MITCHELL | HAMLINE
School of Law

Cybaris®

Volume 16 | Issue 2 Article 1

2025

Patching the CFAA so Researchers No Longer Pay

Joshua Baker

PATCHING THE CFAA SO RESEARCHERS NO LONGER PAY

Joshua Baker

I. Introduction

The Computer Fraud and Abuse Act (CFAA) is the federal statute that criminalizes unauthorized access to computers – i.e. hacking.[1] The CFAA's original scope criminalized intrusion into computers used by the government and financial institutions, but amendments have expanded the scope to include virtually all internet-connected devices.[2] Later amendments to CFAA provided a civil cause of action allowing for victims of computer crime to sue for damages in limited circumstance.[3] A lot has changed in the technology sector since 1986 and at the time of the CFAA's enactment, Congress could not have imagined that hackers would play a pivotal role in helping to safeguard computers against malicious attacks.[4] Unlike today, there was not a nuanced view of hackers or their activities.

Many of the methods and activities that were thought to be solely in the realm of malicious hackers are now used by security researchers, many of whom got their start as "hackers" in the traditional sense, seeking to improve the security of computing systems. While the definition of hackers and hacking has expanded to include "good faith" research, the CFAA does not differentiate between accessing a computer without authorization for benevolent purpose and accessing a computer without authorization for malicious reasons.[5] As the internet

[1] 18 U.S.C. § 1030.

[2] *See United States v. Kramer*, 631 F.3d 900, 902 (8th Cir. 2011) (noting the definition of "computer" is "exceedingly broad," and concluding an ordinary cell phone is a computer); *see also United States v. Nosal* (Nosal II), 844 F.3d 1024, 1050 (9th Cir. 2016), cert. denied, 138 S. Ct. 314 (2017) (noting "protected computers" include "effectively all computers with Internet access…").

[3] Violent Crime Control & Law Enforcement Act of 1994, 1994 Enacted H.R. 3355, 103 Enacted H.R. 3355, 108 Stat. 1796, 2097.

[4] U.S. Dep't of Just., Department of Justice Announces New Policy on Charging Cases Under the Computer Fraud and Abuse Act, https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act (stating that "[c]omputer security research is a key driver of improved cybersecurity").

[5] 18 U.S.C. § 1030(a)(2)(c) (prohibiting unauthorized access of a protected computer to obtain information, stating: "Whoever intentionally access a computer without authorization or exceeds authorized access and thereby obtains information from any protected computer.").

has expanded, so has the need for security research to secure cyberspace from growing threats. In a 2002 memo, Bill Gates, then CEO of Microsoft, acknowledged the need for a security first mindset, "emphasiz[ing] security right out of the box" and the need to "constantly refine and improve security that security as threats evolve."[6] While companies improved their efforts to secure their products, the efforts of security researchers were the primary driver of computer security.[7] According to 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."[8]

So, too, has the federal government recognized the importance of the work of the security research community. The Attorney General's Cyber-Digital Task Force acknowledges this importance, writing that computer security experts provide "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."[9]

Despite these efforts, cybercrime is on the rise.[10] As of this writing, the Cybersecurity & Infrastructure Security Agency's (CISA) Known Exploited Vulnerabilities (KEV) catalog

[6] *Memo from Bill Gates*, Microsoft (Jan. 11, 2002), https://news.microsoft.com/2012/01/11/memo-from-bill-gates/ [https://perma.cc/Q35F-2KJ3].
[7] Brief of Amicus Curiae Computer Security Researchers, *Van Buren*, 141 S. Ct. 1648, 210 L. Ed. 2d 7, 2020 WL 4005654. (citing 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).
[8] *Id.*
[9] *Id.* at 8.
[10] Ani Petrosyan, *Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2023*, Statista (Feb. 12, 2024), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/ [https://perma.cc/9F2N-RJ27].

contains 1236 vulnerabilities confirmed to have been exploited in the wild.[11] One cannot hardly go a day without reading about another security incident in the news. If computer companies truly have committed to security in their products, the real-world effects have yet to be felt. And with immunity from civil liability under the CFAA, it is not the companies whose vulnerabilities are exploited that pay the costs. The security research community stands by to fill this gap, but the risk of prosecution and civil liability under the CFAA continues to chill cybersecurity research.

The Supreme Court's 2021 decision in *Van Buren v. United States* partially limited the scope of the CFAA.[12] Providing some protections to security researchers, the decision prompted changes to the federal criminal charging policy for "good faith security researchers." Although *Van Buren* narrowed the scope of the "exceeds authorized access" phrase in the CFAA, a majority of the research performed by security researchers is done "without authorization" on computers they do not own.[13] While the new charging guidelines provide protections for researchers, the risk of civil ligation remains. Policies for responsible vulnerability disclosure can mitigate some risk, but those protections go only as far as the terms of the policy and rely on the "good faith" of the company to whom the vulnerability is disclosed.[14]

This climate has forced researchers to partially or completely forgo research that may fall afoul of the CFAA. Additionally, confusing and non-standard vulnerability disclosure policies (VDP) leave researchers unsure whether they should disclose vulnerabilities and, if so, to whom. Advocates have called for changes to the CFAA that would provide a safe harbor provision for

[11] *Known Exploited Vulnerabilities Catalog*, Cybersecurity & Security Infrastructure Security Agency, https://www.cisa.gov/known-exploited-vulnerabilities-catalog.
[12] Van Buren v. United States, 141 S. Ct. 1648 (2021).
[13] *Id.*
[14] *See infra* Section IV (B).

security researchers. Absent these changes, however, any and all mitigation to the liability a researcher faces is at the sole discretion of the company whose vulnerabilities they find.

This article will proceed first by providing a more nuanced definition of hackers, showing that Congress's narrow understanding when the CFAA was enacted has functioned to criminalize legitimate research efforts. Second, the article will proceed to discuss the current state of cybercrime, focusing on both the computer industry's historical and current practices that have contributed to the insecurity of the internet. Third, the article will showcase how the CFAA stifles the important work of cybersecurity researchers by exposing them to the risk of prosecution and civil litigation. Recent efforts by the courts, the federal government, and private industry to mitigate the risk have not gone far enough to provide protection to researchers. Finally, the article will discuss the various proposals for amending the CFAA, including redefining "access", "good faith security researcher" and "loss." The article will put forth a proposal of its own: eliminating corporations' immunity from civil liability under the CFAA to not only improve overall cybersecurity but importantly, serve as a shield for security researchers.

II. THE HISTORY OF THE CFAA'S ENACTMENT ASSUMED HACKERS WERE ONLY MALICIOUS.

The Computer Fraud and Abuse Act (CFAA) was initially enacted in 1986 as a response to growing concerns about computer-related crimes in the government and financial sectors.[15] The 1983 film "WarGames" played a significant role in inspiring this legislation after a screening by then President Ronald Reagan at Camp David.[16] The movie, which depicted a young hacker accessing a military supercomputer and nearly triggering a nuclear war, raised awareness among

[15] 86 CIS PL 99474; 99 CIS Legis. Hist. P.L. 474.

[16] Kevin Bankston, *How Sci-Fi Like WarGames Led to Real Policy During the Reagan Administration*, Slate (Oct. 8, 2018), https://slate.com/technology/2018/10/reagan-wargames-star-wars-science-fiction-policy.html [https://perma.cc/3AYV-U4K2].

lawmakers about the potential national security risks posed by unauthorized computer access.[17] This fictional scenario prompted real-world discussions in Congress about the need for comprehensive cybersecurity legislation.[18] As a result, the CFAA, as originally drafted, aimed to protect sensitive information stored on government and financial institution computers, recognizing the potential national security risks associated with unauthorized access to such data.[19] The CFAA criminalized unauthorized access to government and financial institution computers with intent to defraud.[20] Additionally, the CFAA criminalized causing damage to computers accessed without authorization and trafficking in passwords that would allow unauthorized access to a government computer or otherwise affect interstate commerce.[21] Congress believed this legislation, coupled with "active efforts of industry to safeguard their property", would address the growing issue of computer crime.[22] Thus, when the CFAA was enacted, Congress considered the issue of cybercrime to be one of dual responsibility: the computer industry working to prevent cybercrimes and the government enforcing the law when they do occur.[23]

As technology and society changed, Congress updated the CFAA to address new and emerging concerns around cybercrime. In response to the growth of network connected computers, the CFAA was expanded to include computers used in interstate or foreign commerce, expanding the act's reach beyond government and financial systems, encompassing a wide range of private sector computers.[24] The CFAA was later amended again to expand the

[17] Synopsis, WarGames Plot, IMDB, https://www.imdb.com/title/tt0086567/plotsummary/?ref_=tt_stry_pl#synopsis [https://perma.cc/9Y4L-HGGY].
[18] *See supra* note16.
[19] *Id.*
[20] Pub. L. No. 99-474, 100 Stat. 1213 (1986)
[21] *Id.*
[22] 132 Cong. Rec. H3275-76(daily ed. June 3, 1986) (statement of Rep. Hughes).
[23] *Id.*
[24] Violent Crime Control& Law Enforcement Act of 1994, Pub. L. No. 108 Stat. 1796, 2097.

definition of "protected computer" to include not only those used in interstate and foreign commerce but also communication.[25] This change effectively brought all internet-connected computers under the CFAA's purview, significantly broadening its reach in this era of rapidly expanding internet adoption.[26]

Additionally, and perhaps most significantly so far as liability to researchers is concerned, Congress made an exception to the economic loss doctrine, amending the CFAA to provide a civil cause of action to victims of cybercrime.[27] In 2001, the CFAA was again amended to provide immunity from civil liability for the negligent design or manufacture of computer hardware, computer software, or firmware.[28] The end result of these amendments was an expansion of the risks researchers face under the CFAA, while the computer industry was provided immunity from civil liability for damages their products may create.

