Richmond Journal of Law & Technology

Volume 29 | Issue 1 Article 3

11-30-2022

Shooting the Messenger: Remediation of Disclosed Vulnerabilities as CFAA "Loss"

Riana Pfefferkorn
Stanford Internet Observatory

SHOOTING THE MESSENGER: REMEDIATION OF DISCLOSED VULNERABILITIES AS CFAA "LOSS"

Riana Pfefferkorn*

Cite as: Riana Pfefferkorn, Shooting the Messenger: Remediation of Disclosed Vulnerabilities as CFAA "Loss," 29 RICH. J.L. & TECH. 89 (2022).

* Research Scholar, Stanford Internet Observatory. The Internet Observatory's funding sources are available at https://cyber.fsi.stanford.edu/io/news/stanford-internet-observatory-two-years. Thanks to Dan Bateyko and to participants in the 2022 Cybersecurity Law and Policy Scholars Conference for their helpful comments and suggestions on an earlier draft, and to the hardworking staff of the Richmond Journal of Law and Technology. This article is dedicated to the memories of Peter Eckersley, Elliot Harmon, Dan Kaminsky, Dmitry Karshtedt, and Sherwin Siy.

Abstract

The Computer Fraud and Abuse Act (CFAA) provides a civil cause of action for computer hacking victims that have suffered certain types of harm. Of these harms, the one most commonly invoked by plaintiffs is having suffered $5,000 or more of cognizable "loss" as defined by the statute. In its first-ever CFAA case, 2021's *Van Buren v. United States*, the Supreme Court included intriguing language that "loss" in civil cases should be limited to "technological harms" constituting "the typical consequences of hacking." To date, lower courts have only followed the Court's interpretation if their circuit already interpreted "loss" narrowly pre-*Van Buren* and have continued to approach "loss" broadly otherwise.

Van Buren did not fully dissipate the legal risks the CFAA has long posed to a particular community: people who engage in good-faith cybersecurity research. Discovering and reporting security vulnerabilities in software and hardware risks legal action from vendors displeased with unflattering revelations about their products' flaws. Research activities have even led to criminal investigations at times. Although *Van Buren* narrowed the CFAA's scope and prompted reforms in federal criminal charging policy, researchers continue to face some legal exposure. The CFAA still lets litigious vendors "shoot the messenger" by suing over security research that did them no harm. Spending just $5,000 addressing a vulnerability is sufficient to allow the vendor to sue the researcher who

reported it, because such remediation costs qualify as "loss" even in courts that read that term narrowly.

To mitigate the CFAA's legal risk to researchers, a common proposal is a statutory safe harbor for security research. Such proposals walk a fine line between being unduly byzantine for good-faith actors to follow and lax enough to invite abuse by malicious actors. Instead of the safe harbor approach, this article recommends a simpler way to reduce litigation over harmless research: follow the money.

The Article proposes (1) amending the CFAA's "loss" definition to prevent vulnerability remediation costs alone from satisfying the $5,000 standing threshold absent any other alleged loss, and (2) adding a fee-shifting provision that can be invoked where plaintiffs' losses do not meet that threshold. Tightening up the "loss" calculus would disqualify retaliatory litigation against beneficial (or at least benign) security research while preserving victims' ability to seek redress where well-intended research activities do cause harm. Fee-shifting would deter weak CFAA claims and give the recipients of legal threats some leverage to fight back. Coupled with the *Van Buren* decision, these changes would reach beyond the context of vendor versus researcher: they would help rein in the CFAA's rampant misuse over behavior far afield from the law's core anti-hacking purpose.

I. INTRODUCTION

[1] The Computer Fraud and Abuse Act (CFAA)[1] is the nation's federal computer trespass statute. It prohibits trespass and damage to or theft from a computer and allows victims to recover civilly for the "loss" incurred in responding to an intrusion.[2]

[2] As "an anti-hacking statute,"[3] the CFAA has hindered cybersecurity progress by treating those who seek to fix cybersecurity shortcomings the same as those who seek to exploit them. The law is so broad that it can be read to prohibit not just malicious computer intrusions and destruction, but also research that aims in good faith to improve the state of computer security by finding digital security vulnerabilities and reporting them to the product vendors.[4] These activities are chilled by the threat of liability under the CFAA.

[3] The Supreme Court's first-ever CFAA case, 2021's *Van Buren v. United States*,[5] somewhat reined in the law's scope. It thus partially mitigated the legal threat to security researchers, especially by prompting

[1] Computer Fraud and Abuse Act of 1986, 18 U.S.C. § 1030.

[2] 18 U.S.C. §§ 1030(a)(2), (a)(5), (e)(11), (g); *see also* Robert Chesney, *Cybersecurity Law, Policy, and Institutions* 17 (U. of Texas Law, Pub. Law Research Paper No. 716, Aug. 23, 2021) (framing the statute as one involving trespass and theft).

[3] United States v. Nosal, 676 F.3d 854, 857 (9th Cir. 2012) (en banc).

[4] JOSEPH LORENZO HALL & STAN ADAMS, TAKING THE PULSE OF HACKING: A RISK BASIS FOR SECURITY RESEARCH 8–11 (2018), https://josephhall.org/papers/2018-03-27-Risk-Basis-for-Security-Research-FNL.pdf [https://perma.cc/9SQG-GZLD]; Cybersecurity Information Sharing Act, 6 U.S.C. § 1501(17) ("The term 'security vulnerability' means any attribute of hardware, software, process, or procedure that could enable or facilitate the defeat of a security control.").

[5] Van Buren v. United States, 141 S. Ct. 1648 (2021).

changes in federal criminal charging policy. However, some risk remains, principally of civil litigation. Although *Van Buren* narrowly interpreted "loss" in the civil context to "focus on technological harms,"[6] a review of subsequent CFAA decisions reveals that lower courts have not followed the Court's lead unless their precedent already favored a narrow reading of that term.[7]

[4] The CFAA's definition of "loss" is why, even after *Van Buren*, vendors can threaten legal action against security researchers. If a vendor spends enough money investigating and repairing (or "patching") a flaw (or "bug"), the Act grants the vendor standing to file suit and "shoot the messenger" who brought the vulnerability to its attention. For a vendor that finds and patches its own bugs, there is nobody to sue; repairs are part of the cost of doing business. Yet, if a vulnerability is found and reported by an outsider rather than an insider, the CFAA lets a vendor externalize its remediation costs onto the outsider, even where the outsider has done no damage to the vendor's computer systems. This is comparable to someone who, having "enter[ed] a doorway with no lock," alerts the building owner to the insecure entryway, only to be "held liable for the cost of installing a lock afterwards."[8] *Van Buren* does not foreclose such "shooting the messenger" lawsuits.

[5] To shield good-faith security researchers from legal risk, commentators have frequently proposed adding a "safe harbor" to the CFAA for researchers' activities. After critiquing the safe-harbor approach, this Article suggests an alternative way to protect researchers from civil liability: amending the Act to (1) preclude vulnerability remediation costs

[6] *Id.* at 1659–60.

[7] *See infra* Section IV.B.

[8] Note, *Immunizing the Internet, or: How I Learned to Stop Worrying and Love the Worm*, 119 HARV. L. REV. 2442, 2454 (2006) (criticizing the "loss" definition as "overinclusive" because patching costs are "money that one should reasonably expect users to spend anyway" upon discovery of a security flaw, "regardless of whether their systems have been attacked.").

alone from supplying statutory standing and (2) shift fees onto civil plaintiffs who prove unable to meet the revised statutory standing bar. This proposal would deter legal threats over beneficial research while preserving liability in instances of bad-faith or malicious conduct or where well-intended research goes awry.

