systems to the Internet. During this period, a series of high-profile vulnerabilities in widely used products like Microsoft's Windows XP operating system drove home the need to

https://www.wsj.com/articles/hackers-change-ransomware-tactics-to-exploit-coronavirus-crisis-11589448602; David E. Sanger, *et al.*, *Amid Pandemic and Upheaval, New Cyberthreats to the Presidential Election*, N.Y. Times (June 7, 2020), https://www.nytimes.com/2020/06/07/us/politics/remote-voting-hacking-coronavirus.html; Brian Krebs, *Hacked Cameras, DVRs Powered Today's Massive Internet Outage*, Krebs on Security (Oct. 21, 2016), https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage.

[6] An early Internet worm, written by a graduate student at Cornell University, led to both the first criminal conviction under the CFAA and the creation of the first computer security incident response team ("CSIRT") at Carnegie Mellon University. *See United States v. Morris*, 928 F.2d 504 (2d Cir. 1991); *CERT Coordination Center*, Wikipedia, https://en.wikipedia.org/wiki/CERT_Coordination_Center.

focus on security in designing new software.[7] As Microsoft CEO Bill Gates recognized in an influential 2002 memo, truly “trustworthy computing” requires “refin[ing] and improv[ing] that security as threats evolve.”[8]

But the computer security field has not been exclusively or even primarily driven by large corporations. In the words of amicus Alex Stamos, former Chief Security Officer for Yahoo and Facebook:

> More than any other field of computing, security has benefited from the existence of a large, diverse, unofficial community of researchers and practitioners. I can think of few advancements in semiconductor design that did not originate in a well-funded corporate or academic lab, but a majority of the advancements in finding and fixing security flaws over the last two decades has come from the “security research community.”[9]

[7] John Markoff, *Stung by Security Flaws, Microsoft Makes Software Safety a Top Goal*, N.Y. Times (Jan. 17, 2002), https://www.nytimes.com/2002/01/17/business/stung-by-security-flaws-microsoft-makes-software-safety-a-top-goal.html.

[8] *Gates memo: ‘We can and must do better’*, CNET (Jan. 15, 2002), https://www.cnet.com/news/gates-memo-we-can-and-must-do-better.

[9] Expert Report and Decl. of Alex Stamos ¶16, *Apple, Inc. v. Corellium, LLC*, No. 9:19-cv-81160-RS, ECF No. 451-6 (S.D. Fla. 2020) (“Stamos Decl.”). “The computer security research community is comprised of not only computer security companies but also individuals and organizations with expertise in computer security.” DOJ, *Report of the Attorney General’s Cyber-Digital Task Force*

The federal government has also heralded the contributions of the security research community. For example, the Attorney General's Cyber-Digital Task Force wrote in 2018 that computer security experts make "valuable contributions to combating cyber threats by discovering significant exploitable vulnerabilities affecting, among other things, the confidentiality of data, the safety of Internet-connected devices, and the security of automobiles."[10]

Decades of experience[11] have shown that *independent auditing and testing* of computers by members of the security research community—often in a manner unanticipated and even disapproved by the computers' owners—is particularly effective at discovering serious vulnerabilities in widely used software and devices. Just as the drafter of a legal brief can overlook even the most glaring typo, the original developers of software may simply miss their own errors, which can be more apparent

109 (July 2, 2018) ("*Cyber-Digital Task Force*"), https://www.justice.gov/ag/page/file/1076696/download.

[10] *Cyber-Digital Task Force*, *supra* note 9, at 109-10; *see also, e.g.*, Commerce Dep't, *International Cybersecurity Priorities: Fostering Cybersecurity Innovation Globally* (June 26, 2017), https://www.commerce.gov/sites/default/files/2018-06/International%20Cybersecurity%20Priorities%20Report.pdf (discovery of vulnerabilities is "a key aspect of security research as well as an integral part of the burgeoning security industry").

[11] Like other research communities, the security research community exchanges information about discoveries and techniques in peer-reviewed journals published by organizations such as the Association of Computing Machinery, USENIX, and popularly attended conferences such as DEF CON, Black Hat, and CanSecWest. *See* Stamos Decl., *supra* note 9, ¶ 16.

to outsiders. For similar reasons, existing products that gain wider adoption are exposed to new use cases and more attention from researchers, leading to the discovery of new flaws—as was recently the case with Zoom's videoconferencing software.[12] In addition, independent researchers may be able to develop specialized techniques to uncover flaws. Large technology companies like Google and Apple have highly skilled in-house security teams, but even these companies rely heavily on discoveries from beyond their corporate walls. Outside researchers may work in tandem or with the permission of these in-house security teams, or they may work independently, without any official permission.

When outside researchers discover a vulnerability, they often follow a disclosure process, exchanging information with vendors or others about the nature of the flaw so that it can be fixed or mitigated. Disclosure is frequently an iterative process, with researchers working collaboratively with computer owners to assess and mitigate the problem. Disclosures can also include a "proof-of-concept" that the vulnerability can truly be exploited. Creating a proof-of-concept might seem risky, but it is often necessary to demonstrate the severity of the vulnerability or to test possible fixes.

[12] *See, e.g.*, Kate O'Flaherty, *Zoom Users Beware: Here's How A Flaw Allows Attackers To Take Over Your Mac Microphone And Webcam*, Forbes (Apr. 1, 2020), https://www.forbes.com/sites/kateoflahertyuk/2020/04/01/zoom-users-beware-heres-how-a-flaw-allows-attackers-to-take-over-your-mac-microphone-and-webcam/#46b25e612fbe.

B. Security Researchers Have Made Important Contributions to the Public Interest by Identifying Security Threats in Essential Infrastructure, Voting Systems, Medical Devices, Vehicle Software, and More.