While amendments to the CFAA have contributed to increased liability for researchers, to this day Congress's initial beliefs about hacking continue to impact the current state of cybersecurity. The beliefs that hacking could only be malicious, and that the computer industry would safeguard against cybercrime has proven false on both accounts. The computer industry has not met expectations in preventing cybercrime, leaving a large group of hackers dedicated to finding vulnerabilities in software and hardware that malicious actors seek to exploit. The CFAA, however, does not distinguish between good and bad hackers, and this fundamental misunderstanding of who hackers are and what they do has resulted in both criminalization of

[25] Economic Espionage Act of Pub. L. No. 104-294, 110 Stat. 3488, 3491 (defining "protected computer" as any computer "which is used in or affecting interstate or foreign commerce or communication, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States").

[26]Computer Crimes, 61 Am. Crim. L. Rev. 441, 451 n.81 (2024).

[27] *See supra* note 3.

[28] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT Act) ACT OF 2001, 107 Pub.L. No. 107=56,115 Stat. 272, 38284.

and civil liability for important security research. To better understand why this differentiation matters, first one must get a broader sense of hackers and hacking culture.

A. The Dual Morality of Hacking is Not Recognized by the CFAA.

Media reporting and popular culture generally associate the term hacker with unethical behavior.[29] During House discussions regarding the CFAA, there was concern that hackers were being glamorized in the media, and there was a need to acknowledge hackers for what they are: criminal trespassers.[30] While it is true that some hackers may have malicious motivations, not all accept the definition of a hacker as such. Before hackers took on a negative connotation, it was used as a term of endearment: "a clever programmer who produced elegant code for solving difficult problems."[31] Hackers are a large and diverse group with wide-ranging goals and motivations; therefore, members of the hacking community cannot be singularly defined. Reasons for engaging in hacking are personal and expansive: "curiosity, thrill-seeking, extortion, academic interest, a desire to fix problems, and the urge to wreak havoc."[32] Hacker, however, is often utilized as a catch-all term that doesn't differentiate the purpose of the individual.[33]

To account for the alternate purposes of hackers, the term has been further differentiated as "white hat" hackers and "black hat" hackers. "Black hat" hackers seek to do harm, "motivated by mischief or profit rather than by actually fixing vulnerabilities and security flaws."[34] "White hat" hackers, on the other hand, "seek to improve cybersecurity by finding vulnerabilities in hardware and software."[35] The singular term, "hacker", can never fully account for the wide

[29] *Synopsis*, Hacking Is Not a Crime, https://www.hackingisnotacrime.org [https://perma.cc/PRN3-HQK9].
[30] *Supra* note 22.
[31] SCOTT J. SHAPIRO, FANCY BEAR GOES PHISHING 46 (1st ed. 2023).
[32] Shooting the Messenger: Remediation of Disclosed Vulnerabilities as CFAA "Loss," 29 Rich. J.L. & Tech. 89, 101 (2022) (citing Ido Kilovaty, Freedom to Hack, 80 OHIO ST. L.J. 455, 480 (2019)).
[33] *Id.*
[34] *Id.*
[35] *Id.* at 101-02.

range of motivations behind hacking, and some have called for alternative designations that encompass the purpose of the individual. The terms "Hacktivist," "Researcher," or "Whistleblower" have been suggested as an alternative to "white hat" hacker to account for the purpose behind the hacker's actions.[36] To further differentiate, the terms "Attacker," "Malicious Adversary," or "Threat Actor" have been suggested as a replacement for "black hat" hacker.[37] Aside from the negative connotation associated with the word hacker, there is also a misunderstanding of who hackers are. While there is no singular defining characteristic of a hacker, studies have revealed a more precise definition of those who engage in hacking.

B. Hackers are Often Not the Criminal Masterminds the CFAA was Enacted to Punish.

In general, those engaged in hacking tend to be young men bored "with work or school, nonsocial, and have few outside activities."[38] The initial motivation for these young hackers is fun: providing an intellectual challenge, puzzle solving, and an opportunity to gain esteem in the eyes of their peers.[39] Most learned hacking techniques from other hackers in online forums where peer pressure fosters an environment of escalation of increasing deviant behavior.[40] With the rise of the internet, many "get their start as part of an online video game culture."[41] Of those charged with cybercrimes, 80% had no prior criminal history.[42] Unlike other categories of crime, cybercriminals tend to have higher education and employment status.[43] Cyber-offenders

[36] Tenets, Hacking is Not a Crime, https://www.hackingisnotacrime.org/conduct [https://perma.cc/Y828-JBBS].

[37] *Id.*

[38] W. Cagney McCormick, *The Computer Fraud & Abuse Act: Failing to Evolve with the Digital Age*, 16 SMU Sci. & Tech. L. Rev 481, 483 (2013) (citing Scott Tulman, *Unique Characteristics of Computer Crime Prosecutions and Offers*, in I1B-40A *Criminal Defense Techniques* § 40A.03[2] (2011)).

[39] *See supra* note 31, at 292.

[40] *Id.* at 292 (describing deviant behaviors ranging from "game cheats and booting to profit-oriented cybercrime").

[41] *Id.*

[42] *Id.*

[43] *See supra* note 39, at 293 (citing Alice Hutchings, "Cybercrime Trajectories: An Integrated Theory of Initiation, Maintenance, and Desistance," in *Crime Online: Correlates, Causes, and Context,* ed. Thomas J. Holt (Durham, NC: Carolina Academic Press, 2016), 117-40).

generally believe that they will not be caught and that law enforcement lacks the capability to investigate cybercrimes.[44] These hackers are "moral agents, possessing a sense of justice purpose, and identity" who take responsibility for their actions.[45] They are, however, apt to justify attacks: blaming victims for not securing their computers or minimizing the amount of harm they have caused.[46] Importantly, most juvenile and young adult offenders tend to "age out of crime."[47] Numerous criminal hackers transition from cybercrime to cybersecurity, where the same skills they've acquired can be used to protect rather than harm.[48] In fact, it is generally a prerequisite in the cybersecurity community to have been a hacker to understand how to defend against attackers.[49] This is because the methods and tools utilized by attackers are also used by researchers to discover vulnerabilities before they can be exploited by those attackers.

C. The Methods and Tools Used by Hackers are Morally Agnostic.

Hackers use a multitude of security tools to find vulnerabilities. Port and networking scanning is a method for scanning servers on the internet to check for open ports – essentially channels by which computers communicate.[50] Certain open ports can be indicative of a misconfiguration on the server or other potential vulnerabilities, and therefore, port scanning is a highly effective tool for testing network security and the efficacy of a network's firewall.[51] Both researchers and attackers scan the internet for these misconfigurations or vulnerabilities, only differing in what they intend to do once they find one: researchers responsibly disclose their findings, while attackers seek to exploit them. Hackers also utilize data scraping and automated

[44] *Id.* at 292.
[45] *Id.* at 293 (noting that undeserving targets are left alone while target those believed to be deserving).
[46] *Id.*
[47] *Id.*
[48] *Id.* at 295.
[49] *Id.* at 89.
[50] *See supra note* 7, at 20.
[51] *Id.*

access testing, a method by which a script can automatically access all of a website's available directories.[52] These tools can find portions of websites that were not intended to be publicly available and, therefore, provide access to potentially private or sensitive information.[53] Reverse engineering and code inspection allows hackers to examine source code and work backwards to determine how the software and computer systems function.[54] This method allows hackers to find potential code or computer system vulnerabilities.[55] What they choose to do after discovering vulnerabilities is ultimately what defines a hacker as a researcher or an attacker. Another method that hackers utilize is brute force attacks to guess passwords. Brute forcing can be used by an attacker to gain unauthorized access to an account, or it can be used by a researcher to check if default passwords were not changed in a system, presenting a significant risk of breach or exploitation by an attacker.[56] Additionally, hackers can utilize a security testing method known as "fuzzing."[57] Fuzzing is an automated process by which "junk inputs" are thrown at a computer system, causing it to crash or otherwise have the system respond in an unintended way, thereby exposing vulnerabilities.[58] This list is by no means exhaustive.[59] One important takeaway is that these tools and methods are morally agnostic: it is the intent of the person using them that determines whether they are used to cause or prevent harm.[60] The CFAA,

[52] *Id.* at 18.
[53] *Id.*
[54] *Id.* at 21; *see also Source Code*, WIKIPEDIA, https://en.wikipedia.org/wiki/Source_code (last accessed Dec. 8, 2024),[https://perma.cc/P9A4-27UW].
[55] *Id.*
[56] *Brute Force Attack*, OWASP, https://owasp.org/www-community/attacks/Brute_force_attack (last visited Dec. 8, 2024), [https://perma.cc/ RCU6-RSF3] (describing how attackers utilize brute force attacks); *but see An Overview of the Usage of Default Passwords*, Elec. & Computer Eng'g & Computer Sci. Fac. Pubs. (2018), https://digitalcommons.newhaven.edu/cgi/viewcontent.cgi?article=1070&context=electricalcomputerengineering-facpubs, [https://perma.cc/7L4R-Z88P] (describing breaches exploiting default user credentials and tests showing that default passwords remain a significant problem).
[57] *See supra* note 3, at 158.
[58] *Id.*
[59] *Security Hacker*, WIKIPEDIA, https://en.wikipedia.org/wiki/Security_hacker#Techniques, [https://perma.cc/8C5D-9ZPG].
[60] *Shapiro, supra* note 31, at 159.

however, does not consider a hacker's motivations or the purpose behind the methods and tools utilized by hackers, leaving both malicious attackers and benevolent researchers caught in its wake.