II. THE COMPUTER FRAUD AND ABUSE ACT

[6] The CFAA is "a civil and criminal anti-hacking statute designed to prohibit the use of hacking techniques to gain unauthorized access to electronic data."[9] At a high level, the CFAA prohibits two types of conduct: accessing a computer without authorization and exceeding authorized access to a computer.[10] To grasp why these prohibitions pose a threat to security researchers requires understanding a few additional provisions of the statute.

A. Obtaining Information from a Protected Computer

[7] Several offenses under the CFAA require the involvement not merely of a computer, but of a "protected computer."[11] As defined by the Act, "protected computer" means any computer or device that can connect to the Internet.[12]

[9] Cvent, Inc. v. Eventbrite, Inc., 739 F. Supp. 2d 927, 932 (E.D. Va. 2010).

[10] *See* 18 U.S.C. §§ 1030(a), (b), (e)(1).

[11] 18 U.S.C. §§ 1030(a)(2)(C), (a)(4), (a)(5), (a)(7).

[12] *Id.* § 1030(e)(2)(B) ("[T]he term 'protected computer' means a 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[.]").

[8] This loose definition of "protected computer" is part of what makes one of the Act's substantive offenses, subsection 1030(a)(2)(C), very broad in scope. Subsection 1030(a)(2)(C) is "[t]he least demanding CFAA provision."[13] It requires only that the defendant "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer[.]"[14] It does not require that the defendant cause (or threaten to cause) any harm to the protected computer, in contrast to several other subsections of the statute.[15] Nor does this subsection specify what kind of information must be obtained or how much.[16] Obtaining "*some* information—*any* information" is enough.[17]

[9] This combination of "protected computer" and "obtaining information" makes the language of subsection (a)(2)(C) worryingly broad in scope. "Because a 'protected computer' is any computer with internet access, and 'obtain' includes merely viewing information, any person who intentionally views information on a computer can potentially incur liability

[13] Samantha Jensen, Comment, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81, 94 (2013).

[14] 18 U.S.C. § 1030(a)(2)(C).

[15] *Compare id.* (no harm or threat requirement), *with id.* §§ 1030(a)(5), (7) (requiring that a defendant cause harm or threaten to cause harm).

[16] *Compare id.* § 1030(a)(2)(C) (prohibiting obtaining mere "information from any protected computer"), *with id.* § 1030(a)(2)(A)–(B) (prohibiting obtaining financial records or information from any United States agency).

[17] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1578 (2010); *see also id.* at 1567 ("Since most forms of unauthorized access will reveal information to read, even if it is only the prompts or graphic interface provided to those with access, the new § 1030(a)(2) effectively criminalized all interstate hacking."); United States v. Auernheimer, 748 F.3d 525, 537–38 (3d Cir. 2014) ("The crime is complete even if the offender never looks at the information and immediately destroys it, or the victim has no idea that information was ever taken.").

depending on how the court interprets authorization." [18] For years, subsection (a)(2)(C) was recognized for having the potential to be treated as "an overwhelmingly overbroad enactment" that would criminalize large swaths of innocuous behavior unless it was narrowly interpreted by the courts.[19] The Supreme Court rejected such a result in 2021, siding with the narrower interpretation adopted by several courts of appeal.[20] However, all of those cases limited the statute's scope by reading "authorization" narrowly — not by limiting what "obtains information" requires.[21]

B. "Loss" for Purposes of Civil Claims

[10] In addition to criminal penalties, the CFAA also provides a private right of action to "[a]ny person who suffers damage or loss by reason of a violation of [the statute.]"[22] The Act limits the bases on which a civil action

[18] Jensen, *supra* note 13, at 94 n.86 (citing S. Rep. No. 99-432, at 6 (1986)).

[19] United States v. Drew, 259 F.R.D. 449, 466 (C.D. Cal. 2009).

[20] Van Buren v. United States, 141 S. Ct. 1648, 1653–54 (2021) (discussing the split between circuits that took "a broader view" and those that took the narrower view propounded by the defense).

[21] *Id.* at 1662 ("In sum, an individual 'exceeds authorized access' when he 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 him."); United States v. Nosal, 676 F.3d 854, 859–60 (9th Cir. 2012) (en banc); Jensen, *supra* note 13, at 130–31 ("Since obtaining information from a protected computer translates into viewing any information on any computer, the court [in *Nosal*] correctly surmised that adopting the government's definition [of 'exceeds authorized access'] would impermissibly 'transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved.'"); *see also* Sandvig v. Barr, 451 F. Supp. 3d 73, 91 (D.D.C. 2020) ("The Court agrees with the clear weight of relevant authority and adopts a narrow interpretation of . . . 'accesses . . . without authorization' that excludes terms-of-service violations.").

[22] 18 U.S.C. §§ 1030(c), (g).

may be brought, of which the most common is "loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value."[23] The CFAA defines "loss" to mean, as relevant here, "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense."[24] If the plaintiff fails to allege losses of at least $5,000, the CFAA claim will be dismissed for lack of jurisdiction.[25]

[11] The federal courts differ in how broadly they construe this definition, particularly the "cost of responding to an offense" portion. The Ninth Circuit reads the definition as "a narrow conception of 'loss,'" limited to "harms caused by computer intrusions, not general injuries unrelated to the hacking itself."[26] Similarly, district courts in the Second Circuit limit the "loss" definition's "cost of responding to an offense" language to "situations involving damage to or impairment of the protected computer."[27] Likewise, district courts in the Eighth Circuit have repeatedly

[23] *Id.* §§ 1030(c)(4)(A)(i)(I), (g); BRENDA R. SHARTON ET AL., KEY ISSUES IN COMPUTER FRAUD AND ABUSE ACT (CFAA) CIVIL LITIGATION (2022), Westlaw W-014-6206 ("Plaintiffs typically rely on the first factor, which requires proof that the computer fraud caused a combined loss of at least $5,000 to one or more persons during any one-year period."); U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES 42 (2010), https://www.justice.gov/criminal/file/442156/download [https://perma.cc/N8SF-DB2N] ("Of these enumerated harms, prosecutors most commonly charge loss.").

[24] 18 U.S.C. § 1030(e)(11).

[25] *See* Nick Akerman, *Why Two District Courts Dismissed Valid Computer Fraud and Abuse Claims for Lack of Jurisdiction*, CASETEXT (Sept. 1, 2010), https://casetext.com/analysis/why-two-district-courts-dismissed-valid-computer-fraud-and-abuse-claims-for-lack-of-jurisdiction-1 [https://perma.cc/32C9-WNJS].

[26] Andrews v. Sirius XM Radio Inc., 932 F.3d 1253, 1262–63 (9th Cir. 2019); Calendar Research LLC v. StubHub, Inc., No. 17-CV-04062, 2020 U.S. Dist. LEXIS 112361, at *79 (C.D. Cal. May 13, 2020) ("[A] [p]laintiff must show [its] loss is related to [defendant's] allegedly unlawful access.").

[27] Better Holdco, Inc. v. Beeline Loans, Inc., No. 20-CV-8686, 2021 U.S. Dist. LEXIS 138908, at *8–10 (S.D.N.Y. July 26, 2021) ("In assessing whether certain costs are

held that "[t]he weight of relevant authority restricts the CFAA 'loss' requirement to actual computer impairment[,]" with Third Circuit district courts ruling similarly.[28]

[12] The Fourth Circuit, by contrast, has called the "loss" definition a "broadly worded provision."[29] The Sixth and Eleventh Circuits also ostensibly employ a broader reading,[30] although the Sixth Circuit recently

properly considered the 'cost of responding to an offense,' [Second Circuit district courts] focus on the connection between the plaintiff's response and 'damage to or impairment of the protected device.'" (citing 18 U.S.C. § 1030(e)(11)). In tension with this "damage or impairment" requirement, other Southern District decisions have allowed "loss" to include the cost of investigations that ultimately found no actual damage. *See id.* at *10–11 (citing Kaufman v. Nest Seekers, LLC, No. 05-CV-6782, 2006 U.S. Dist. LEXIS 71104, at *24–25 (S.D.N.Y. Sept. 26, 2006); Univ. Sports Publ'ns Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 387 (S.D.N.Y. 2010)).