1. Election Security

Independent and academic security researchers have made major contributions to election security. In 2010, for example, Washington, D.C. invited the public to test a pilot project that would allow overseas absentee voters to cast their votes online.[13] Within 48 hours, independent researchers, including amicus J. Alex Halderman, were able to change every vote and reveal almost every secret ballot, using the same publicly available information that would be known to any real-life attacker.[14] As a result, the District's Board of Elections and Ethics discontinued its plans to use the digital voting system.[15] Similarly, when a Swiss e-voting system made its source code public in 2019 and invited independent researchers to test the system's security, researchers uncovered vulnerabilities that would allow attackers to secretly tamper with cast votes.[16]

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

[14] *Id.*

[15] *Id.*

[16] *See* Sarah Jamie Lewis, *et al.*, *Trapdoor Commitments in the SwissPost E-Voting Shuffle Proof*, Univ. of Melbourne, https://people.eng.unimelb.edu.au/vjteague/SwissVote; Rolf Haenni, *Swiss Post Intrusion Test: Undetectable Attack Against Vote Integrity and*

And this year, security researchers from MIT, including amicus Michael A. Specter, discovered security flaws in a mobile application called Voatz that has been used in federal, state, and municipal U.S. elections to allow people to vote directly from their smartphones.[17] The security flaws would allow attackers to alter, stop, or expose voters' ballots.[18] Recognizing the importance of such independent security testing, the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency ("CISA") invites security researchers to test voting machines for vulnerabilities at the annual DEF CON security conference.[19]

2. Medical Devices

The healthcare industry increasingly relies on connected, implantable devices. Such devices offer significant public health opportunities, but also invite the risk of malfunction and create vulnerabilities that attackers can exploit. Outside security researchers have uncovered numerous threats to implantable medical devices capable of being programmed wirelessly, such as pacemakers, defibrillators, and insulin pumps. For example, security researcher Jay Radcliffe

Secrecy, Bern Univ. of Applied Sciences, https://e-voting.bfh.ch/app/download/7833162361/PIT2.pdf.

[17] 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* at 1 (Feb. 13, 2020), https://internetpolicy.mit.edu/wp-content/uploads/2020/02/SecurityAnalysisOfVoatz_Public.pdf.

[18] *Id.*

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

discovered a flaw in his own Medtronic insulin pump that could allow malicious actors to remotely disable the pump or even deliver insulin dosages at lethal rates.[20] Five years later, Radcliffe found that flaws in new models of insulin pumps still allowed attackers to remotely trigger unauthorized insulin injections.[21]

Recognizing the value of such studies, the federal government and medical device makers have encouraged further independent research. After Radcliffe's insulin pump research, FDA regulators reached out to him for assistance.[22] And in 2019, ten medical device makers, including Medtronic, took part in an initiative coordinated by the FDA called "#WeHeartHackers," in which the companies shared over thirty medical devices with researchers for independent security testing.[23]

3. Vehicular Safety

While the automotive sector has swiftly embraced computerized and Internet-connected systems, flaws in

[20] *See* Mandeep Khera, *Think Like a Hacker: Insights on the Latest Attack Vectors (and Security Controls) for Medical Device Applications*, 11 J. Diabetes Sci. & Tech. 207, 208 (2016).

[21] *See* Tod Beardsley, *R7-2016-07: Multiple Vulnerabilities in Animas OneTouch Ping Insulin Pump*, Rapid7 (Oct. 4, 2016), https://blog.rapid7.com/2016/10/04/r7-2016-07-multiple-vulnerabilities-in-animas-onetouch-ping-insulin-pump/.

[22] Mike Hoskins, *Diabetes Device 'Hacker' Joins Forces with FDA*, Healthline (June 27, 2019), https://www.healthline.com/diabetesmine/diabetes-device-hacker-joins-forces-with-fda#2.

[23] *See The #WeHeartHackers Initiative*, #WeHeartHackers, https://wehearthackers.org/.

these systems can jeopardize drivers' privacy in their location history, expose vehicles to theft, and threaten the safety of occupants and bystanders. As the FTC has recognized, security researchers have furthered "consumers' privacy, security, and safety" by uncovering security vulnerabilities in connected cars.[24] In 2015, for example, amici Charlie Miller and Chris Valasek discovered that attackers could hack a Jeep Cherokee from miles away, using a cellular network to access the car's brakes and bring it to a stop.[25] As a result of that research, Chrysler created a software fix and issued a 1.4 million vehicle recall.[26] In 2016, independent researcher Troy Hunt reported a flaw in a Nissan Leaf mobile app that allowed attackers to spy on driver data and drain car batteries.[27] The same day, Nissan deactivated the app, removing the vulnerability.[28]

[24] *Examining Ways to Improve Vehicle and Road Safety: Hearing Before the Subcomm. on Commerce, Manufacturing, and Trade of the H. Comm. on Energy and Commerce*, 114th Cong. (2015) (statement of the FTC), https://www.ftc.gov/system/files/documents/public_statements/826551/151021vehiclesafetytestimony.pdf.

[25] Andy Greenberg, *Hackers Remotely Kill a Jeep on the Highway – With Me in It*, Wired (July 21, 2015), https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

[26] Andy Greenberg, *After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix*, Wired (July 24, 2015), https://www.wired.com/2015/07/jeep-hack-chrysler-recalls-1-4m-vehicles-bug-fix/.

[27] Ashley Carman, *Nissan Leaf's App Could Let Hackers Run Down Batteries and See Trip Logs*, The Verge (Feb. 24, 2016), https://www.theverge.com/2016/2/24/11110156/nissan-leaf-hack-vulnerability-app.

[28] Elizabeth Weise, *Nissan Leaf App Deactivated Because It's Hackable*, USA Today (Feb. 26, 2016), https://www.usatoday.com/story/tech/news/2016/02/24/nissan-disables-app-hacked-electric-leaf-smart-phone-troy-hunt/80882756/.