III. THE CFAA PROVIDES CORPORATIONS IMMUNITY FROM CIVIL LIABILITY AND SHIFTS THE COST OF CYBERCRIME TO EVERYONE ELSE.

Estimates of the cost of cybercrime have risen from an estimated 1 billion dollars at the enactment of the CFAA to 452 billion dollars in 2024 with estimates up to 1.8 trillion dollars by 2028.[61] During this time, software and hardware vulnerabilities have increased dramatically. Since tracking began in 1999, the number of Common Vulnerabilities and Exposures (CVE) that have been published has risen from 321 in 1999 to 28,961 in 2023.[62] Through three quarters in 2024, the number of reported vulnerabilities is at 29,004 making it a record year with an additional quarter yet to be reported.[63] The number of security incidents that make use of software vulnerabilities continues to rise.[64] Havibeenpwned.com, a website that tracks website breaches and the exposed account information obtained in those breaches, has 834 breaches listed in its database consisting of over 14 billion compromised accounts.[65] Personal information exposed in these breaches includes names, passwords, physical addresses, dates of birth, employers, government-issued IDs, and social security numbers.[66] Many of these data breaches occurred because attackers exploited vulnerabilities in the company's software or hardware.[67]

[61] Ani Petrosyan, *Annual Number of Data Compromises and Individuals Impacted in the United States from 2005 to 2023*, STATISTA (Feb. 12, 2024), https://www.statista.com/forecasts/1399040/us-cybercrime-cost-annual [https://perma.cc/9F2N-RJ27].

[62]*Metrics*, CVE, https://www.cve.org/about/Metrics, [https://perma.cc/3RSK-KVHT].

[63] *Id.*

[64] *Id.* at 61.

[65] HAVEIBEENPWNDED, https://haveibeenpwned.com, [https://perma.cc/Y3DF-MC3J]

[66] *Breached Websites that Have Been Loaded into Have I Been Pwned*, HAVEIBEENPWNDED, https://haveibeenpwned.com/PwnedWebsites [https://perma.cc/54PV-B5ZU].

[67] *Id.*

In 2013, a data breach containing information for 153 million Adobe accounts was posted online.[68] While the passwords for accounts in the dataset were encrypted, poor cryptography allowed them to be easily converted back to plain text.[69] In 2018, a database containing billions of data records for Apollo was compromised.[70] The database was publicly available on the internet and did not require a password to access it.[71] In 2019, verifications.io, an email address validation service, suffered a breach exposing personal information of over 750 million users.[72] Similar to the Apollo breach, a database was public-facing without requiring a password.[73] In 2021, a Facebook hack compromised the data of over 500 million users.[74] The information was allegedly obtained by exploiting a vulnerability that Facebook had claimed to have fixed two years prior.[75] In 2022, a vulnerability in the Twitter site allowed information on over 6 million users to be extracted.[76] The vulnerability was introduced in a June 2021 update to their code.[77] In 2024, user data for almost 50 million AT&T customers was published online.[78] AT&T denied that there was a data breach for nearly 2 weeks before acknowledging that the breach did happen.[79] In all of these instances, the CFAA immunizes the negligence of corporations

[68] *Breached Websites that Have Been Loaded into Have I Been Pwned*, HAVEIBEENPWNDED, https://haveibeenpwned.com/PwnedWebsites#Adobe [https://perma.cc/A5CF-J28S]. (listing breaches in the following paragraph as by no means exhaustive, but just a quick highlight of breaches that occurred because of poor security practices).

[69] *Id.*

[70] *Breached Websites that Have Been Loaded into Have I Been Pwned*, HAVEIBEENPWNDED, https://haveibeenpwned.com/PwnedWebsites#Apollo [https://perma.cc/A5CF-J28S].

[71] *Id.*

[72] *Breached Websites that Have Been Loaded into Have I Been Pwned*, HAVEIBEENPWNDED, https://haveibeenpwned.com/PwnedWebsites#VerificationsIO [https://perma.cc/A5CF-J28S].

[73] *Id.*

[74] *Breached Websites that Have Been Loaded into Have I Been Pwned*, HAVEIBEENPWNDED, https://haveibeenpwned.com/PwnedWebsites#Facebook [https://perma.cc/A5CF-J28S].

[75] *Id.*

[76] *Breached Websites that Have Been Loaded into Have I Been Pwned*, HAVEIBEENPWNDED, https://haveibeenpwned.com/PwnedWebsites#Twitter [https://perma.cc/A5CF-J28S].

[77] *Id.*

[78] *Breached Websites that Have Been Loaded into Have I Been Pwned*, HAVEIBEENPWNDED, https://haveibeenpwned.com/PwnedWebsites#AllegedATT [https://perma.cc/A5CF-J28S].

[79] *Id.*

responsible for the breaches. Even when a corporation is breached due to a vulnerability in the software or hardware of a vendor, under the CFAA, those vendors face no civil liability for the damage those vulnerabilities caused. Spending on cybersecurity increases every year – projected to reach $215 billion in 2024 – and yet the number of breaches every year continues to rise.[80] While the correlation between the increase in software vulnerabilities and the increase in data breaches does not necessarily give rise to causation, it's not too far of a leap to think that if the computer industry were to release software with fewer vulnerabilities in their products, fewer would be able to be exploited in data breaches.

However, this is not our reality; software vendors consistently release products and software with vulnerabilities.[81] Even if vendors release fixes once a vulnerability is discovered, risk remains; not all vulnerabilities are known and patched before they are exploited by attackers.[82] It's estimated that 80 percent of intrusions into federal computer systems are attributable to software errors, or poor-quality software.[83] And despite the growing number of vulnerabilities, breaches, and costs associated with software vulnerabilities, the time and effort spent on software security is declining.[84] Sammy Migues, principal at Imbricate Security and co-author of the Building Security in Maturity Model (BSIMM) report, notes that companies tend to think of security vulnerabilities as "shrinkage" and until "shrinkage of revenue from software

[80] David Malmstrom, *Data Breach Securities Class Actions: Record Settlements and Investor Clams on the Rise,* Harvard Law School Forum on Corporate Governance (Aug. 21, 2024), https://corpgov.law.harvard.edu/2024/08/21/data-breach-securities-class-actions-record-settlements-and-investor-claims-on-the-rise/#4 [https://perma.cc/KW2E-RMK3].

[81] *See supra* note 38, at 484. (citing Clay Wilson, *Computer Attack and Cyber Terrorism: Vulnerabilities and Policy Issues for Congress* 5*,* CRS REPORT FOR CONGRESS (2003).

[82] *Id*.

[83] *Id.* at 485.

[84] Taylor Armerding, *Zero-day software defects are leading to many very bad days,* NERD FOR TECH (Oct. 28, 2024), https://medium.com/nerd-for-tech/zero-day-software-defects-are-leading-to-many-very-bad-days-c1d9d032ad63 [https://perma.cc/H9JY-CKGN].

defects broadly hits unacceptable levels, there won't be a lot of change."[85] Companies facing no liability for hardware and software vulnerabilities will surely not lead to this change. In fact, those in the cybersecurity industry have recently taken Microsoft to task for using one of their own security flaws as an opportunity to upsell customers on their own security offerings.[86] While certainly not alone in the computer industry, Microsoft has a sordid history of releasing buggy products that are exploited by attackers.

In 1994, Microsoft found itself scrambling to catch up to competitors like Netscape, which was already beginning to showcase the power of the internet.[87] A potential nightmare scenario was upon Microsoft: a world where consumers preferred competitors' less expensive hardware with the Netscape web browser providing access to the internet, forgoing the more expensive machines running the Microsoft Windows operating system.[88] By mid-1994, compared to the year prior, the number of websites grew from 2,700 to 23,500, almost exclusively run on the UNIX operating system running on Java.[89] Crucially, Microsoft was virtually nowhere to be found on the internet.[90] Microsoft had some serious ground to cover and they did just that.[91] Congress's expectation that industry would safeguard its products and actively prevent cybercrime was soon forgotten.

In an effort to catch Netscape, Microsoft added the internet into almost all aspects of the Windows operating system, including a web browser, Internet Explorer, in their latest version,

[85] *Id.*
[86] Alex Stamos, *Microsoft's Dangerous Addiction to Security Revenue*, SentinelOne (Jan. 31, 2024), https://www.sentinelone.com/blog/microsofts-dangerous-addiction-to-security-revenue/
[87] *Id.* at 141.
[88] *Id.* at 143.
[89] *Id.* at 142 (noting that Java was a programming language developed by Sun Microsystems).
[90] *Id.* at 143 (noting in a memo to employees, Bill Gates, after 10 hours of web browsing, discovered there were virtually no Microsoft file formats to be found on the internet).
[91] *Id.* at 144.

Windows 95.[92] Previously, security was not a substantial concern for Microsoft as its main product, Windows, was for personal computers: this new push for internet connectivity would expose the vulnerabilities in the operating system and applications.[93] While security concerns were considered, they paled in comparison to the pressure to incorporate the Internet into every aspect of the new Windows 95 operating system; the push for Internet features in lieu of security consideration would have disastrous consequences.[94] Rushed development and poor coding practices were exploited mercilessly.[95] Rather than working to prevent cybercrime, Microsoft, in releasing poorly tested software and the vulnerabilities that came with it, would become the leading enabler of cybercrime.