[28] Burnett v. Grundy, No. 14-00301-CV, 2014 U.S. Dist. LEXIS 192624, at *5 (W.D. Mo. Oct. 28, 2014) (citing Dewitt Ins., Inc. v. Horton, No. 13-CV-2585, 2014 U.S. Dist. LEXIS 72384, at *10 (E.D. Mo. May 28, 2014)); Volpe v. Abacus Software Sys. Corp., No. 20-10108, 2021 U.S. Dist. LEXIS 112641, at *15–16 (D.N.J. June 16, 2021). *But see* Ervin & Smith Advert. & Pub. Rels., Inc. v. Ervin, No. 08-CV-459, 2009 U.S. Dist. LEXIS 8096, at *25–27 (D. Neb. Feb. 3, 2009) (rejecting defendant's argument that "loss" must be constrained to "the physical damage done to Plaintiff's computer system only.").

[29] A.V. *ex rel.* Vanderhye v. iParadigms, LLC, 562 F.3d 630, 646 (4th Cir. 2009). District courts in the Fourth Circuit have relied on this language when counting as "loss" expenses that seem loosely tethered to repairing the alleged intrusion. *E.g.*, Space Sys./Loral, LLC v. Orbital ATK, Inc., 306 F. Supp. 3d 845, 852–53 (E.D. Va. 2018) ("[Plaintiff] presents the costs it incurred as a result of the alleged CFAA violation that included conducting a damage assessment and convening and communicating with NASA and [Defendant] regarding the alleged breach."); Estes Forwarding Worldwide LLC v. Cuellar, 239 F. Supp. 3d 918, 927–28 (E.D. Va. 2017) (allowing "loss" to include the cost of plaintiff's lawsuit against Comcast to uncover defendant's identity as the Comcast subscriber whose IP address was used to improperly access plaintiff's Google Drive account).

[30] Brown Jordan Int'l, Inc. v. Carmicle, 846 F.3d 1167, 1173 (11th Cir. 2017); Yoder & Frey Auctioneers, Inc. v. EquipmentFacts, LLC, 774 F.3d 1065, 1073-74 (6th Cir. 2014).

opined that the "loss" definition "confirm[s] the Act's narrow scope" by "aim[ing] at preventing the typical consequences of hacking" (as distinguished from misuse of information), language the Supreme Court borrowed when interpreting the CFAA the following year.[31]

[13] The statutory "loss" definition has received occasional attention in academic literature. On the one hand, it has been criticized for enabling harsher penalties in criminal CFAA cases, where victim losses heavily influence sentencing,[32] because courts let hacking victims tally their own costs with little rigor or scrutiny.[33] Victims control how much time and resources they expend "responding to an offense," and courts accept the dollar numbers victims submit without question.[34] Plus, the value of employees' and consultants' time makes $5,000 a low bar to hit.[35] On the

[31] Van Buren v. United States, 141 S. Ct. 1648, 1660 (2021) (quoting Royal Truck & Trailer Sales & Serv. v. Kraft, 974 F.3d 756, 760 (6th Cir. 2020)).

[32] United States v. Agarwal, 24 F.4th 886, 889 (3d Cir. 2022) ("Under the United States Sentencing Guidelines (USSG), the recommended prison term is influenced heavily by the loss suffered by the victims.").

[33] *See* James T. Graves et al., *Perception Versus Punishment in Cybercrime*, 109 J. CRIM. L. & CRIMINOLOGY 313, 321 (2019) ("[T]he CFAA is prone to inflated loss calculations.").

[34] Jennifer Granick, *Faking It: Calculating Loss in Computer Crime Sentencing*, 2 I/S: J.L. & POL'Y FOR INFO. SOC'Y 207, 215, 221–22 (2006) ("Damage from an offense is a function of the idiosyncrasies of incident investigation, including the skills, experience, hourly rate, and remediation choices of the victim, and not necessarily the offender's actions.").

[35] "It is well settled that the value of time for employees who investigate [the defendant's] access qualifies as a loss." Shawn E. Tuma, *What Does the CFAA Mean and Why Should I Care?—A Primer on the Computer Fraud and Abuse Act for Civil Litigators*, 63 S.C. L. REV. 141, 187 (2011). Perhaps $5,000 was a meaningful amount in 1986, but these days it is a fraction of the cost of hiring an incident response firm after an attack. *See* Mike Burgard, *Cyber Incident Response: The Real Cost of Not Having a Plan or Cyber Insurance*, MARCO (May 25, 2021), https://www.marconet.com/blog/cyber-incident-response [https://perma.cc/4XXK-ZXYW]; Andrea M. Matwyshyn & Stephanie K. Pell, *Broken*, 32 HARV. J.L. & TECH. 479, 557 n.408 (2019) ("[I]n light of the time value of

other hand, courts' narrow interpretation of "loss" in the civil context was recently critiqued for denying Americans the CFAA as a vehicle for remedying the alleged unwanted collection and misuse of their private information by corporate defendants.[36]

[14] All told, however, out of the ample academic literature about the CFAA, little focuses on the "loss" provision.[37] This may surprise practicing lawyers, since what losses courts will count for standing purposes is a question of great consequence to practitioners litigating CFAA claims (and of course, to their clients).[38] For example, the CFAA has been invoked repeatedly in consumer privacy lawsuits, but courts almost always dismiss the claim due to plaintiffs' inability to meet the $5,000 jurisdictional minimum, because "the loss of personal information is not a cognizable loss under the statute."[39] The meaning of "loss" is frequently dispositive in civil litigation, yet it is rarely examined in CFAA scholarship.

---

money, even the statutory minimum amount of $5000 required by 18 U.S.C. 1030(g) translates to at least $8000 in 2018 dollars.").

[36] *See* Alicia Nakhjavan, Note, *The "Worst Law in Technology": How the Computer Fraud and Abuse Act Allows Big Businesses to Collect and Sell Your Personal Information*, 87 BROOK. L. REV. 1077, 1087 (2022) ("This limited definition of loss has prevented many Americans from obtaining the relief the CFAA offers, particularly when the claim is based on a loss of personal privacy.").

[37] *E.g.*, Ioana Vasiu & Lucian Vasiu, *Break on Through: An Analysis of Computer Damage Cases*, 14 PITT. J. TECH. L. & POL'Y 158, 186–192 (2014); George Roach & William J. Michiels, *Damages Is the Gatekeeper Issue for Federal Computer Fraud*, 8 TUL. J. TECH. & INTELL. PROP. 61, 62 (2006).

[38] *Cf.* Sharton et al., *supra* note 23 (providing practical guidance to practitioners on this issue); Tuma, *supra* note 35, at 182–88 (pairing guidance to civil litigators on how to sufficiently plead the $5,000 threshold with specific examples of what has and has not constituted a loss in court decisions).

[39] Nakhjavan, *supra* note 36, at 1081–82, 1087–95. While in private practice from 2011 to 2015, the author of this Article defended clients in multiple consumer privacy class actions where her case team successfully obtained the dismissal of the CFAA claim on just these grounds.