4. Internet Security

Independent security researchers have discovered and fixed potentially devastating network security flaws. That includes "WannaCry," perhaps the "worst cyberattack in history," which infected and disabled hundreds of thousands of computers around the world over the course of several days in 2017.[29] WannaCry's rapid spread resulted in billions of dollars of damage, and caused serious disruptions in medical procedures throughout the UK's National Health Service, as well disrupting police departments, universities, and transit and manufacturing companies.[30] The damage would have been even greater, however, if not for Marcus Hutchins, a twenty-three year old security researcher living in rural England, who studied WannaCry during his spare time and devised a way to effectively shut it down.[31]

Hutchins is far from the only researcher to have made significant contributions to Internet security in recent years by discovering or devising fixes to major network security vulnerabilities. Other examples include:

- "KRACK," which can "destroy[] nearly all WiFi security," discovered by two researchers at a Belgian university;[32]

[29] Andy Greenberg, *The Confessions of Marcus Hutchins, the Hacker Who Saved the Internet*, Wired (May 12, 2020), https://www.wired.com/story/confessions-marcus-hutchins-hacker-who-saved-the-internet/.

[30] *Id.*

[31] *Id.*

[32] Sean Gallagher, *How the KRACK attack destroys nearly all Wi-Fi security*, Ars Technica (Oct. 16, 2017), https://arstechnica.com/

- "Shellshock," categorized by the National Institute of Standards and Technology ("NIST") as a critical vulnerability that would allow attackers to entirely take over millions of affected computers, discovered and fixed by a programmer in his spare time;[33] and

- "DROWN," which could allow attackers to decrypt secure communication with millions of affected websites, discovered by a team of academic and outside security researchers, including amicus J. Alex Halderman.[34]

Further examples of contributions by security researchers could be drawn from any number of other sectors, including industrial control systems ("ICS") associated with power

information-technology/2017/10/how-the-krack-attack-destroys-nearly-all-wi-fi-security/.

[33] Nicole Perlroth, *Security Experts Expect 'Shellshock' Software Bug in Bash to Be Significant*, N.Y. Times (Sept. 25, 2014), https://www.nytimes.com/2014/09/26/technology/security-experts-expect-shellshock-software-bug-to-be-significant.html; Ben Grubb, *Stephane Chazelas: The Man Who Found the Web's 'Most Dangerous' Internet Security Bug*, Sydney Morning Herald (Sept. 27, 2014), https://www.smh.com.au/technology/stephane-chazelas-the-man-who-found-the-webs-most-dangerous-internet-security-bug-20140926-10mixr.html.

[34] Dan Goodin, *More than 11 million HTTPS websites imperiled by new decryption attack*, Ars Technica (Mar. 1, 2016), https://arstechnica.com/information-technology/2016/03/more-than-13-million-https-websites-imperiled-by-new-decryption-attack/; The DROWN Attack (last updated July 1, 2016), https://drownattack.com/.

plants, dams, and other critical infrastructure.[35] Such research is essential to our nation's security.

II. The Broad Interpretation of the CFAA Adopted by the Eleventh Circuit Chills Valuable Security Research.

A. The Eleventh Circuit's Interpretation of the CFAA Would Extend to Violations of Website Terms of Service and Other Written Restrictions on Computer Use.

The CFAA's language is notoriously ambiguous. The statute makes it a crime to "intentionally access[] a computer without authorization or exceed[] authorized access, and thereby obtain[] . . . information from any protected computer." 18 U.S.C. § 1030(a)(2)(C). Although the statute defines "exceeds authorized access" as "to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter," 18 U.S.C. § 1030(e)(6), it does not define either "with authorization" or "without authorization."

The formulation adopted by the Eleventh Circuit in this case for assessing whether someone "exceeds authorized access" to a computer under the CFAA turns on the computer owner's unilateral policies regarding use of its networks. *See United States v. Van Buren*, 940 F.3d 1192, 1207-08 (11th Cir. 2019). Mr. Van Buren, a

[35] *See, e.g.*, DHS, CISA, *ICS Alert (ICS-ALERT-10-301-01) Control System Internet Accessibility* (Oct. 28, 2010), https://www.us-cert.gov/ics/alerts/ICS-ALERT-10-301-01.

police officer in Cumming, Georgia, was convicted under subsection (a)(2)(C) of "exceed[ing] authorized access" to the Georgia Crime Information Center database because he accessed information he was otherwise entitled to access, but for a purpose not permitted by the written use policy governing the database. *Id.* at 1207.

Although this case involves a law enforcement database, the Eleventh Circuit's rule could apply any time someone accesses a computer or network in violation of the owner's stated policies governing access and use of the computer. Examples of cases alleging violations of such policies have involved employment agreements, *see United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) (en banc) ("*Nosal I*"); *United States v. Rodriguez*, 628 F.3d 1258 (11th Cir. 2010), and the terms of service governing social networks and other websites, *see United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009). Under this theory, a computer owner can grant someone access to given files or a website hosted on a server without any physical or "code-based" restrictions—no technological barrier stopped Mr. Van Buren from running the search of law enforcement records for a non-law-enforcement purpose—but still insist that certain forms of access or use of those files "exceeded authorization" under the CFAA. *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1600 (2003) (distinguishing between "code-based" and "contract-based" theories of authorization).[36]

[36] Professor Kerr has since acknowledged that even premising "authorization" solely on "code-based" restrictions is unworkably vague. Orin S. Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. 1143, 1164 (2016).

B. Standard Computer Security Research Methods Can Violate Written Access Restrictions.

The broad interpretation of the CFAA adopted by the Eleventh Circuit imperils a wide swath of valuable security research.

First, a great deal of security research necessarily takes place on systems or software subject to written terms of service, because that is the only way the software is made available to the public. Under the Eleventh Circuit's rule, researchers risk CFAA liability if they violate any of these terms.