Vulnerabilities in Outlook and Word would wreak havoc on the internet.[96] Viruses hidden in macros-enabled Word documents were sent out via email and, when opened by the recipient, would automatically run the hidden code and send to the recipient's contacts.[97] While initially these viruses were not destructive, the volume of emails caused servers to become overwhelmed and soon unresponsive.[98] Later variations were much more harmful. A particularly nasty attack, named ILOVEYOU, deleted every image file it could find, hid files, and renamed files, inserting its code, to be run again when users tried to open the infected files.[99] The virus took advantage of a flaw in Outlook whereby the application did not read the entirety of a file name and a flaw in Windows that allowed code in email attachments to run automatically upon clicking.[100] The virus

[92] Shapiro, *supra* note 31, at 144.
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] *Id.* at 146.
[97] *Id.* at 147.
[98] *Id.*
[99] *Id.* at 149.
[100] *Id.* (explaining that the file was named "LOVE-LETTER-FOR-YOU.TXT.vbs" which denoted it is a file that contains code, but Outlook stopped parsing the filename after the first period, making it appear to be an innocuous text file).

spread faster than anything in history to that point, causing networks to become unresponsive: it was estimated that 10 percent of the world's computers were infected with a total cost approaching 10 billion dollars.[101] The Windows operating system did nothing to stop the virus from deleting files and spreading with impunity.[102] Microsoft wasn't held financially responsible for rampant abuse of vulnerabilities and the damage they caused, but Bill Gates did release a memo at least acknowledging the poor security practices and a plan to fix them.[103] Unfortunately, this wasn't the first time vulnerabilities in software products were easily exploited causing the internet to come to a halt. In fact, over a decade earlier the computer industry was put on notice, but the first CFAA prosecution made one thing clear: companies would not bear the responsibility for the harm their insecure products caused.

A. The First CFAA Conviction Puts Security Research on Notice

The first prosecution under the CFAA was not an attacker seeking to do harm but a young computer scientist exploring the then-young internet as part of his PhD thesis[104]. Robert Morris Jr. was a graduate student at Cornell University in the school's computer science program[105]. As part of his role as the school's system administrator, he discovered a major security flaw in the UNIX operating system that could be exploited over the internet.[106] He shared this discovery with a friend, and neither had ever heard of a program being used to spread on the internet before.[107] Morris carefully ensured that his code didn't risk destroying data before releasing the

[101] *Id.*
[102] *Id.*
[103] Gates, *supra* note 6.
[104] *Shapiro, supra* note 31, at 71.
[105] *Id.* at 4.
[106] *Id.* at 71.
[107] *Id.* (noting Morris decided to showcase the flaws for his PhD thesis, and thus "the brilliant project", as they called it, was born. As history would have it the project, a scientific endeavor as far as Morris was concerned, would come to know Morris's discoveries by a different name: "The Morris Worm").

program on the internet.[108] Within hours of releasing the internet worm, Morris realized there was a problem.[109] Due to a miscalculation in his program, numerous networks across the country were offline.[110]

The FBI opened an investigation against Robert Morris Jr., but they were unsure of how to proceed.[111] Nobody had yet been tried under the CFAA, and the language of the CFAA did not make it clear under what section Morris should be charged.[112] Ultimately, the government elected to charge Morris with a felony, given the amount of damage his actions had caused.[113]

At his trial, Morris argued that the CFAA required dual intent: both intent to access a computer *and* intent to cause damage.[114] The trial court judge disagreed with Morris' reading of the law, instead giving the jury instructions that the government need not prove Morris intended to cause damage, only that he intended to release the worm.[115] The juror delivered a unanimous guilty verdict.[116]

[108] *Id.* at 71 (noting that, according to Paul Graham's testimony, any feature that risked destroying data was out of the question).

[109] *Id.* (noting that the worm worked by exploiting four vulnerabilities in the UNIX operating system that allowed it to rapidly spread across the young internet. As careful as he was, Morris made one miscalculation in his programming. The worm was set to check if a computer was already infected with the worm to ensure that the worm would not reinfect the same computer more than once, but just in case network administrators tried to delete the program, Morris included instructions to have the worm automatically install itself every seventh time. Had Robert chosen a lower reinfection rate, say 1 in 700, "the worm would have spread harmlessly and the brilliant project would have succeeded brilliantly").

[110] *Id.* at 4 (listing affected networks including Cornell, the University of Pittsburgh, the RAND corporation, the University of Minnesota, the Stanford Research Institute, the University of Utah, the Lawrence Livermore National Laboratory, the Los Alamos National Laboratory, and NASA Ames Research Center).

[111] *Id.* at 32.

[112] *Id.* at 56 (explaining that the Department of Justice could either charge Morris with a misdemeanor under section (a)(3) for unauthorized access to a government computer or with a felony under section (a)(5) for unauthorized intrusions that caused $1,000 or more in damages. At the time it was unclear whether an individual needed to both intentionally access a computer and intentionally cause damage).

[113] *Id.* 56-57, 70 (noting that damages under the CFAA can be aggregated and thus the damage was calculated based on all system administrators work in eliminating the worm, patching their systems, and bringing them back online. The total damage was estimated to be $475,000).

[114] *Id.* at 60.

[115] *Id.* at 74.

[116] *Id.*

B. Precedent is Set, Leaving Researchers Liable for Any Damage Caused by Unauthorized Access to Computers.

Morris appealed his conviction, continuing his argument that the CFAA required intent for both unauthorized access and intent to cause damage.[117] Morris argued that the Senate and House comments supported his position.[118] Specifically, he pointed to the Senate Report stating that "the new subsection 1030(a)(5) to be created by the bill is designed to penalize those who *intentionally alter, damage, or destroy* certain computerized data belonging to another."[119] The House Judiciary Committee stated that a new section to the CFAA "can be characterized as a *'malicious damage'* felony violation involving a Federal interest computer."[120] Finally, Morris noted that a member of the House Judiciary Committee referred to the offense as "*'malicious damage'* felony during the floor debate."[121] Unfortunately for Morris, the Second Circuit Court of Appeals disagreed, holding that "[d]espite some isolated language in the legislative history that arguably suggests a scienter component for the 'damages' phrase […], the wording, structure, and purpose of the subsection, […] persuade us that the 'intentionally' standard applies only to the 'accesses' phrase of section 1030(a)(5)(A), and not to its 'damages' phrase."[122] Morris' conviction was upheld, and with it, a message was sent: hackers are criminally liable for any and all damages that result from intentional unauthorized access to a computer.[123] Morris was the first person charged and convicted under the CFAA, despite the good intentions for undertaking his project. While the law and its interpretation by the courts were rigid, history would be much kinder to Morris and the importance of cybersecurity that his work underscored.

[117] United States v. Morris, 928 F.2d 504, 505 (2d Cir. 1991).
[118] *Id.* at 508.
[119] *Id.* (citing Senate Report at 10, U.S. Code Cong. & Admin. News at 2488)(emphasis added).
[120] *Id.* (citing H.R. Rep. No. 99-612, 99th Cong. 2d Sess. at 7 (1986)) (emphasis added).
[121] *Id.* (citing 132 Cong. Rec. H3275, 3276 (daily ed. June 3, 1986) (remarks of Rep. Hughes)) (emphasis added).
[122] *Id.* at 509.
[123] *Id.* at 511.

C. Robert Morris Births an Industry

The computer community was fractured over Morris' actions.[124] Some did not see Morris as the folk hero that did the world a favor for exposing the flaws in the system and refused to accept that it was the computer community's fault for not fixing the flaws sooner.[125] Others noting that Morris' actions were not malicious, praised him for exposing vulnerabilities and poor practices of network administration thereby making the internet safer.[126] One supporter "predicted that history would vindicate Morris: 'When all is said and done, this kid is going to come down as a folk hero.'"[127]

Indeed, history has been kind to Morris. The FBI credits the Morris Worm and the vulnerabilities it exposed with almost independently launching the cybersecurity industry.[128] Within days of the launch of the Morris Worm the Department of Defense set up the country's first computer emergency response team:[129] the CERT/CC at Carnegie Mellon University.[130] Developers began creating computer intrusion detection software.[131] Network administrators began utilizing firewalls to protect their networks.[132] Companies began implementing password management systems.[133] Ironically, Morris achieved the mission he set out on for his PhD thesis and opened the world's eyes to the importance of cybersecurity.[134] While new measures are now

[124] *Shapiro, supra* note 31, at 48.
[125] *Id.* (A sentiment that is still used today to silence cybersecurity researchers).
[126] *Id.* at 49.
[127] *Id.*
[128] *The Morris Worm, 30 Years Since First Major Attack on the Internet*, FBI (Nov. 2, 2018), https://www.fbi.gov/news/stories/morris-worm-30-years-since-first-major-attack-on-internet-110218.
[129] *Id.*
[130] Wikipedia. https://en.wikipedia.org/wiki/CERT_Coordination_Center#History
[131] *Id.*
[132] *What is the Morris Worm? History and Modern Impact*, OKTA (Aug. 29, 2024), https://www.okta.com/identity-101/morris-worm/ [https://perma.cc/9UBN-QEJC].
[133] *Id.*
[134] *Id.*

taken to protect computers from vulnerabilities, the creators of these vulnerabilities remain largely immune from any liability for the damage their creations cause.