III. THE CFAA'S THREAT TO SECURITY RESEARCH

[15] One aspect of the CFAA that has been well-documented is the chilling effect the law has had on the field of cybersecurity research. For years, the CFAA has been an object of fear for security researchers. A history of civil lawsuits and even criminal charges stemming from research activities has induced the understandable concern that their work could expose them to liability due to the law's notoriously broad substantive scope.[40]

A. "Hackers" and Vulnerability Disclosure

[16] The community of people who look for computer security vulnerabilities is large and diverse. It encompasses a range of different motivations and goals, including mere curiosity, thrill-seeking, extortion, academic interest, a desire to fix problems, and the urge to wreak havoc.[41] Everyone in the community, regardless of their motivation, falls under the banner of "hackers," notwithstanding the negative connotation the word carries. In fact, malicious hackers comprise only a fraction of this community.[42] Malicious individuals are commonly referred to as "black hat" hackers, "motivated by mischief or profit rather than by actually fixing vulnerabilities and security flaws."[43] Unlike black hat hackers, "white hat" (or "ethical") hackers seek to improve cybersecurity by finding

[40] *See, e.g.*, Hall & Adams, *supra* note 4; Nat Meysenburg, *Cybersecurity Research Should Not Be a Crime: Why We Need Clear, Permanent CFAA and DMCA Exemptions*, NEW AM. (Nov. 18, 2021), https://www.newamerica.org/oti/briefs/cybersecurity-research-should-not-be-a-crime/ [https://perma.cc/GLA5-SC8N].

[41] Ido Kilovaty, *Freedom to Hack*, 80 OHIO ST. L.J. 455, 480 (2019).

[42] *Id.*

[43] *Id.* at 482.

vulnerabilities in hardware and software.[44] White hat hackers then disclose such vulnerabilities in a manner that makes them likely to be fixed (or "patched"), all while taking measures to do minimal harm in the process.[45] White hats may operate under contract with vendors (which also typically employ their own internal security teams), although independent white-hat vulnerability researchers far outnumber contractors and internal employees.[46] White hat hacking is the category of activity this Article contemplates when referring to "good faith" security research.

[17] In between white and black hats are "gray hat" hackers, whose motivations are more ambiguous.[47] Some may have the same goals as white hats but are more willing to break the law in looking for bugs and to go public with their findings in order to draw attention to vulnerabilities and shame vendors into fixing them.[48] Other gray hats may have financial motives more akin to black hats, leading them to monetize the vulnerabilities they find by selling that information to third parties rather than disclosing vulnerabilities to the vendor so they can be patched.[49]

---

[44] *Id.* at 481.

[45] *Id.* ("It would be best . . . to define white hats as hackers who seek to improve security while minimizing possible harm to the vulnerable target by neither exploiting the vulnerability nor selling it to malicious actors."); Cassandra Kirsch, *The Grey Hat Hacker: Reconciling Cyberspace Reality and the Law*, 41 N. KY. L. REV. 383, 385–86 (2014).

[46] Alexander Gamero-Garrido et al., *Quantifying the Pressure of Legal Risks on Third-party Vulnerability Research*, *in* CC'17: PROC. OF THE 2017 ACM SIGSAC CONF. ON COMPUT. & COMMC'NS SECURITY 1501 (2017), https://acmccs.github.io/papers/p1501-gamero-garridoA.pdf [https://perma.cc/53VE-CWN6].

[47] *See* Kilovaty, *supra* note 41, at 483; Kirsch, *supra* note 45, at 386.

[48] Kilovaty, *supra* note 41, at 482 ("Another distinction made [between white and gray hats] in literature is based on disclosure: hackers disclosing vulnerabilities directly to the vendor are white hats, while those publicizing vulnerabilities to the broader public are considered gray hats.") (footnote omitted); Kirsch, *supra* note 45, at 388.

[49] Kilovaty, *supra* note 41, at 483.

[18] Given the diversity of the security community, it should come as little surprise that there is a longstanding difference of opinion about how best to disclose vulnerabilities.[50] That is because the consequences of disclosure can vary depending on how broad the dissemination is (*i.e.*, to the vendor only versus the public at large) and what those who receive the disclosure do with that knowledge.[51] Disclosing a bug ought to improve security by prompting the vendor to patch the bug (rather than sweeping it under the rug and leaving users at risk).[52] However, disclosure can also impair security. Releasing detailed information about the flaw to the general public instead of the vendor could enable malicious actors to exploit it before the vendor can release a patch.[53]

[19] There are several types of disclosure commonly used within the security community. The first approach is generally known as "full disclosure." A hacker who uses full disclosure releases the details of the bug to the public without first notifying the vendor, so that either the vendor will be pressured into fixing the bug or, if the vendor takes no action, affected users can act to protect themselves.[54] Compare that with "responsible disclosure," wherein a researcher first reports a bug to the vendor and allows the vendor some time to fix the bug before publicly disclosing it.[55] However, there is still disagreement over what exactly responsible

[50] *Id.* at 505 ("[T]here should be consensus on how to disclose vulnerabilities in an acceptable manner. At present, the philosophy on disclosure is highly fragmented and context-dependent.").

[51] *Id.* at 513.

[52] *See* Kirsch, *supra* note 45, at 388; Kilovaty, *supra* note 41, at 514.

[53] Kirsch, *supra* note 45, at 388.

[54] Kilovaty, *supra* note 41, at 516–17.

[55] *Id.* at 514–16.

disclosure means in this context.[56] Next, a "coordinated vulnerability disclosure" is when a researcher reports a vulnerability to the vendor (or to a relevant government agency that can in turn notify the vendor) and the parties then work collaboratively throughout the reporting, investigation, and remediation process before any party makes a public disclosure of the vulnerability.[57] Coordinated vulnerability disclosure is a form of responsible disclosure.[58] Finally, those who wish to exploit vulnerabilities for their own ends (such as black hats and intelligence agencies) favor "nondisclosure," in which the actor does not report the discovered vulnerability.[59]

[20] To encourage the responsible reporting of vulnerabilities (and harness hackers into playing by a set of rules), many organizations now publish vulnerability disclosure programs (VDPs), which invite hackers to test the organization's products for flaws and report what they find.[60] Organizations might also offer "bug bounty" programs (often hosted by a third-party platform), in which hackers are paid rewards for finding and

[56] *Id*. This Article's proposal for protecting good-faith security research sidesteps the debate over what counts as "responsible disclosure." For our purposes, it does not matter precisely how someone disclosed a vulnerability; it matters only that they were the messenger who notified the vendor of it. *See infra* Section VI.B.

[57] *Coordinated Vulnerability Disclosure*, MICROSOFT SEC. RESPONSE CTR., https://www.microsoft.com/en-us/msrc/cvd [https://perma.cc/5LEB-RHWH].

[58] DANIEL ETCOVITCH & THYLA VAN DER MERWE, COMING IN FROM THE COLD: A SAFE HARBOR FROM THE CFAA AND THE DMCA § 1201 FOR SECURITY RESEARCHERS 12–13 (2018), https://dash.harvard.edu/bitstream/handle/1/37135306/ComingOutoftheCold_FINAL.pdf?sequence=1&isAllowed=y [https://perma.cc/LD3Y-TBTW].

[59] Kilovaty, *supra* note 41, at 514.

[60] Jasmine Arooni, Note, *Debugging the System: Reforming Vulnerability Disclosure Programs in the Private Sector*, 73 FED. COMMC'N L.J. 443, 445 n.6 (2021).

reporting vulnerabilities in compliance with terms set by the bounty offeror; these are effectively monetized VDPs.[61]

B. Legal Risk to Researchers Under the CFAA

[21] One reason that VDPs and bug bounties exist is to establish, through contract, "an alternative legal regime for facilitating ethical hacking," amidst a statutory landscape that is "not well tailored to accommodate 'white-hat' security research."[62] Along with other federal and state laws, the CFAA has long posed a serious risk of civil and criminal liability to security researchers, which paradoxically impedes rather than promotes the goal of better security.[63]

[22] The CFAA has always posed a risk to researchers, even in its early days. An early CFAA criminal prosecution involved a graduate student whose research into the poor state of network security on the then-nascent Internet went awry in late 1988, wreaking havoc on computer networks around the country.[64] The CFAA has continued to cast a pall over security

[61] *Id.*; *see* Kirsch, *supra* note 45, at 397; Gamero-Garrido et al., *supra* note 46, at 1503.