Second, even where computer owners' policies are not fully explicit, researchers' ability to access and use computers may be at odds with the particular means of access the owners believe to be "authorized." If there is no effective technological barrier in place, therefore, users may inadvertently "exceed access" under a broad interpretation of the CFAA merely by accessing computers in an unanticipated manner. In *United States v. Auernheimer*, 748 F.3d 525, 530-31 (3d Cir. 2014), for example, the defendant was charged with violating the CFAA for demonstrating automated access to thousands of public-facing AT&T websites that the company had not "expected people to find," even though they were accessible to anyone who knew the website addresses.[37] Kerr, *Norms of Computer Trespass*, 116 Colum. L. Rev. at 1164.

[37] Despite the public accessibility of the AT&T websites, the district court in *Auernheimer* concluded that the indictment "sufficiently allege[d] the elements of unauthorized access." *United States v. Auernheimer*, No. 11-CR-470 SDW, 2012 WL 5389142, at *3 (D.N.J. Oct. 26, 2012), *rev'd on other grounds*, 748 F.3d at 529.

Researchers are hard-pressed to avoid these risks. 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. The work involves trial and error, as researchers look for vulnerabilities in complex systems. Sometimes researchers employ a chain of techniques that seek to leverage one basic flaw to discover more serious vulnerabilities or demonstrate access to more sensitive data,[38] and often it is the initial stages of their work that involves forms of "access" of uncertain legality. Common techniques include:

Scraping and automated access. Rapidly accessing and downloading data using automated means can provide insight that would be all-but-impossible to gain by accessing the data manually. For example, by rapidly checking thousands of common subdirectory naming patterns on a website, an automated script can find or "scrape" sections of the website that should not be publicly accessible but that the website owner may have inadvertently misconfigured.[39] Finding these inadvertently public websites can prevent serious exposures of private and sensitive data.

However, many website terms of service explicitly prohibit visitors from using automated means of access, including scraping, even though websites often make little or no technological effort to prevent it. *See, e.g.*, *United States v. Manning*, 78 M.J. 501, 512 (A. Ct. Crim. App. 2018)

[38] *See, e.g.*, *Privilege escalation*, Wikipedia, https://en.wikipedia.org/wiki/Privilege_escalation.

[39] *See DirBuster*, SecTools, https://sectools.org/tool/dirbuster.

(using scraping tool disallowed by acceptable use policy exceeded authorized access). Even when scraping is not explicitly prohibited, it may run against website owners' expectations, as in *Auernheimer*, because it allows a researcher to discover publicly accessible websites that were intended to be private. In either case, scraping can be unauthorized access under a broad interpretation of the CFAA. *See* Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. Sci. & Tech. L. 372 (2018).

Port and network scanning. Somewhat analogously, researchers can scan a server for open "ports," designated endpoints in networking software that designate types of communications allowed by the server. Finding certain open ports can be strongly indicative of misconfiguration or other vulnerabilities, and port scanning is therefore highly "valuable for testing network security and the strength of the system's firewall."[40] Like scraping, port scanning is frequently forbidden in terms of service governing network access.[41] There are also several popular tools and projects, such as Project Sonar, ZMap, and Shodan that allow researchers to scan much or all of the Internet to catalog the prevalence of vulnerabilities on publicly accessible computers or Internet of Things ("IoT") devices.[42] At this

[40] *What is a port scan?*, Palo Alto Networks, https://www.paloaltonetworks.com/cyberpedia/what-is-a-port-scan.

[41] *See, e.g.*, *Acceptable Use Policy for XFINITY® Internet*, Comcast (Sept. 21, 2017), https://www.xfinity.com/corporate/customers/policies/highspeedinternetaup (prohibiting "unauthorized port scanning").

[42] *See, e.g.*, Timothy B. Lee, *Here's what you find when you scan the entire Internet in an hour*, Wash. Post (Aug. 18, 2013),

scale, it is impossible to assess the wishes of every relevant computer owner, placing these resources on uncertain legal grounds under a broad interpretation of the CFAA.[43]

Reverse engineering and code inspection. Reverse engineering is an important method by which researchers can detect potential vulnerabilities in code and computer systems by working backwards to determine how they are built. It is so useful that the NSA has published a version of its own powerful reverse engineering tool to "make the software reverse engineering process more efficient" and "level the playing field for cybersecurity professionals."[44]

But software terms of use and terms of service commonly prohibit reverse engineering.[45] Even when

https://www.washingtonpost.com/news/the-switch/wp/2013/08/18/heres-what-you-find-when-you-scan-the-entire-internet-in-an-hour/ (describing use of ZMap to find prevalence of Universal Plug and Play vulnerability); Liam Tung, *Over 350,000 Microsoft Exchange servers still open to flaw that's under attack: Patch now*, ZDNet (Apr. 7, 2020), https://www.zdnet.com/article/over-350000-microsoft-exchange-servers-still-open-to-flaw-thats-under-attack-patch-now (Project Sonar).

[43] *See* Marcia Hofmann, *Legal Considerations for Widespread Scanning*, Rapid7 (Oct. 30, 2013), https://blog.rapid7.com/2013/10/30/legal-considerations-for-widespread-scanning.

[44] Natalie Pittore & Liam Davitt, *Ghidra—the Software Reverse Engineering Tool You've Been Waiting for—is Here!*, NSA Central Security Service (Mar. 5, 2019), https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/1775584/ghidra-the-software-reverse-engineering-tool-youve-been-waiting-for-is-here/.