IV. THE CFAA CHILLS NECESSARY SECURITY RESEARCH.

The broad language and scope of the CFAA provides myriad ways a researcher may find themselves criminally prosecuted and civilly liable, which has led to a chilling effect on cybersecurity research. In a study by the Center for Democracy & Technology, Participants (researchers and hackers) listed the CFAA as the primary source of risk in their research.[135] Over half of those respondents reported forgoing some research or avoiding research altogether that might bring liability under the CFAA.[136] A large majority of concerns stemmed from the uncertainty around the definition of the term "access", which remains undefined in the CFAA.[137]

The uncertainty of the extent of CFAA applicability has forced researchers to first investigate the legal implications of their work before acting. For instance, when launching a community-led project to improve internet security, Rapid7, a cybersecurity-focused corporation, recommended that anyone planning on contributing to the project first consult an attorney, noting it's

[135] Joseph Lorenzo Hall & Stan Adams, *Taking the Pulse of Hacking: A Risk Basis for Security Research*, Ctr. for Democracy & Tech., March 2018, at 9.

[136] *Id.*

[137] *Id.* ("What this means for researchers is that, when they wish to interface with another machine or system, it is not always clear what they can do. One researcher noted that some servers were configured in a way that essentially allowed unfettered public access, making it impossible to determine what kinds of access the server's owner intended. One researcher reported trying to avoid implicating the CFAA while researching onboard vehicle diagnostic systems where the car was also connected to the manufacturer's servers because of uncertainty about the bounds of authorized access. One subject indicated uncertainty as to how the CFAA might apply to accessing malware hosts. Another noted that, in certain scanning exercises, there was no method by which operators could signal whether or not they authorized access to information on their systems. As a result, the researcher was forced to choose between not conducting the research or potentially running afoul of the CFAA. Although network scanning has, as one subject notes, become a standard practice, many researchers employ methods to make their web traffic readily identifiable to allow operators to send opt-out messages. Another subject noted preference for a method of scanning which results in obtaining zero data, thereby leaving that element of Section 1030(a)(2)(C) unsatisfied.").

impossible to know if scanning computers on the internet won't be violative of the CFAA.[138] It's impossible to know the number of researchers that elected to not contribute to the project, but even if it was just one, that's one less person working to make the internet a more secure space. In this way, the CFAA contributes to the problems faced by the world today by forcing researchers trying to improve cybersecurity to sit on the sidelines while cybercrime continues to increase.

To assist researchers in navigating the legal landscape created in part by the CFAA, the Electronic Frontier Foundation (EFF) created the Coders' Rights Project.[139] The vulnerability reporting FAQ lists ten things a researcher must consider when publishing vulnerability information to limit legal risks. Even these are no guarantee, and researchers remain at risk of retaliation for disclosing vulnerabilities.

In one case, MIT researchers who discovered security vulnerabilities in a mobile voting platform chose to first disclose their findings to the Department of Homeland Services in an attempt to protect themselves from retaliation from the platform's creator.[140] In another instance, researchers discovered a flaw in another voting system that could allow attackers to change votes without detection.[141] Despite the seriousness of their findings, they were forced to limit their research to only publicly facing aspects of the voting system to limit their legal risk.[142] History

[138] Marcia Hofmann, *Legal Considerations for Widespread Scanning*, RAPID7 (Oct. 30, 2013), https://www.rapid7.com/blog/post/2013/10/30/legal-considerations-for-widespread-scanning/ [https://perma.cc/K53W-33GA].
[139] *Coders' Rights Project*, EFF, https://www.eff.org/issues/coders [https://perma.cc/3TWM-7C9Y] (last visited Dec. 18, 2024).
[140] Brief of Amicus Curiae Computer Security Researchers, Electronic Frontier Foundation, Center for Democracy & Technology, Bugcrowd, Rapid7, Scythe, and Tenable in Support of Petitioner, *Van Buren*, 141 S. Ct. 1648, 210 L. Ed. 2d 26, 2020 WL 4005654 at *29. (In addition to having already sought legal assistance from the MIT Technology Law Clinic.).
[141] *Id* at *10.
[142] *Id* at *32.

had already provided ample reason for these and other security researchers to limit their research or otherwise take extraordinary steps in disclosing their findings.

In 2008, three students at MIT discovered vulnerabilities in the Massachusetts Bay Transit Authority's (MBTA) ticketing system.[143] The students planned to showcase their findings at DEFCON, a computer security conference in Las Vegas. [144] The MBTA filed a lawsuit claiming, among other things, violations of the CFAA.[145] Before the students presentation at DEFCON, the court issued a temporary restraining order preventing the students from "providing program, information, software code, or command that would assist another in any material way to circumvent or otherwise attack the of the Fare Media System."[146] The order "pre-emptively gagging security researchers" was unprecedented according the EFF.[147] The charges were eventually dismissed in 2009, but highlighted the legal risk faced by researchers.

In 2010, Andrew Auernheimer disclosed a vulnerability in AT&T servers to media outlet Valleywag, which included over 114,000 email addresses.[148] Auernheimer was charged under

[143] Jon Choate, *MBTA v. Anderson: D. Mass: MIT Students' Security Presentation Merits Temporary Restraining Order*, Jolt Digest (Aug. 15, 2008), http://jolt.law.harvard.edu/digest/mbta-v-anderson [https://perma.cc/9GL9-64KZ] (The students showed that vulnerabilities with the system allowed the CharlieCards to reprogrammed, allowing the money stored on the cards to be increased to $600. They were also able to show that the cards could be read by non-MBTA equipment and this coupled with software written by the students allowed for the cards' encryption to decrypted.).

[144] Call the cops on second thought, Scientific American (Aug. 14, 2008), http://www.scientificamerican.com/blog/post.cfm?id=call-the-cops-on-second-thought-don-2008-08-14 (https://web.archive.org/web/20110320041140/http://www.scientificamerican.com/blog/post.cfm?id=call-the-cops-on-second-thought-don-2008-08-14).

[145] Massachusetts Bay Transportation Authority v. Anderson et al., No. 1:2008cv11364 (D. Mass. Aug. 10, 2008) (Justia).

[146] Temporary Restraining Order, Massachusetts Bay Transportation Authority, No. 1:2008cv11364 at 2 (the Fare Media System was the third-party employed by the MBTA for managing fare tracking, charging, and fare collection) (Justia).

[147]Declan McCullagh, *Judge orders halt to Defcon speech on subway card hacking*, CNET (Aug. 9, 2008), http://news.cnet.com/8301-1009_3-10012612-83.html (https://web.archive.org/web/20090925032115/http://news.cnet.com/8301-1009_3-10012612-83.html).

[148]Timothy B. Lee, *Internet troll "weev" sentenced to 41 months for AT&T/iPad hack,* Ars Technica (Mar. 18, 2013 11:35 AM), https://arstechnica.com/tech-policy/2013/03/auernheimer-aka-weev-sentenced-to-41-months-for-attipad-hack/ (Daniel Spitler discovered the security flaw in AT&T servers that disclosed iPad user's email addresses when sent a unique ICC-ID – the serial number for a SIM card associated with AT&T network. AT&T fixed the

section 18 U.S.C 1030(a)(2)(C), among others, for obtaining information from a protected computer without authorization.[149] Auernheimer argued that he "served the public by exposing AT&T's non-existent security and cavalier disregard of its customer's information."[150] Despite the customer information being exposed on a public-facing webpage, AT&T did not intend for the information to be public, so Auernheimer's discovery and disclosure of the information was deemed without authorization and in violation of the CFAA.[151] That the CFAA criminalized Auernheimer for notifying the public that their private information was publicly exposed rather than AT&T for exposing it can only be described as Kafkaesque. After failing to get the charges dismissed, Auernheimer was convicted and sentenced to 41 months in prison in 2012.[152] Again, the broad language and scope of the CFFA provided wide latitude for criminal prosecution.[153]

A. Recent Legal Developments Provide some Protections but Don't Go Far Enough to Protect Researchers.

Recent decisions and policy changes have served to provide some protection to researchers from criminal prosecution. Those decisions only had an ancillary impact on researchers as they were not addressing the specific use cases for when a researcher might find themselves in violation of the CFAA. However, they did force the Department of Justice to

misconfiguration on their servers, but there was no way of knowing whether attackers took advantage of the misconfiguration prior to its patching.).

[149] United States v. Auernheimer, No. 11-cr-470 (SDW), 2012 U.S. Dist. LEXIS 158849 at *2 (D.N.J. Oct. 26, 2012).

[150] *Id.* at *20.

[151] Karen McVeigh, *Hacker Andrew 'Weev' Auernheimer attempts to overturn conviction*, The Guardian (Mar. 19, 2014, 8:54 EDT), https://www.theguardian.com/technology/2014/mar/19/hacker-andrew-auernheimer-try-overturn-conviction [https://perma.cc/8G22-KFJD].

[152]Joe Silver, *"Weev" prosecutor admits: I don't understand what the hacker's co-conspirator did*, Ars Technica (Mar. 20, 2014, 2:40 PM), https://arstechnica.com/tech-policy/2014/03/lawyers-for-self-described-hacker-weev-contest-his-computer-fraud-conviction/ (reporting that on appeal, Auernheimer argued the CFAA should not apply because visiting a public webpage did not bypass code-based security, but the court vacated his conviction on jurisdictional grounds, leaving the CFAA issue unresolved.).

[153] *Id.; see also* note152 (reporting Hanni Fakhoury, staff attorney at the EFF, believed Auernheimer's case was an example of a prosecution aimed at a person, not a crime.)

reconsider and update their charging policy for “good faith security researchers.” These are steps in the right direction, but as soon discussed, they do not go far enough to protect researchers from criminal liability and are silent on civil liability.