[62] Amit Elazari, *Private Ordering Shaping Cybersecurity Policy: The Case of Bug Bounties*, *in* REWIRED: CYBERSECURITY GOVERNANCE 232 (Ryan Ellis & Vivek Mohan eds., 2019); *see* Arooni, *supra* note 60, at 445 n.6.

[63] *See generally* Hall & Adams, *supra* note 4 (listing the CFAA as a primary source of legal risk to researchers, along with the Digital Millennium Copyright Act (DMCA), 17 U.S.C. §§ 512, 1201–1205, 1301–1332); SUNOO PARK & KENDRA ALBERT, A RESEARCHER'S GUIDE TO SOME LEGAL RISKS OF SECURITY RESEARCH 6–23 (2020), https://clinic.cyber.harvard.edu/files/2020/10/Security_Researchers_Guide-2.pdf [https://perma.cc/MAM5-CHBZ] (listing the CFAA, the DMCA, copyright, contract, trade secrets, export control, and federal wiretapping laws as sources of legal risk).

[64] United States v. Morris, 928 F.2d 504 (2d Cir. 1991); *see also* Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1159 (2016) ("[*United States v. Morris* was] [t]he very first federal appellate case on the meaning of authorization in the CFAA[.]").

research in the years since.[65] Discovering and reporting security vulnerabilities may draw legal threats from vendors, notwithstanding a researcher's responsible disclosure practices.[66] Vendors "tend to get testy when deficiencies in their products and services are unceremoniously exposed[,]" and hackers have in the past been enjoined from, and even criminally prosecuted for, publishing unflattering research findings.[67]

[23] The advent of VDPs and bug bounties has in some respects only perpetuated the problem of researchers bearing liability by enabling vendors to control outside research into their products while providing little legal assurance to the researcher in return.[68] The terms of these programs are often poorly drafted, voluminous, and impose onerous requirements on researchers, making compliance difficult.[69] At the same time, these terms often do not contain strong contractual protections from liability for researchers, and indeed tend to allocate legal risk to the participant.[70]

---

[65] *See Computer Fraud and Abuse Act (CFAA)*, NAT'L ASS'N CRIM. DEF. LAW., https://www.nacdl.org/Landing/ComputerFraudandAbuseAct [https://perma.cc/8FEN-GMPH].

[66] Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453, 1466–67 (2016); Gamero-Garrido et al., *supra* note 46, at 1501; Hall & Adams, *supra* note 4, at 12.

[67] Mayer, *supra* note 66, at 1466–67; Kilovaty, *supra* note 41, at 501–02.

[68] Thomas E. Kadri, *Digital Gatekeepers*, 99 TEX. L. REV. 951, 977–82 (2021); Elazari, *supra* note 62, at 11–12; Kilovaty, *supra* note 41, at 504.

[69] Arooni, *supra* note 60, at 451 ("Poorly crafted legal terms may subject a researcher to unknown liability, while overly-restrictive terms muzzle researchers and discourage research."); Elazari, *supra* note 62, at 24 ("[H]ackers are expected to master (and read) around twenty to thirty pages before submitting a bug, and also debate how to address potential conflicts: a considerable informational burden.").

[70] Kilovaty, *supra* note 41, at 504 ("[D]ue to differences in bargaining power, as well as stakes, the contractual language does not always provide for a 'safe harbor' for security researchers."); Elazari, *supra* note 62, at 26 (stating that common practice in VDP and bug bounty legal terms "shifts the legal risk to the hacker"); *see also* ETCOVITCH & VAN DER MERWE, *supra* note 58, at 39 ("[T]he disclosure schedule is entirely determined by

[24] As a result of this hostile legal environment, good-faith researchers have been scared to undertake research projects that might expose them to liability.[71] This is bad news for the rest of us. Discussions of the CFAA's legal threat have "emphasized that cybercrime liability is, in fact, backfiring: by chilling vital research, cybercrime law actually reduces computer security."[72] The law's chilling effect on security testing means vulnerabilities may go undiscovered, or at least unreported to the affected vendors.[73] Legal interpretations of the CFAA that blurred "the line between malicious hacking and researching for security vulnerabilities" have historically served only to "give[] cyber security researchers a disincentive to find security flaws, which makes the rest of us less safe" from malicious activity.[74] That is why not just cybersecurity researchers, but the public at large, had so much riding on the outcome of a court case about a crooked cop.[75]

---

the vendor, assuming the finder would like to avoid having legal action levied against them. . . . [I]f a finder actively agrees to participate in a bug bounty program, then she submits to the vendor-determined publication deadline and the conditions stated within the terms of such a program.").

[71] *See* Hall & Adams, *supra* note 4, at 9.

[72] Mayer, *supra* note 66, at 1467.

[73] Kilovaty, *supra* note 41, at 509 ("The CFAA's strict liability for access 'without authorization' is certainly a major threat to security researchers. At the same time, it discourages talented researchers from engaging responsibly with vendors.").

[74] Kirsch, *supra* note 45, at 394*; see also* Trevor A. Thompson, *Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of "White Hats" Under the CFAA*, 36 FLA. ST. U.L. REV. 537, 562–63 (2009) ("[T]his overbroad reach effectively isolates an ethical hacking community that would otherwise both reinforce positive norms within the hacking community and provide the benefits of increased cooperation between ethical hackers and law enforcement.").

[75] *See, e.g.*, Amit Yoran, *The Future of Cybersecurity Law Hinges On The Supreme Court*, FORBES (Nov. 16, 2020, 12:55 PM), https://www.forbes.com/sites/amityoran1/2020/11/16/the-future-of-cybersecurity-law-hinges-on-the-supreme-court/?sh=6afa7fa5528a [https://perma.cc/KU6Z-SCM5] ("The Court's ruling will either be a

IV. *VAN BUREN V. UNITED STATES*

[25] In June 2021, the Supreme Court decided its first-ever CFAA case, *Van Buren v. United States*.[76] The decision was hailed for reining in the scope of the CFAA's "exceeds authorized access" provision.[77] To bolster its conclusion, the Court also weighed in on the meaning of "loss" in the context of civil claims, construing the term narrowly to focus on "technological harms."[78]

---

significant win for the security community, setting the legal parameters for legitimate security research[,] or a detrimental roadblock, pushing security researchers into perilous situations and society into the digital Dark Ages."); Joseph Marks & Tonya Riley, *The Cybersecurity 202: There's finally a Supreme Court battle coming over the nation's main hacking law*, WASH. POST (Apr. 24, 2020, 7:30 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2020/04/24/the-cybersecurity-202-there-s-finally-a-supreme-court-battle-coming-over-the-nation-s-main-hacking-law/5ea1ade6602ff140c1cc5f51/ [https://perma.cc/A8KV-Z3RP] ("If the court agrees to narrow how prosecutors can use the law, it would be a huge victory for security researchers. . . . It would also make the Internet far safer, [cybersecurity professionals] say. . . That's because current interpretations of [the CFAA], have made researchers wary of revealing bugs they find because they fear getting in trouble . . .").

[76] 141 S. Ct. 1648 (2021).

[77] *E.g.*, Orin S. Kerr, *The Supreme Court Reins in the CFAA in* Van Buren, REASON: VOLOKH CONSPIRACY (June 9, 2021, 8:32 PM), https://reason.com/volokh/2021/06/09/the-supreme-court-reins-in-the-cfaa-in-van-buren [https://perma.cc/Y47T-VDHU] ("*Van Buren* is a major victory for those of us who favor a narrow reading of the CFAA."); David G. Savage, *Unusual Supreme Court majority narrows scope of computer anti-hacking law,* L.A. TIMES (June 3, 2021, 12:21 PM), https://www.latimes.com/politics/story/2021-06-03/unusual-supreme-court-majority-narrows-scope-of-anti-hacking-computer-law [https://perma.cc/MJD6-CC3A] ("The [American Civil Liberties Union] welcomed the decision as 'an important victory for civil liberties and civil rights enforcement in the digital age.'").