[45] *See* Joseph Lorenzo Hall & Stan Adams, *Taking the Pulse of Hacking: A Risk Basis for Security Research* 10 n.9, CDT (Mar.

researchers reverse engineer software running solely on their own computers, they may do so in order to document or modify how these devices connect to remote servers, implicating the CFAA's prohibitions on exceeding authorized access.[46] As with other techniques, researchers who reverse engineer to inspect code for vulnerabilities have been met with CFAA threats.[47]

C. The Broad Interpretation of the CFAA Discourages Researchers from Pursuing and Disclosing Security Flaws.

Once a researcher discovers vulnerabilities in a product, notifying a company or the public of the flaw may prompt the company to fix the vulnerability, preventing bad actors from discovering and exploiting it. But researchers face a dilemma if they violate any written restrictions in identifying the vulnerability in the course of their research. By disclosing, researchers may reveal that they contravened the owner's access preferences, and may expose themselves to a lawsuit or criminal liability under the broad interpretation of the CFAA. As such, the government's reliance on this broad interpretation of the statute conditions security improvements on researchers'

2018), https://cdt.org/wp-content/uploads/2018/04/2018-03-27-Risk-Basis-for-Security-Research-FNL.pdf.

[46] *See, e.g.*, Bill Budington, *Ring Doorbell App Packed with Third-Party Trackers*, EFF (Jan. 27, 2020), https://www.eff.org/deeplinks/2020/01/ring-doorbell-app-packed-third-party-trackers.

[47] *See, e.g.*, Sean Gallagher, *Oracle security chief to customers: Stop checking our code for vulnerabilities [Updated]*, Ars Technica (Aug. 11, 2015), https://arstechnica.com/information-technology/2015/08/oracle-security-chief-to-customers-stop-checking-our-code-for-vulnerabilities.

tolerance of the risk of being sued or prosecuted for reporting vulnerabilities.

Even as some companies have expressed appreciation for the work of independent security researchers, others have proven quick to lash out against them. In 2018, for example, security researchers at the DEF CON security conference's "Voting Village" discovered vulnerabilities in election machines made by the manufacturer Election Systems and Software ("ES&S"). In response, ES&S threatened legal action, forcing the Village to retain counsel.[48] Those threats also prompted members of the Senate Committees on Intelligence and Homeland Security and Governmental Affairs to admonish ES&S that "independent testing is one of the most effective ways to understand and address potential cybersecurity risks."[49] The senators wrote they were "disheartened that ES&S . . . is not supportive of independent testing."[50] Nevertheless, ES&S doubled down, responding that it would not "provide or submit any hardware, software, source code or other intellectual property to unvetted, anonymous security researchers, nor would [it] make public any assessments of vulnerability findings."[51]

[48] *See* Press Release, Voting Village at DEF CON Promotes Election Security and Integrity (Aug. 12, 2018), https://www.documentcloud.org/documents/6144470-ES-S-legal-threat.html.

[49] Letter from Senators Kamala D. Harris, Susan M. Collins, Mark R. Warner, and James Lankford, to Tom Burt, President and CEO, Election Systems and Software (Aug. 22, 2018), https://www.harris.senate.gov/imo/media/doc/August%2022%202018%20-%20Letter%20to%20ESS.pdf.

[50] *Id.*

[51] Letter from Tom Burt, President and CEO, Election Systems and Software, to Senators Kamala D. Harris, Susan M.

ES&S is not the only company in the election security space to threaten security researchers. In 2019, the mobile voting company Voatz reported a University of Michigan student to the FBI because the student conducted research into Voatz's mobile voting app for an undergraduate election security course.[52] With the coronavirus pandemic adding new urgency to an already-exploding market for digital voting systems, attempts to chill security research into such systems are particularly misguided. Any vulnerability could have devastating consequences, from exposing individuals' votes, to falsifying election results, to undermining public faith in the legitimacy of our democratic system. And without independent researchers testing the security of voting systems, it is not possible to ensure that the systems are secure, or that their results are accurate. Similar examples appear in many other sectors. In 2015, for example, a researcher canceled a talk at a security conference in Singapore about security flaws in a popular networked surveillance camera that would allow attackers to remotely access the camera and its footage, after he received legal threats from one of the vendors implicated by the research.[53]

Collins, Mark R. Warner, and James Lankford (Aug. 24, 2018), https://regmedia.co.uk/2018/08/28/essresponseletter.pdf.

[52] 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.

[53] Darren Pauli, *Talk revealing p0wnable surveillance cams pulled after legal threat*, The Register (Oct. 8, 2015), https://www.theregister.com/2015/10/08/hitb_remote_exploit_ip_cameras/?mt=1444351029389.

As the Department of Justice has recognized, this is a serious problem. Because the CFAA and similar laws chill "legitimate security research" by criminalizing cybersecurity experts' "methods of searching for and analyzing vulnerabilities," DOJ's Cyber-Digital Task Force has specifically recommended that the agency adopt explicit carve-outs to "encourage and protect legitimate computer security research" from criminal liability.[54]

Yet despite the DOJ's recognition that the CFAA chills valuable security research, its prosecutors continue to assert a broad interpretation of CFAA liability. Companies and the government have even taken the position that the act of reporting a vulnerability may *itself* violate access restrictions. In 2008, the Massachusetts Bay Transit Authority ("MBTA") invoked the CFAA to try to enjoin two independent security researchers from presenting truthful information about vulnerabilities in the MBTA's fare collection system at a security conference.[55] And in *United States v. McDanel*, the government brought criminal CFAA charges against a defendant who discovered a security vulnerability, alerted the company, and then, when the company refused to fix the problem, alerted the company's customers.[56] Although the company

[54] *Cyber-Digital Task Force*, *supra* note 9, at 110.

[55] *See MBTA v. Anderson*, No. 08-cv-11364, slip op. (D. Mass. Aug. 9, 2008) (granting temporary restraining order), https://www.eff.org/files/filenode/MBTA_v_Anderson/mbta-temp-restraining-order.pdf; *see also* Jon Choate, *Commentary, MBTA v. Anderson: D. Mass: MIT Students' Security Presentation Merits Temporary Restraining Order*, Harv. J.L. & Tech. Digest (2008), http://jolt.law.harvard.edu/digest/mbta-v-anderson.