1. Van Buren Limits Some Risks but Leaves Many Questions Unanswered.

In 2021, the Supreme Court addressed the scope of the CFAA for the first time."[154] The Court held that the "exceeds authorized access" clause of the CFAA applies only when an individual “accesses a computer with authorization but then obtains information located in particular areas of the computer—such as files, folders, or databases—that are off-limits to them”[155]. The Court rejected the government's broader interpretation, which would have criminalized violations of purpose-based restrictions on access.[156] The majority reasoned that accepting the government's interpretation would attach criminal penalties to a “breathtaking amount of commonplace computer activity” and allow private parties to make violations of the CFAA via their computer-use policies.[157] However, in a footnote, the Court declined to address whether access violations of the CFAA should rely on “technological (or “code-based”) limitations on access, or instead also looks to limits contained in contracts or policies.”[158] While the Court narrowed the scope of the CFAA with its ruling, as discussed, the majority of the researchers’ activities can be deemed to be “without authorization,” which the Court did not address. Additionally, there is a risk of liability under contract theory or corporate policies, as the

[154] *Van Buren v. United States*, 593 U.S. 374, 381 (2021). (involving Nathan Van Buren, a police sergeant in Georgia, who used his authorized access to a law enforcement database to retrieve information about a license plate in exchange for money from an acquaintance.).

[155] *Id.*

[156] *Id.* at 390. (citing *United States v. Rodriguez*, 628 F. 3d 1258 (CA11 2010); *United States v. John*, 597 F. 3d 263 (CA5 2010); *Int'l Airport Ctrs., L.L.C. v. Citrin*, 440 F. 3d 418 (CA7 2006); *EF Cultural Travel BV v. Explorica, Inc*., 274 F. 3d 577 (CA1 2001); *but see Royal Truck & Trailer Sales & Serv., Inc. v. Kraft,* 974 F. 3d 756 (CA6 2020*); United States v. Valle,* 807 F. 3d 508 (CA2 2015); *WEC Carolina Energy Solutions LLC v. Miller*, 687 F. 3d 199 (CA4 2012); *United States v. Nosal,* 676 F. 3d 854 (CA9 2012).)

[157] *Id.*at 376.

[158] *Id.* at 408.

Court declined to require that a technological barrier be bypassed as the amicus brief submitted by computer security researchers had hoped for.[159]

2. The Ninth Circuit Limits CFAA's Liability for Accessing Public Information.

In 2022, the Ninth Circuit Court of Appeals, on remand in light of its recent *Van Buren* decision, addressed the application of the CFAA to web scraping of publicly available data.[160] The court was left to decide whether hiQ's continued scraping of LinkedIn's public data after receiving the cease-and-desist letter constituted accessing a computer "without authorization" under the CFAA.[161] The court, in its second decision on this case following a remand from the Supreme Court to reconsider in light of Van Buren v. United States, held that hiQ's scraping of public LinkedIn profiles did not violate the CFAA. The court reasoned that the CFAA's "without authorization" provision is best understood as applying only to private information that requires permission or authentication to access.[162] The court held that the CFAA distinguishes between three different kinds of computer systems: "(1) computers for which access is open to the general public and permission is not required, (2) computers for which authorization is required and has been given, and (3) computers for which authorization is required but has not been given."[163] Since LinkedIn's member profiles were public and did not require authorization to view, they fell within the first category of computers, and thus, the court concluded that the CFAA did not apply to hiQ's scraping activities.[164] The decision emphasized that the CFAA was primarily designed to combat hacking and unauthorized access to private information, not to police the use of public

[159] *Supra* note 7, at 17.

[160] hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180 (9th Cir. 2022) (involving a data analytics company, that scraped public profile information from LinkedIn's website until LinkedIn sent a cease-and-desist letter and implemented technical measures to prevent scraping.).

[161] *Id.* at 1195.

[162] *Id.* at 1201.

[163] *Id.* at 1197-98.

[164] *Id.*

data.[165] The ruling implies that if information is publicly available on a website without authentication or password protection, a violation of the terms of service or defiance of a cease-and-desist letter will not give rise to liability under the CFAA. [166] While the ruling is a good start in protecting researchers, but this is just one circuit that has further narrowed the applicability of the CFAA. Questions still remain whether other circuits will come to the same conclusion, leaving researchers in the same limbo that split circuit courts had forced the Supreme Court to interpret in *Van Buren v. United States*. 2022 was a banner year for attempts to limit research liability under the CFAA and the courts weren't the only ones to get in on the action.

3. DOJ Policy Shields "Good-Faith" Researchers from Criminal Prosecution.

In 2022, the Department of Justice (DOJ) announced a new policy of no longer charging security researchers acting in "good faith" with CFAA violations.[167] The policy change was partially prompted by the Supreme Court's ruling in *Van Buren* and, like the Court, falls short of requiring the defeat of a technical limitation for computer access to be unauthorized.[168] This means that written policies, "such as when an employee violates a contract that puts certain files off limits in all situations, or when an outsider receives a cease-and-desist (C&Ds) letter informing them that their access is now unauthorized," may still give rise to criminal prosecution

[165] *Id.* at 1201.

[166] *Id.* at 1200 (While this article is solely focused on the risk the CFAA imposes on researchers, the court noted other causes of action available to "victims of data scraping" including trespass to chattels, copyright infringement, misappropriation, unjust enrichment, conversion, breach of contract, or breach of privacy.).

[167] 9-48.000 – Computer Fraud and Abuse Act, https://www.justice.gov/opa/press-release/file/1507126/dl [https://perma.cc/4H22-8CUT](Adopting the definition of "good faith security research" as "accessing a computer solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in a manner designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices, machines, or online services to which the accessed computer belongs, or those who use such devices, machines, or online services. Security research not conducted in good faith – for example, for the purpose of discovering security holes in devices, machines, or services in order to extort the owners of such devices, machines, or services – might be called "research" but is not in good faith.").

[168] Andre Crocker, *DOJ's New CFAA Policy is a Good Start But Does Not Go Far Enough to Protect Security Researchers*, EFF (May 19, 2022), https://www.eff.org/deeplinks/2022/05/dojs-new-cfaa-policy-good-start-does-not-go-far-enough-protect-security [https://perma.cc/X85Y-KBW8].

under the CFAA.[169] Additionally, the new policy isn't binding on the courts and can be rescinded at any time.[170] Even if it were, what constitutes "good faith security research" isn't black and white and even the definition provided by DOJ constitutes mostly examples of research activities that may or may not be covered by the policy.[171] Even if a defendant tries to convince the DOJ that their actions are "good faith security research," it cannot be used as an affirmative defense.[172] If the DOJ brings a charge under the CFAA, "good faith security research" is not grounds for dismissal.[173] Thus, while this policy change by the DOJ at least expresses an understanding of the importance of security research and seeks to limit criminal liability, it does nothing to shield researchers from the risk of frivolous and overly broad CFAA civil litigation.[174]

Unfortunately, the risk of being sued civilly for reporting a discovered vulnerability to the affected party remains.[175] Brian Krebs, a cybersecurity expert who runs krebsonsecurity.com, reports that when researchers reach out to seek advice on how best to report a security vulnerability, it's not criminal prosecution they are most worried about but rather "[i]t's that they're going to get sued by the company responsible for the security vulnerability or data leak."[176] Given these concerns and the failure of Congress and the courts to provide more protection for researchers, efforts in the private sector have been made to mitigate this risk. Bug bounties and Vulnerability Disclosure Programs (VDP) present some promise in protecting security researchers, but they come with their own limitations.

[169] *Id.*
[170] *Id.*
[171] *Supra* note 164.
[172] *What Counts as "Good Faith Security Research?",* KrebsonSecurity (Jun. 3, 2022), https://krebsonsecurity.com/2022/06/what-counts-as-good-faith-security-research/ [https://perma.cc/5MJU-Y9WU].
[173] *Id.*
[174] *See supra* note 165.
[175] *See supra* note 169.
[176] *Id.*

B. Researchers Attempt to Protect Themselves by Responsibly Disclosing Vulnerabilities to Companies Only Goes as Far as Those Companies Willing to Adopt Them.

In 2001, a hacker, known as Rain Forest Puppy (RFP), released his "disclosure policy for publishing information about security holes," which could be used to serve others who were searching for bugs and vulnerabilities.[177] The purpose was to try to standardize the process by which researchers and vendors could work together on security bug disclosures.[178] RFP laid out this framework to avoid vendors trying to blame researchers who found the bug and vice versa, researchers trying to blame vendors for shoddy work or rushing to launch a product before it was fully secure.[179] RFP's disclosure policy was designed to start communication between vendors and researchers to "get the bugs fixed."[180] While this disclosure policy was initiated from the researcher's side, RFP did find vendors receptive to the process, including Microsoft and other smaller software vendors.[181]

The concept of voluntary vulnerability disclosure was slowly integrated into vendors' processes. In a process that began in 2005, the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) released ISO/IEC 29147.[182] ISO/IEC 29147 sought to standardize the process by which vulnerabilities are disclosed.[183] For security researchers, this means having a "process through which vendors and vulnerability

[177] Kim Zetter, *Three Minutes with Rain Forest Puppy*, PCWorld.com (Sept. 28, 2001), http://pcworld.com/news/article/0%2Caid%2C63944%2C00.asp (https://web.archive.org/web/20010930194040/http://pcworld.com/news/article/0,aid,63944,00.asp).