[78] *Van Buren*, 141 S. Ct. at 1659–60.

[26] *Van Buren* involved a police officer who had authorization to access a police department database, but who searched it for a corrupt purpose in violation of the department's acceptable-use policy.[79] This search prompted the officer's prosecution and conviction under the CFAA's "exceeds authorized access" provision.[80] The Court granted certiorari in order to resolve a circuit split that had persisted for the better part of a decade over whether the "exceeds authorized access" provision applied "only to those who obtain information to which their computer access does not extend," or whether it also reached "those who misuse access that they otherwise have."[81]

[27] The Court adopted the narrower interpretation, holding that "an individual 'exceeds authorized access' when he 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 him."[82] Using information one is authorized by the computer owner to access, but for an impermissible purpose, is not "exceeding authorized access."[83] The contrary interpretation, the Court reasoned, "would attach criminal penalties to a breathtaking amount of commonplace computer activity[,]" such as checking personal email or sports scores at work in violation of an employer's computer-use policy.[84] If it "exceeds authorized access" to misuse one's otherwise permissible computer access, "then millions of otherwise law-abiding citizens are criminals."[85] The Court

[79] *Id.* at 1653.

[80] *Id*.

[81] *Id.* at 1653–54.

[82] *Id.* at 1662.

[83] *Id.* at 1661–62.

[84] *Van Buren*, 141 S. Ct. at 1661–62.

[85] *Id.* at 1661.

declined to read the statute so broadly, and accordingly overturned Mr. Van Buren's conviction under section 1030(a)(2).[86]

A. Impact on Good-Faith Security Research

[28] *Van Buren* reduced the threat the law poses to security researchers by stating that violations of policies or agreements are not CFAA violations too. Going forward, the Court's ruling should shield researchers from liability for "exceeding authorized access" under the CFAA if they violate a vendor's terms of service or other contractual clauses (such as in a VDP or bug bounty program) that put constraints on how the researcher may gather information and what uses she may make of it.[87]

[29] The decision has induced federal law enforcement to change its stance toward security research. [88] In May 2022, almost a year after the *Van Buren* decision, the Department of Justice revised its charging policy for the CFAA.[89] In a move that surprised the cybersecurity community, the DOJ announced that going forward, federal prosecutors "should decline prosecution if available evidence shows the defendant's conduct consisted

[86] *Id.* at 1662.

[87] Aaron Mackey & Kurt Opsahl, *Van Buren is a Victory Against Overbroad Interpretations of the CFAA, and Protects Security Researchers*, ELEC. FRONTIER FOUND. (June 3, 2022), https://www.eff.org/deeplinks/2021/06/van-buren-victory-against-overbroad-interpretations-cfaa-protects-security [https://perma.cc/N3GA-PBG3]; Timothy Edgar, *Why Van Buren Is Good News for Cybersecurity*, LAWFARE (Aug. 4, 2021, 10:18 AM), https://www.lawfareblog.com/why-van-buren-good-news-cybersecurity [https://perma.cc/U22F-LNFM].

[88] *Department of Justice Announces New Policy for Charging Cases under the Computer Fraud and Abuse Act*, U.S. DEP'T OF JUST. (May 19, 2022), https://www.justice.gov/opa/pr/department-justice-announces-new-policy-charging-cases-under-computer-fraud-and-abuse-act [https://perma.cc/9ZVB-L5T7] [hereinafter *DOJ Press Release*].

[89] U.S. Dep't of Just., Just. Manual § 9-48.000 (2022) [hereinafter *DOJ Charging Policy*].

of, and the defendant intended, good-faith security research."[90] This is a significant move that may allay some of the historical fears surrounding the CFAA.

[30] The new policy adopts the definition of "good-faith security research" adopted by the Copyright Office in the 2021 triennial rulemaking under the Digital Millennium Copyright Act (DMCA).[91] To wit:

> "good faith security research" means 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.[92]

[31] The DOJ policy continues: "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."[93]

---

[90] *Id.*

[91] *See* 37 CFR § 201.40(b)(16).

[92] *Id.* (quoting U.S. COPYRIGHT OFF., SECTION 1201 RULEMAKING: EIGHTH TRIENNIAL PROCEEDING TO DETERMINE EXEMPTIONS TO THE PROHIBITION ON CIRCUMVENTION 258 (2021)).

[93] *DOJ Charging Policy*, *supra* note 89.

[32] The May 2022 policy replaces the Department's previous CFAA charging policy from 2014,[94] which listed factors for federal prosecutors to consider (such as the need for deterrence and the sensitivity of the system or information affected) when deciding whether a CFAA prosecution "should be pursued because a substantial federal interest would be served by prosecution."[95] It is possible to interpret the new policy as recognition that the "federal interest" is better served by encouraging rather than punishing researchers' efforts to improve the nation's cybersecurity.[96] This view is bolstered by Deputy Attorney General Lisa Monaco's statement in a press release about the new policy: "[c]omputer security research is a key driver of improved cybersecurity . . . and today's announcement promotes cybersecurity by providing clarity for good-faith security researchers who root out vulnerabilities for the common good."[97]

[33] To hear some DOJ officials tell it, the new policy is practically superfluous. According to DAG Monaco's statement, "[t]he department has never been interested in prosecuting good-faith computer security research

[94] *DOJ Press Release*, *supra* note 88 (indicating that the 2022 policy supersedes prior 2014 policy with immediate effect).

[95] Memorandum from Eric H. Holder, Jr., Att'y Gen., to the U.S. Att'ys & Assistant Att'y Gens. for the Crim. & Nat'l Sec. Divs. (Sept. 11, 2014), https://www.eff.org/files/2017/03/14/15-1_ex_to_mtd_reply_-_charging_memo.pdf [https://perma.cc/TZM4-RQ3M].

[96] *See* Riana Pfefferkorn, *America's anti-hacking laws pose a risk to national security*, BROOKINGS: TECHSTREAM (Sept. 7, 2021), https://www.brookings.edu/techstream/americas-anti-hacking-laws-pose-a-risk-to-national-security/ [https://perma.cc/2U4H-H2SA] (commenting on the status of public and private cybersecurity while highlighting legal risk as a barrier to good-faith cybersecurity research); Kimberly Adams & Daniel Shin, *"Good faith" hackers get a break from the government*, MARKETPLACE TECH (May 25, 2022), https://www.marketplace.org/shows/marketplace-tech/good-faith-hackers-get-a-break-from-the-government/ [https://perma.cc/PTB9-SMFT] (acknowledging an administrative shift due to the timing of the new DOJ policy).

[97] *DOJ Press Release*, supra note 88.

as a crime[.]"[98] Further, according to Leonard Bailey, who heads the Cybersecurity Unit of the DOJ's Computer Crime and Intellectual Property Section (CCIPS), there has been only one CFAA prosecution in the past decade against a security researcher.[99]

[34] However, the Department's claims do not paint the full picture. Given the chance, the DOJ had previously refused to disavow that it might someday prosecute researchers for CFAA violations.[100] The existence of only one recent prosecution does not imply that that defendant was the only researcher *investigated* by the federal government in the last ten years. (Prosecutions in open court are just the tip of the law enforcement iceberg, and the number of investigations that did not culminate in prosecution cannot be easily quantified. Plus, federal investigators do not tend to publicize the details of open investigations.[101]) The new charging policy is therefore significant, despite Department officials' downplaying its importance and despite the existing dearth of prosecutions.