[56] *See* Paul Ohm, *The Myth of the Superuser: Fear, Risk, and Harm Online*, 41 U.C. Davis L. Rev. 1327, 1349 (2008).

fixed the bug, the government brought CFAA charges against McDanel for the act of truthfully communicating information about it.[57]

Regardless of whether courts would agree that the mere act of truthfully reporting a vulnerability could be grounds for criminal liability under the CFAA, security researchers who discover vulnerabilities must nonetheless decide whether disclosing the flaw is worth the risk of inviting a protracted legal battle over their right to speak out.

As a result of the broad interpretation of the CFAA, fear of civil and criminal exposure often prevents security researchers from testing systems as thoroughly as they otherwise would or from disclosing vulnerabilities they discover. Even when researchers choose to notify a computer owner of a vulnerability, risk of liability under the CFAA may lead them to limit their engagement with the owner, which can make the disclosure process far less effective.

Through its Coders' Rights Project, amicus EFF frequently offers pro bono counsel to security researchers seeking to engage in public-interest security research that would run afoul of the broad interpretation of the CFAA.[58] Though EFF counsels these clients on how to reduce their legal risk, some are nonetheless dissuaded from either

[57] *Id.* After McDanel appealed his conviction, the government dropped the charges. McDanel had already served eighteen months in prison.

[58] *See Coders' Rights Project*, EFF, https://www.eff.org/issues/coders.

pursuing their work or publicizing the results. This is a significant loss for computer security.

An in-depth study conducted by amicus CDT in 2018 confirmed that the CFAA results in widespread chill of security testing that researchers perceive as legally risky under the CFAA.[59] The study surveyed twenty academic and independent security researchers with qualitative methods to understand how researchers decide whether to pursue or avoid certain kinds of projects.[60] Half of the subjects reported that they considered the CFAA to be a primary source of risk.[61] More than half of those reported avoiding some or all types of research that might implicate the CFAA.[62] The interview subjects noted uncertainty surrounding what activities "exceed authorized access" under the CFAA. As a result, some subjects avoided any potential risk of CFAA liability by avoiding networked systems entirely.[63] Others tried to avoid work that involved terms of service agreements where possible.[64] Several interview subjects stated that they tried to carefully read terms of service, but noted the practical impossibility of doing so at scale—for example, in an Internet-wide network scan.[65] Several researchers experienced retaliation for

[59] *See* Hall & Adams, *supra* note 45.

[60] *Id.* at 4.

[61] *Id.* at 9.

[62] *Id.*

[63] *Id.* at 9-10.

[64] *Id.* at 10.

[65] *Id.*

disclosing vulnerabilities, ranging from verbal and written threats of legal action to FBI investigation in one case, and arrest in another.[66] To mitigate these risks, many researchers disclose vulnerabilities to an intermediary rather than to companies directly.[67]

Amici themselves have limited the methods or scope of their research, or specifically tailored their methods of disclosure, in order to mitigate the risk of CFAA liability. When amicus Michael A. Specter, along with other MIT researchers, uncovered security vulnerabilities in Voatz's mobile voting platform, the researchers—cognizant of Voatz's aggressive response to security researchers in the past—sought legal counsel from the Boston University/MIT Technology Law Clinic, and disclosed their findings first to the Department of Homeland Security, in part to protect themselves against retaliation.[68] When amici Michael A. Specter and J. Alex Halderman studied the security of the Democracy Live Omniballot System, a web-based voting platform that has been used or approved for use in fourteen states and the District of Columbia,[69] they identified security flaws that could allow attackers to alter votes without detection.[70] But they were unable

[66] *Id.* at 12.

[67] *Id.*

[68] *See* Abby Abazorius, *MIT researchers identify security vulnerabilities in voting app*, MIT News (Feb. 13, 2020), http://news.mit.edu/2020/voting-voatz-app-hack-issues-0213.

[69] *Approvals, Reviews, and Certifications*, Democracy Live, https://democracylive.com/approvals-reviews-and-certifications/.

[70] Michael A. Specter & J. Alex Halderman, *Security Analysis of the Democracy Live Online Voting System* (June 7, 2020), https://internetpolicy.mit.edu/wp-content/uploads/2020/06/OmniBallot.pdf.

to test comprehensively because "[a]ccessing non-public server functionality might raise legal issues."[71] They wrote, "To avoid these issues, we constrained our analysis to publicly available portions of the OmniBallot system," noting that "this approach limit[ed] our ability to identify vulnerabilities in Democracy Live's server-side code and infrastructure—an important task for future work."[72]

D. Voluntary Disclosure Guidelines and Industry-Sponsored Bug Bounty Programs Are Not Sufficient to Mitigate the Chill.

In recent years, there has been increasing recognition that companies should not meet vulnerability disclosures with threats or lawsuits. Beginning in 2013, the International Organization for Standardization ("ISO") published voluntary guidelines for "how to process and remediate reported potential vulnerabilities in a product or service."[73] Similar guidelines have been endorsed by NIST, the FTC, and members of Congress.[74]

[71] *Id.* at 7.

[72] *Id.*

[73] *See* ISO/IEC 30111:2019, *Information Technology – Security Techniques – Vulnerability Handling*, ISO (Oct. 2019), https://www.iso.org/standard/69725.html; ISO/IEC 29147:2018, *Information Technology – Security Techniques – Vulnerability Disclosure*, ISO (Oct. 2018), https://www.iso.org/standard/72311.html.