[178] *Id.*

[179] *Id.*

[180] *Id.*

[181] *Id.*

[182] *A brief history of vulnerability disclosure*, disclose.io, https://disclose.io/history/ [https://perma.cc/DE76-3B5Q] (last visited Dec. 18, 2024).

[183] *Vulnerability disclosure*, ISO, https://www.iso.org/obp/ui/#iso:std:iso-iec:29147:ed-1:v1:en [https://perma.cc/Z8NJ-GEH2](The goal of vulnerability disclosure was four-fold according to ISO/IEC: "a) ensuring that identified vulnerabilities are addressed; b) minimizing the risk from vulnerabilities; c) providing users with sufficient information to evaluate risks from vulnerabilities to their systems; [and] d) setting expectations to promote positive communication and coordination among involved parties.") (last visited Dec. 18, 2024).

finders may work cooperatively in finding solutions that reduce the risks associated with a vulnerability."[184] While introducing this standard was undoubtedly important, not all vendors follow ISO/IEC standards and the policy is paywalled.

The Cybersecurity & Infrastructure Security Agency (CISA) has released its vulnerability disclosure policy template for agencies seeking to implement a disclosure policy.[185] The policy lays out guidelines for research, appropriate test methods, and the scope of testing.[186] Whether additional government agencies choose to adopt CISA's recommended template is up to those agencies. Where to find information about which agencies have adopted a VDP and how to find their VDP is not listed, leaving researchers to either track down this information, accept the risk of liability should an agency not have a VDP, or forgo research altogether.

Efforts to standardize VDPs continued when Disclose.io was formed in 2018.[187] Disclose.io seeks to standardize vulnerability disclosure programs and to have them include "'safe harbor' language that protects well-intended hackers from legal action[.]"[188] The lack of consistency and absence of "safe harbor" language is a deterrent to disclosing bugs for those who discover them.[189] The project hopes that including standard language in contracts will provide an

[184] *Id.*
[185] *Vulnerability Disclosure Policy* Template, CISA (last accessed Dec. 18, 2024), https://www.cisa.gov/vulnerability-disclosure-policy-template [https://perma.cc/ZL29-TDDN] (The policy outlines an authorization section that reads: "If you make a good faith effort to comply with this policy during your security research, we will consider your research to be authorized, we will work with you to understand and resolve the issue quickly, and *AGENCY NAME* will not recommend or pursue legal action related to your research. Should legal action be initiated by a third party against you for activities that were conducted in accordance with this policy, we will make this authorization known.")
[186] *Id.*
[187] Sean Gallagher, *New open source effort: Legal code to make reporting security bugs safer,* Ars Technica https://arstechnica.com/information-technology/2018/08/new-open-source-effort-legal-code-to-make-reporting-security-bugs-safer/#gsc.tab=0 (Disclose.io is a collaborative project that expanded on the work done by Bugcrowd and CipherLaw's Open-Source Vulnerability Disclosure Framework, Amit Alazari's #legalbugbounty, and Dropbox's call to protect security researchers.) (Aug. 2, 2018, 8:00 AM).
[188] *Id.*
[189] *Id.*

opportunity to "foster security research instead of stifling it."[190] To make finding information on VDPs easier, a database of companies and information on where to find their vulnerability disclosure policy is available for anyone to search.[191] However, the database does not show which, if any, of these programs have adopted the standard language recommended by disclose.io and only one program is listed as having a full "safe harbor" provision.[192] Without further voluntary adoption of the standard contract language, however, researchers still lack protections for the security research they perform.

In 2022, the quest for standardizing vulnerability disclosure continued when the Internet Engineering Task Force (IETF) introduced RFC 9116.[193] RFC 9116 seeks to standardize where researchers can find information about a company's disclosure policy directly from the company's website. Information includes who to contact, a URL to the company's disclosure policy, and the expiration of the policy.[194] This year, Cloudflare, a DNS provider, created a dashboard to make it easy for web domain administrators to incorporate and encourage adoption of this standard.[195] As with all attempts to make vulnerability disclosure more transparent and standardized, RFC 9116 only goes so far as the company is willing to adopt it.

However, even in instances where a company has adopted a disclosure program or bug bounty, security researchers have still face the threat of CFAA charges. For instance, when drone manufacturer DJI implemented a bug bounty program, they told computer researcher Kevin

[190] *Id.*

[191]Disclose.io, *Programs*, https://disclose.io/programs/ [https://perma.cc/BPB5-YPJX] (As of this writing there are 2,388 entries in the database that can help security researchers find the vulnerability disclosure policy of vendors.) (last accessed Dec. 18, 2024).

[192] *Id.*

[193] *RFC 9116, A File Format to Aid in Security Vulnerability Disclosure*, IETF (Apr. 2022), https://www.rfc-editor.org/rfc/rfc9116 [https://perma.cc/SDS8-5ZNX].

[194] *Id.* (An example of Google's sexurity.txt page can be found at https://www.google.com/.well-known/security.txt).

[195] Alexandra Moraru and Sam Khawase, *Enhance your website's security with Cloudflare's free security.txt generator,* Cloudflare (Oct. 6, 2024), https://blog.cloudflare.com/security-txt/ [https://perma.cc/TS3W-S3TU].

Finisterre that security issues with their servers were covered under the program.[196] When Finisterre discovered vulnerabilities that could allow an attacker to access user's private information, DJI did an about-face, telling Finisterre that the company's servers weren't covered under the bounty program after all, threatening Finisterre with CFAA charges.[197] In another example, Voatz, a digital election system manufacturer, implemented a VDP to ensure their systems were secure. When an undergraduate student, relying on the terms of the VDP, began performing security research on Voatz's systems they were reported to the FBI by Voatz.[198] The student's research complied with the terms of the VDP at the time the research was undertaken, but Voatz publicly claimed that the student's work violated the terms of the VPD – the terms they claim were violated were added later only when word of their referral of the student to the FBI was made public.[199] An additional issue is that while there are guidelines in creating a VDP to provide safe harbor or limit liability under the CFAA, ultimately researchers are bound by the terms the company chooses to set.[200] Frequently, this includes a provision that a researcher may not disclose any discovered vulnerabilities to any entity but the company itself.[201] Should a researcher discover a serious vulnerability exposing customers to risk and report it to the company under their VDP, only to find that the company made no efforts to fix the security issues, the researcher may not disclose the issue to affected parties, the public, or law enforcement without exposing themselves to the risk of litigation for violating the CFAA.[202] As

[196] *Supra* note 7, at 31 (citing 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/.).

[197] *Id.*

[198] *Id.* at 32 *(*citing 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).

[199] *Id.*

[200] *Id.* at 33 (providing an example of a corporate VDP policy can be found at https://ziphq.com/trust/security but note this serves only as an example and this article makes no claims as to the merits of this particular VDP.).

[201] *Id.*

[202] *Id.*

previously discussed, it is not mere conjecture; companies frequently avoid fixing the vulnerabilities in their products and often deny they exist until a breach or security incident is made public.[203]

Without Congressional action to amend the CFAA once again, researchers will, despite the myriad efforts undertaken, always be reliant on the whims of judicial holdings, changes in prosecution policies, or discretion of private corporations to determine whether their work will fall afoul of the CFAA.

V. CFAA AMENDMENT PROPOSALS THAT LIMIT SECURITY RESEARCHER LIABILITY.

Congress has several courses of action it could take to amend the CFAA and limit liability under the CFAA for researchers. Any or all of them would offer protections, allowing researchers to work without fear. Many of these are not new; they have been presented by legislators, advocated for by interest groups, or suggested legal experts in the field. This article will present these arguments for amending the CFAA and conclude with a seemingly counterintuitive point: that increasing corporate liability could actually reduce researchers' liability.

A. Redefining "Without Authorization" to Include Code-Based Access Restriction.

In response to the death of internet activist Aaron Swartz[204], H.R. 2454 – Aaron's Law Act of 2013 was introduced in the House of Representatives.[205] The bill sought to redefine "access without authorization" as "obtaining information on a protected computer that the accessor lacks authorization to obtain by knowingly circumventing one or more technological or

[203] *Id.* at 33-34.
[204] Wikipedia, https://en.wikipedia.org/wiki/Aaron_Swartz.
[205] H.R. 2454, 113th Cong. (2013).

physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information."[206] Requiring the bypassing of some technological measure would provide some protection to legitimate researchers, but instances where technological measures were meant to be in place but improperly configured might still give rise to liability under the CFAA.[207] For this reason, the EFF made a recommendation that went further, not only shielding researchers from liability for ineffective access control but also explicitly providing that violations of terms of service, agreements, or contractual obligations would not give rise to liability under the CFAA.[208] These amendments would go where the *Van Buren* Court was unwilling: requiring that access without authorization requires defeating a technological barrier while eliminating criminalization of a breach of contract. While this proposal seeks to limit a researcher's criminal liability under the CFAA, the next proposal would provide researchers protection from civil liability.

B. Safe Harbor for "Good Faith Security Researchers."

The threat of civil action looms large for security researchers and, given the new DOJ policy, is likely the largest risk they face.[209] Rapid7 proposal for security researcher protections

[206] *Id.*

[207] *See* United States v. Auernheimer, 2012 U.S. Dist. LEXIS 158849, 2012 WL 5389142 (finding potential CFAA liability where AT&T claimed it did not intend for customer records to be public and noting that databases configured with blank passwords may still give rise to liability if accessed without authorization.).