[98] *Id.*

[99] Derek B. Johnson, *The (still) unanswered questions around the CFAA and 'good faith' security research*, SC MEDIA (June 6, 2022), https://www.scmagazine.com/analysis/rsac/the-still-unanswered-questions-around-the-cfaa-and-good-faith-security-research [https://perma.cc/Y6R3-NDLK]. Bailey did not specify the defendant in that case; without that information, it is not possible to evaluate whether that prosecution would now be disfavored under the new policy.

[100] Van Buren v. United States, 141 S. Ct. 1648, 1661 (2021) ("the Government stops far short of endorsing" limitations that might "cabin its prosecutorial power") (citing Sandvig v. Barr, 451 F. Supp. 3d 73, 81–82 (D.D.C. 2020)); *Sandvig*, 451 F. Supp. 3d at 81 ("[A]dvisory and non-binding statements and Department of Justice policies do not eliminate the reasonable fear of prosecution.").

[101] *See Can I obtain detailed information about a current FBI investigation that I see in the news?*, FBI, https://www.fbi.gov/about/faqs/can-i-obtain-detailed-information-about-a-current-fbi-investigation-that-i-see-in-the-news [https://perma.cc/P9CF-46JB].

[35] The DOJ's policy is undeniably an important step forward in restoring trust between the security community and the authorities charged with protecting the public. Nevertheless, it cannot fully assuage researchers' fears. For one thing, this is a non-binding policy, not a law.[102] Even if charging good-faith researchers is disfavored, a prosecutor would still have the discretion to do so.[103] Additionally, the policy does not forbid investigating researchers over their work. Nor could it: after all, a determination that particular research counts as good faith (and so the researcher should be let off the hook) will surely require some amount of government scrutiny.[104] Researchers may reasonably wonder how intrusive that process might be.[105] Finally, the DOJ policy has no effect on prosecutions under state-level anti-hacking laws. State laws remain a source of potential criminal liability for security research. Indeed, a Missouri journalist was recently threatened with prosecution by the state governor for responsibly disclosing serious flaws he had found in a state agency website.[106]

---

[102] *Sandvig*, 451 F. Supp. 3d at 81 (emphasizing the 2014 version of the policy).

[103] *See Van Buren*, 141 S. Ct. 1648 at 1661–62 (emphasizing the discretionary nature of the plain language in the 2014 version of the policy).

[104] The good-faith determination is to be made on "available evidence," and prosecutors can consult CCIPS about how it applies in specific situations. *DOJ Charging Policy*, *supra* note 89.

[105] For a firsthand account of the stressful experience of a federal criminal CFAA investigation (one infamous for culminating in the defendant's suicide), see Quinn Norton, "Life Inside the Aaron Swartz Investigation," THE ATLANTIC (Mar. 3, 2013), https://www.theatlantic.com/technology/archive/2013/03/life-inside-the-aaron-swartz-investigation/273654/ [https://perma.cc/UV62-HMDP].

[106] *See* Rachel Treisman, *A Missouri newspaper told the state about a security risk. Now it faces prosecution*, NPR (Oct. 14, 2021, 4:37 PM), https://www.npr.org/2021/10/14/1046124278/missouri-newspaper-security-flaws-hacking-investigation-gov-mike-parson [https://perma.cc/3TF6-46FL]; Jason Hancock, *Prosecutor: No 'criminal intent' by reporter Missouri governor accused of hacking*, MO. INDEP. (Feb. 21, 2022, 1:14 PM), https://missouriindependent.com/2022/02/21/

[36] The new policy's biggest limitation, however, is that it has no effect on civil CFAA claims.[107] The policy is for federal prosecutors, therefore it does not bind the hands of private plaintiffs.[108] This distinction matters a lot to researchers trying to assess their legal risk, because it is civil litigation that accounts for the majority of CFAA cases (against all defendants, not just researchers), according to a 2016 study by Jonathan Mayer.[109] The study found that both civil and criminal CFAA cases are more frequent now than earlier in the statute's lifetime.[110] Following an initial "stead[y] increas[e]," "cybercrime charging leveled off" after the mid-2000s, whereas "[c]ivil cybercrime litigation has unambiguously exploded."[111] "The increase in criminal prosecutions and convictions, while significant, is not nearly as abrupt or substantial as the apparent increase in civil litigation."[112] That is, if a researcher is accused of violating the CFAA, there were already good odds even before the DOJ's policy shift that the accusation arose in a civil complaint rather than a criminal indictment. Going forward (and assuming the new DOJ policy has legs), researchers' CFAA liability risk for responsibly finding and disclosing security vulnerabilities can be expected to arise almost exclusively in the civil litigation context.

---

prosecutor-no-criminal-intent-by-reporter-missouri-governor-accused-of-hacking/ [https://perma.cc/AKC6-ZSGC].

[107] Andrew Crocker, *DOJ's New CFAA Policy is a Good Start but Does Not Go Far Enough to Protect Security Researchers*, ELEC. FRONTIER FOUND.: DEEPLINKS (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/7Y9Y-6GZQ] ("[The new policy] does nothing to lessen the risk of frivolous or overbroad CFAA civil litigation against security researchers, journalists, and innovators.").

[108] *DOJ Press Release*, *supra* note 88.

[109] Mayer, *supra* note 66, at 1472–77.

[110] *Id.*

[111] *Id.* at 1472, 1475.

[112] *Id.* at 1476.

[37] This lingering civil risk exposure matters because the *Van Buren* ruling has not been universally welcomed among private-sector vendors. Voatz, a mobile voting app company, gained notoriety in 2019 for referring a college student to law enforcement for research that complied with its bug bounty terms at the time.[113] The company responded to *Van Buren* with a webinar in which its outside counsel warned security researchers that certain research methods could still violate the CFAA after *Van Buren* "even if [their] purpose is noble."[114] Voatz's counsel also told researchers the "safest bet" was to "work with [vendors] to identify any security vulnerabilities."[115] This stance accorded with the *amicus curiae* brief the same attorney filed for Voatz in *Van Buren*, which urged the view that external research must follow terms dictated by the vendor, either through a bug bounty program or "direct collaboration" with the vendor.[116] Although Voatz's preferred broad interpretation of the CFAA's "exceeds

[113] Yael Grauer, *Safe Harbor, or Thrown to the Sharks by Voatz?*, COINTELEGRAPH MAG. (Feb. 7, 2020), https://cointelegraph.com/magazine/2020/02/07/safe-harbor-or-thrown-to-the-sharks-by-voatz [https://perma.cc/TS6G-RNZA]; Kevin Collier, *FBI investigating if attempted 2018 voting app hack was linked to Michigan college course*, CNN (Oct. 5, 2019, 4:23 PM), https://www.cnn.com/2019/10/04/politics/fbi-voting-app-hack-investigation [https://perma.cc/VC22-F3YU]. To date, charges have not publicly been filed against the student or students in question.

[114] Voatz, *Voatz: Van Buren vs. United States Explained, June 29th, 2021*, YOUTUBE, at 40:20–42:04 (July 2, 2021), https://www.youtube.com/watch?v=0uU6CO7WUrw [https://perma.cc/BPN8-SQ8L].

[115] *Id.*

[116] *See* Brief for Voatz, Inc. as Amici Curiae Supporting Respondents, Van Buren v. United States, 141 S. Ct. 1648 (2021) (No. 19-783). The brief caused a furor in the security community, prompting an open letter signed by numerous security experts pushing back against Voatz's view of the CFAA and perceived factual inaccuracies in the brief. *Response to Voatz's Supreme Court Amicus Brief*, disclose.io (Sept. 14, 2020), https://disclose.io/uploads/voatz-response-letter.pdf [https://perma.cc/2LHF-TF3Y].

authorized access" provision[117] was not adopted by the Court,[118] Voatz's attitude toward the Court's ruling indicates that vendors will still look for ways to impose legal liability on security research.