[74] NIST, *Cybersecurity Framework Version 1.1* (Apr. 16, 2018), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf; FTC, *Public Comment on NTIA Safety Working Group's "Coordinated Vulnerability Disclosure 'Early Stage' Template"*, (Feb. 15, 2017), https://www.ftc.gov/system/files/documents/advocacy_documents/

Additionally, many technology companies and components of the government such as the Department of Defense have created their own vulnerability disclosure guidelines. Many explicitly invite researchers to search for vulnerabilities, and some also offer financial rewards to researchers who uncover and report them, a practice known as a "bug bounty."[75]

Although vulnerability disclosure programs and bug bounties can lessen the chilling effects of a broad interpretation of the CFAA as to a company's own products by explicitly assuring researchers that their contributions are authorized within a given scope of engagement, they are far from sufficient.

First, not all companies run vulnerability disclosure programs. Despite growing endorsement of such programs, as of 2018, 93% of the Forbes Global 2000 companies still had no policy in place to receive, respond, and resolve critical bug reports submitted by the outside world.[76]

ftc-staffcomment-national-telecommunications-information-administration-regarding-safetyworking/170215ntiacomment.pdf; Markup of H.R. 6620, H.R.6735, H.R. 6740, H.R. 6742, and S.1281, 115th Cong. (Sept. 13, 2018) (Statement of Rep. Jim Langevin) ("The use of vulnerability disclosure policies is widely considered a best practice . . . . A vulnerability disclosure policy is an open hand of friendship to the hacker community . . . . These are the good guys."), https://www.youtube.com/watch?time_continue=815&v=D0TXFRYNGos (comments at 13:42).

[75] *See Public Bug Bounty List*, Bugcrowd, https://www.bugcrowd.com/bug-bounty-list/ (catalogue of bug bounty programs).

[76] *118 Fascinating Facts from HackerOne's Hacker-Powered Security Report 2018*, HackerOne (Aug. 27, 2018), https://www.

Second, vulnerability disclosure programs do not entirely immunize researchers from legal risk. Through their non-negotiable contractual terms, such programs generally authorize specific types of security research and vulnerability disclosures, sometimes attempting to provide a legal safe harbor.[77] But even where companies do provide an explicit safe harbor, their protections are generally limited to specific types of research and disclosures. Moreover, those terms can change at the whim of the company. Researchers who uncover a vulnerability not of the type solicited by the vulnerability disclosure programs—or who disclose vulnerabilities in ways not condoned by the programs—continue to face the same precarious legal position that they would in the absence of any program at all. For example, when the consumer drone manufacturer DJI launched a bug bounty program in 2017, DJI told computer security researcher Kevin Finisterre that the program covered security issues in the company's servers. When Finisterre then reported vulnerabilities that could allow attackers to access unencrypted flight logs, drivers' licenses, and passports, DJI told him that the company's servers were not in the scope of the program after all, and threatened him with CFAA charges.[78]

hackerone.com/blog/118-Fascinating-Facts-HackerOnes-Hacker-Powered-Security-Report-2018.

[77] *See, e.g.*, *Responsible Research and Disclosure Policy*, Facebook, (last updated Mar. 31, 2020), https://www.facebook.com/whitehat.

[78] Sean Gallagher, *Man gets threats—not bug bounty—after finding DJI customer data in public view*, Ars Technica (Nov. 17, 2017), https://arstechnica.com/information-technology/2017/11/dji-left-private-keys-for-ssl-cloud-storage-in-public-view-and-exposed-customers/.

Indeed, the existence of a vulnerability disclosure program can signal that the company is receptive to independent security research and willing to repair flaws, but it is not a guarantee. In the context of digital elections systems, for example, governments and the public recognize that extensive testing is essential to ensure reasonably reliable voting systems. As a result, manufacturers in this space may develop vulnerability disclosure programs to signal a heightened sensitivity toward security concerns. But companies have retaliated even against researchers following the terms of the vulnerability disclosure programs. The undergraduate student whom Voatz reported to the FBI, for example, had been conducting his research in compliance with the vulnerability disclosure program Voatz had in place at the time.[79] Voatz publicly stated that the student's research had violated the terms of the program—but Voatz had added the terms in question only after news of its FBI referral became public.[80]

Third, even companies seeking, in good faith, to mitigate all legal risk to security researchers may not be able to do so because of the uncertainty around the CFAA's key terms. The Justice Department has issued a seven-page document providing guidance on how companies can best do just that, in order to better detect vulnerabilities. But even the DOJ itself does not suggest that its lengthy framework fully avoids risk of CFAA

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

[80] *Id.*

liability. Instead, the Department states only that taking the prescribed steps may "*substantially reduc[e]* the likelihood that [the] described activities will result in a civil or criminal violation of the law under the [CFAA]."[81] And, in any case, fewer than twenty companies running vulnerability disclosure programs reportedly follow the DOJ guidelines on how to effectively provide a legal safe harbor for research.[82]

Finally, researchers are bound to the disclosure requirements that the disclosure program lays out—and those requirements frequently require that researchers agree not to disclose information of the vulnerability to any party other than the company itself.[83] Where security researchers discover a flaw exposing customers to a security risk and report the flaw to the company, only to find that the company takes no steps to patch the vulnerability, the researchers are unable to disclose the flaw to other affected entities, the public, or law

[81] DOJ, Computer Crimes and Intellectual Property Section, *A Framework for a Vulnerability Disclosure Program for Online Systems* (July 2017), https://www.justice.gov/criminal-ccips/page/file/983996/download (emphasis added).

[82] *See* Amit Elazari, *Standardizing Legal Safe Harbor for Security Research*, Bugcrowd (Aug. 2, 2018), https://www.bugcrowd.com/blog/guest-post-standardizing-legal-safe-harbor-for-security-research/; *see also Public Bug Bounty List*, Bugcrowd, https://www.bugcrowd.com/bug-bounty-list/ (noting whether bug bounty programs provide a legal safe harbor).