[208] *EFF CFAA Revisions – Penalties and Access*, EFF (last accessed Dec. 18, 2024), https://www.eff.org/document/eff-cfaa-revisions-penalties-and-access [https://perma.cc/4WQK-WUSX] (adding the following to the definitions under 18 U.S.C. § 1030 (e): The term "access without authorization" means to circumvent technological access barriers to a computer, file, or data without the express or implied permission of the owner or operator of the computer to access the computer, file, or data, but does not include circumventing a technological measure that does not effectively control access to a computer, file, or data. The term "without the express or implied permission" does not include access in violation of a duty, agreement, or contractual obligation, such as an acceptable use policy or terms of service agreement, with an Internet service provider, Internet website, or employer).

[209] *Supra* note 169; *see also* Harley Geiger, *Proposed security researcher protection under CFAA*, RAPID7 (June 4, 2021), https://www.rapid7.com/blog/post/2021/06/04/proposed-security-researcher-protection-under-cfaa-2/ [https://perma.cc/FT8H-XSM5].

is multi-faceted. First, the proposal would limit the circumstances under which a civil action may be brought.[210] Next, like the aforementioned DOJ policy, which takes its definition from the DMCA Sec. 1201 protections for researchers, Rapid7's proposal would define "good faith security research" but improves upon it by including actions that legitimate security researchers would take: "such a minimizing any damage and making an effort to disclose any discovered vulnerabilities to the computer owner."[211] The definition is more well-defined than the DMCA and DOJ counterparts, recognizing the importance of not being overbroad given that most security research involves computers that the researcher does not own.[212] In addition to a more robust definition of "good faith security research," Rapid7's proposal includes an affirmative defense for conduct that involves subclause (c)(4)(A)(i)(I) allowing researchers to avoid liability should they face a civil suit while acting solely for "good faith security research."[213] This aspect of the proposal provides civil protections, where the DOJ policy was unwilling to go for criminal liability. The proposal would be a great step in protecting legitimate security researchers, but as with most proposals to "fix" the CFAA is not without caveat. For instance, "good faith security researcher" is defined by requiring responsible disclosure of any vulnerabilities discovered as part of the research. As discussed previously, even the act of disclosing vulnerabilities has given rise to threats of civil action under the CFAA. Concerns remain about swinging the pendulum in the other direction by providing overly broad protections that attackers may invoke disingenuously to escape liability for their malicious acts.[214] Rather than providing safe harbor

[210] *Proposed security researcher protection for the Computer Fraud and Abuse Act (CFAA),* Rapid7 (June 6, 2021), https://www.rapid7.com/globalassets/_pdfs/policy/proposed-security-protection-researcher-cfaa.pdf [https://perma.cc/RB35-32RH] ("A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).").
[211] *Id.*
[212] *Id.*
[213] *Id.*
[214] *Id.*

protections for researchers that may be weaponized by attackers, another proposal seeks to shield researchers by redefining a different core term used to determine civil liability under the CFAA: "loss."

C. Amending the Definition of "Loss"

In her well-researched law review article, Riana Pfefferkorn puts forth a novel proposal to protect security researchers from civil liability by amending the CFAA's "loss" definition.[215] In a two-pronged approach, the proposal would 1) amend the definition of "loss" to prevent the costs of remediating a disclosed vulnerability alone, absent any other alleged loss, from meeting the $5,000 threshold and 2) add a fee-shifting provision, shifting litigation costs from defendants to plaintiffs' whose losses do not meet that threshold.[216] The proposal would put an external security researcher reporting a vulnerability to a company on the same legal ground as a member of a company's internal security team. In the latter case, there is nobody for the company to sue; "fixing what the internal team found is just the cost of doing business."[217] Absent any other harm, the company is not a victim of cybercrime as they have suffered no loss, freeing security researchers from the risk of civil liability for responsibly disclosing vulnerabilities.[218] The second proposed amendment would then work as a shield to protect researchers from meritless claims or claims that cannot meet the $5,000 loss threshold without including costs of vulnerability remediation.[219] The risk of being liable for the costs of a defendant's legal fees will deter companies from pursuing meritless claims, but would serve as no barrier for instances

[215] Riana Pfefferkorn, *Shooting the Messenger: Remediation of Disclosed Vulnerabilities as CFAA "Loss,"* 29 RICH. J.L. & TECH. 89 (2022).
[216] *Id.* at 91.
[217] *Id.* at 146.
[218] *Id.*
[219] *Id.* at 157. proposing to add the following sentence to the end of section 1030(g): "In a civil action for violation of this section brought pursuant to subclause (I) of subsection (c)(4)(A)(i), the court in exceptional cases may award reasonable attorney fees and costs to the prevailing party").

where a plaintiff can show they suffered actual "loss" as defined by the proposal.[220] While this fee-shifting arrangement would work to protect researchers who are certain their work has caused no harm, the reality of the work performed by researchers is not so black and white. In interviews with researchers, Brian Krebs notes that while the risk of costly civil litigation for reporting vulnerabilities weighs on researchers, nearly as often researchers expressed unease in reporting vulnerabilities because their research may have gone "just a tad too far."[221] This proposal would likely not shield researchers that, while operating in "good faith," accidentally cause some harm. Where a researcher cannot be sure of the outcome of their research, they may still find themselves at risk of civil liability, even under the changes proposed.

D. Remove Immunity from Civil Liability from Corporations.

All the proposed solutions thus far, would offer significant protections for security researchers while not completely eliminating the risks that researchers face. Even so, even a slightly flawed solution is better than none and given the ever-increasing rise in cybercrime and vulnerabilities waiting to be exploited by hackers, we cannot afford to forgo good solutions in search of the perfect one. It is with that in mind that this article proposes its flawed suggestion for amending the CFAA.

While previous proposals all center around decreasing security researchers' exposure to civil liability under the CFAA, this article proposes increasing exposure to civil liability for "loss" caused by vendor software or hardware vulnerabilities. To achieve this, this article proposes amending section 1030(g) by removing the last line reading: "[n]o action may be brought under

[220] *Id.*

[221] *Supra* note 169 (noting that some common examples include: 1) researchers finding a vulnerability in a database and downloading the entire set of records rather than what would be required for proof-of-concept; and 2) automated scanning that may have actually caused downtime issues that have already been flagged by a company's internal team as a potential cybersecurity attack).

this subsection for the negligent design or manufacture of computer hardware, computer software, or firmware." At first glance, amending the CFAA to once again provide for a civil remedy for "loss" caused by software and hardware companies' products may seem especially punitive, but the purpose is not to punish corporations but to incentivize their cooperation with security researchers.

Software companies have been largely immune to lawsuits for damages as a result of vulnerabilities present in their software. Courts have largely been silent on whether software is a "product," particularly when the software operates as a service or deals primarily with ideas and content, allowing software companies to escape liability under the strict product liability doctrine.[222] According to Thomas F. McKim, author of a treatise on business torts, "despite past dire warnings that software and computers will result in the application of strict liability under product liability law, this has not happened."[223] The economic loss rule also prevents recovery through a tort cause of action when the damage from a software vulnerability affects a person or property but is solely monetary.[224] The ILOVEYOU attack resulted in $10 billion in damages[225], but none would be recoverable because none was physical damage or pain and suffering from a physical injury. Software companies also take steps to immunize themselves from liability through contracts law. Software is generally not "sold" but licensed, subject to end-user license

[222] 4 BUSINESS TORTS § 35.06 (2024) ("This lack of guidance from the courts results from several factors. First, when software is 'defective,' it is likely that any damages would be covered by contract law rather than tort law. These defects do not usually result in injury to other property or personal injury. Second, software often is sold in such a manner that the buyer must agree to the seller's terms which often includes a provision for arbitration. Third, off-the-shelf software is typically not so expensive that buyer is going to sue the creator of the software for alleged defects. Instead, the buyer is apt to purchaser another software program to accomplish the intended goal. Fourth, for the most part, software functions as intended. Finally, software which is apt to result in personal injury is part of a tangible product which uses the software in a computer component. If damages result to person or other property, the resulting lawsuit will concern the tangible product which incorporates the computer and its software.").

[223] *Id.*

[224] Jay M. Feinman, *The Economic Loss Rule and Private Ordering*, 48 ARIZ. L. REV., 813 (2006) ("The most general statement of the economic loss rule is that a person who suffers only pecuniary loss through the failure of another person to exercise reasonable care has no tort cause of action against that person.").

[225] *See supra* note 105.

agreements (EULA) or terms of service (TOS).[226] These agreements typically include anti-consumer terms that "disclaim all warranties and limit remedies to a nominal amount such as $100 or the amount paid in licensing fees."[227] When Congress amended the CFAA in 2001 to provide immunity for software companies, these clickwrap agreements were in their infancy, but since then, they have evolved and ingrained themselves into our everyday internet-connected lives.[228]

There is a risk that removing immunity from civil liability may stifle innovation that we all so profoundly covet and have come to expect from tech companies. However, given the current crisis with internet security and our reliance on software in our daily lives, holding tech companies liable for damage caused by their products would serve as a deterrent to releasing products that have not been properly vetted and tested. More importantly for security researchers, it will serve to incentivize these companies to work *with* security researchers who report vulnerabilities before they can be weaponized, making both the internet safer and, in a strange turn of events, helping to shield those companies from civil liability under the CFAA.

[226] 1 COMPUTER CONTRACTS § 1.01 (2024).

[227] 1 COMPUTER CONTRACTS § 1.01 (2024) (listing additional anti-consumer terms include "an exclusion of warranties, limitation of remedies, the impositions of conditions of use, prohibition of reverse engineering, restrictions on assignability and transferability, and exclusions of indemnification obligations.").

[228] *Id.*