[83] Amici Michael A. Specter and J. Alex Halderman encountered such a term in their work on Democracy Live, and noted that it could "discourage responsible disclosure and could prevent researchers from alerting election officials or the public about flaws that go unfixed." Specter & Halderman, *supra* note 70, at 22.

enforcement without exposing themselves to liability under the CFAA. This is no mere hypothetical; companies frequently ignore serious vulnerabilities that researchers have reported until public disclosure forces the companies to make important security fixes.

In 2010, for example, a team of researchers from the University of California at San Diego and the University of Washington discovered a flaw in GM's OnStar dashboard system in the Chevy Impala that could allow attackers to remotely track vehicles, engage brakes at high speed, or disable brakes altogether. The researchers did not make this information public, and it took GM five years to fix the bug. This glacial response influenced amici Charlie Miller and Chris Valasek to go public with their subsequent findings of security flaws in the Jeep Cherokee.[84]

E. Malicious Actors Seeking Security Flaws Are Not Dissuaded by the CFAA.

Even as public-interest minded researchers test systems to bolster their security, cybercriminals and hostile nation-states search for security flaws to exploit them and are unlikely to be dissuaded by the CFAA.[85]

[84] Andy Greenberg, *GM Took 5 Years to Fix a Full-Takeover Hack in Millions of OnStar Cars*, Wired (Sept. 10, 2015), https://www.wired.com/2015/09/gm-took-5-years-fix-full-takeover-hack-millions-onstar-cars/.

[85] *See generally* DHS Public-Private Analytic Exchange Program, *Commodification of Cyber Capabilities: A Grand Cyber Arms Bazaar* (2019), https://www.dhs.gov/sites/default/files/publications/ia/ia_geopolitical-impact-cyber-threats-nation-state-actors.pdf.

Security researchers should be encouraged to work in the public interest. Instead, a broad interpretation of CFAA discourages them at every step: from conducting security research in the first place, to disclosing security flaws that they discover, to going public with security flaws when companies refuse to patch them. The results of this perverse system of incentives is that discoverable security vulnerabilities remain undetected or unpatched, effectively waiting for attackers to find and exploit them.

The results can be devastating. In 2016, a security researcher discovered that a flaw on the Equifax website could allow attackers to access individuals' personal data, including their social security numbers, full names, birthdates, and city and state of residence.[86] The researcher, who has remained anonymous, downloaded consumer data to demonstrate the flaw, and immediately reported it to Equifax. According to the researcher, Equifax could have fixed the vulnerability "the moment it was found. It would have taken them five minutes, they could've just taken the site down." Instead, Equifax ignored the disclosure and only months later informed the public that attackers had broken into its system and stolen the data of 143 million Americans.[87]

The researcher came forward with this story only after the data breach was already known. Had they taken more aggressive steps when they first realized the scope of the bug, such as providing a deadline for disclosing the

[86] Lorenzo Franceschi-Bicchierai, *Equifax Was Warned*, Vice (Oct. 26, 2017), https://www.vice.com/en_us/article/ne3bv7/equifax-breach-social-security-numbers-researcher-warning.

[87] *Id.*

flaw to the public, they might have persuaded the company to fix the problem sooner, thus avoiding a catastrophic breach. But those aggressive measures might also have provoked the company to lash out and threaten legal action under the CFAA against the researcher, as other companies have done against other researchers in the past. It is not surprising that, given the current legal landscape, the researcher chose to remain quiet instead.

CONCLUSION

Independent computer security research furthers the public interest in secure voting systems, medical devices, critical national infrastructure, vehicles, and many other sectors. But the broad interpretation of the CFAA endorsed by the Eleventh Circuit creates a major obstacle to this important work.

For these reasons, amici urge the Court to reverse the judgment of the Court of Appeals and clarify that contravening terms of service and other written prohibitions on means of access is not a violation of the CFAA.

Respectfully submitted,

Andrew Crocker
Counsel of Record
Naomi Gilens
Electronic Frontier Foundation
815 Eddy Street
San Francisco, California 94109
(415) 436-9333
andrew@eff.org

Dated: July 8, 2020

Counsel for Amici Curiae

APPENDIX

APPENDIX — LIST OF AMICI CURIAE COMPUTER SECURITY RESEARCHERS

(In alphabetical order. Titles given for identification purposes only.)

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

Claudio Guarnieri
Head of Security Lab at Amnesty International

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

Charlie Miller
Principal Autonomous Vehicle Security Architect at Cruise

Katie Moussouris
Founder & CEO Luta Security
Coauthor & coeditor of ISO 29147 & 30111
Creator of Microsoft's bug bounty program
Advisor to the Pentagon for Hack the Pentagon

Kristin Paget
Offensive Security Researcher, Intel Corporation

Marc Rogers
White hat hacker, security researcher & CTI-League founder

Appendix

Dr. Aviel (Avi) D. Rubin
Professor of Computer Science and Technical Director of the Information Security Institute at Johns Hopkins University

Bruce Schneier
Fellow and Lecturer, Harvard Kennedy School

Adam Shostack
Adam Shostack, President, Shostack & Associates

Ashkan Soltani
Independent researcher and technologist

Michael A. Specter
PhD candidate in Computer Science at the Massachusetts Institute of Technology

Alex Stamos
Director of the Stanford Internet Observatory and Lecturer in the Stanford Computer Science Department

Chris Valasek
Principal Autonomous Vehicle Security Architect at Cruise Automation

Tarah Wheeler
Cyber Project Fellow at the Belfer Center for Science and International Affairs at Harvard University's Kennedy School of Government

Appendix

Chris Wysopal
Chief Technology Officer and Chief Information Security Officer, Veracode

Peiter "Mudge" Zatko
Chair of the Board, Cyber Independent Testing Lab

Sarah Zatko
Chief Scientist, Cyber Independent Testing Lab