[38] In fact, the *Van Buren* opinion gives those vendors a possible avenue for doing so. A footnote in the opinion left open the question of whether authorized access may be controlled only through technical ("code-based") access barriers, or also by terms in a contract or policy.[119] This footnote is at odds with the rest of the opinion, leaving commentators struggling to make sense of it.[120] At a minimum, the footnote indicates that vendors could still sue over good-faith research that circumvents a technological access barrier, even though the DOJ has chosen generally to disfavor criminal charges in the same situation.[121] Meanwhile, the Court's footnote dangled the possibility that research that does not circumvent any such barriers might nevertheless still violate the CFAA if it contravenes a contractual or policy provision. Vendors may seize upon the ambiguity the footnote

[117] Brief for Voatz, Inc. as Amici Curiae Supporting Respondents at 3, *Van Buren*, 141 S. Ct. 1648 (No. 19-783).

[118] *See Van Buren*, 141 S. Ct. at 1661.

[119] *Id.* at 1658–59 n.8; *see* Mackey & Opsahl, *supra* note 87 ("[A]lthough the high court did not narrow the CFAA as much as EFF would have liked, leaving open the question of whether the law requires circumvention of a technological access barrier, it provided good language that should help protect researchers[.]").

[120] Kerr, *The Supreme Court Reins in the CFAA in* Van Buren, *supra* note 77 ("My first reaction to this footnote was puzzlement. How can the Court reject the government's view that the policy controls and yet also leave open whether liability looks to policies? How do you reconcile Footnote 8 with the rest of the opinion. . .?"); Mackey & Opsahl, *supra* note 87 ("This footnote is a bit odd, as the bulk of the majority opinion seems to point toward the law requiring someone to defeat technological limitations on access, and throw[s] shade at criminalizing TOS violations.").

[121] *See DOJ Charging Policy*, *supra* note 89.

created and sue researchers civilly, forcing lower courts to address the question the Court left for them to decide.[122]

B. The "Loss" Dicta and Lower Courts' Responses

[39] The "exceeds authorized access" provision is not the only part of the CFAA that the Supreme Court interpreted narrowly. Although *Van Buren* was a criminal case, the Court's opinion included intriguing dicta about limiting the meaning of "loss" in civil cases.[123] In the short time since the opinion issued, however, that dicta has had little effect on how lower courts approach the "loss" analysis. Pre-existing circuit precedent (where there is any) still carries the day, regardless of whether that precedent calls for a narrow or broad reading of "loss."

[40] To bolster its analysis of the "exceeds authorized access" prong, the Court looked to the statute's definitions of "damage" and "loss":

> Recall that violating § 1030(a)(2), the provision under which Van Buren was charged, also gives rise to civil liability. Provisions defining "damage" and "loss" specify what a plaintiff in a civil suit can recover. "'[D]amage,'" the statute provides, means "any impairment to the integrity or availability of data, a program, a system, or information." The term "loss" likewise relates to costs caused by harm to computer data, programs, systems, or information services. The statutory definitions of "damage" and "loss" thus focus on technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data. Limiting "damage" and "loss" in this way makes sense

[122] Kerr, *The Supreme Court Reins in the CFAA in* Van Buren, *supra* note 77 (*Van Buren* "now leaves to lower courts the largely interstitial work of figuring out the hard line-drawing of what exactly" system owners need to do in order to "trigger liability").

[123] *Van Buren*, 141 S. Ct. at 1659.

> in a scheme "aimed at preventing the typical consequences of hacking." The term's definitions are ill fitted, however, to remediating "misuse" of sensitive information that employees may permissibly access using their computers.[124]

[41] The Court pointed out that defendant Van Buren's improper use of a database he was authorized to access "did not impair the 'integrity or availability' of data, nor did it otherwise harm the database system itself."[125] This illustration helped the Court explain why the CFAA's "text and structure" supported its narrow reading of the "exceeds authorized access" provision.[126]

[42] *Van Buren* can be read "to suggest a trend toward a narrower reading of the CFAA, including those provisions concerning damage and loss[.]"[127] However, the Court's dicta about "damage" and "loss" has not revolutionized the federal courts' treatment of plaintiffs' loss allegations in civil CFAA lawsuits. Looking at post-*Van Buren* decisions to date, a pattern emerges: if the court is in a circuit that already interpreted "loss" narrowly pre-*Van Buren*, the court may cite the dicta approvingly, whereas in circuits that take a broader view of "loss" or have no appellate precedent on point, the Court's "loss" language has had little effect on lower courts' decision-making. Often, courts acknowledge *Van Buren* but do not mention the dicta at all in their analysis of whether the plaintiff had established the requisite $5,000 of "loss."

---

[124] *Id.* at 1659–60 (citing 18 U.S.C. §§ 1030(e)(8), (e)(11), (g); *Royal Truck*, 974 F.3d at 760).

[125] *Id.* at 1660.

[126] *Id.*

[127] ACI Payments, Inc. v. Conservice, LLC, No. 21-CV-00084, 2022 U.S. Dist. LEXIS 38222, at *33 n.135 (D. Utah Mar. 3, 2022).

1. Narrow Reading of "Cost of Responding to an Offense"

[43] Recall that courts in the Second and Ninth Circuits adopt a narrow reading of "the cost of responding to an offense."[128] These courts have treated *Van Buren* as being in keeping with that existing view. The Ninth Circuit recently cited *Van Buren*'s "loss" language in a footnote as "requir[ing]" plaintiffs to show technological harm in order to have standing.[129] Likewise, several district courts in the Second[130] and Ninth

[128] Andrews v. Sirius XM Radio Inc., 932 F.3d 1253, 1262–63 (9th Cir. 2019) ("The statute's 'loss' definition—with its references to damage assessments, data restoration, and interruption of service—clearly limits its focus to harms caused by computer intrusions, not general injuries unrelated to the hacking itself."); *ACI Payments*, 2022 U.S. Dist. LEXIS 38222, at *31–32 ("Courts within the Second Circuit narrowly interpret the phrase 'cost of responding to an offense' and limit it 'to situations involving damage to or impairment of the protected computer.'").

[129] hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1195 n.12 (9th Cir. 2022) ("*Van Buren* reviewed the statutory definitions of 'damage' and 'loss' and concluded that this civil remedies provision requires a showing of 'technological harms—such as the corruption of files—of the type unauthorized users cause to computer systems and data.'").

[130] *E.g.*, Zap Cellular, Inc. v. Weintraub, No. 15-CV-6723, 2022 U.S. Dist. LEXIS 168735, at *28–32 (E.D.N.Y. Sept. 19, 2022) (finding plaintiff's loss allegations sufficient under existing circuit precedent without mentioning the dicta in *Van Buren*, which it cited solely for its substantive holding). *See also* El Omari v. Buchanan, No. 20-CV-2601, 2021 U.S. Dist. LEXIS 236933, at *39–40 (S.D.N.Y. Dec. 10, 2021) ("Prior to *Van Buren*, courts in this District similarly interpreted the CFAA to require 'loss' related to damage or impairment of the target computer itself"; finding plaintiff's allegations about loss of his personal information insufficient under this standard), *aff'd*, No. 22-55, 2022 U.S. App. LEXIS 26799 (2d Cir. Sept. 26, 2022) (unpub.); Better Holdco, Inc. v. Beeline Loans, Inc., No. 20-CV-8686, 2021 U.S. Dist. LEXIS 138908, at *9–10 (S.D.N.Y. July 26, 2021) (deeming *Van Buren* consistent with the district's prior caselaw and thus "interpret[ing] 'costs of responding to an offense' as limited to situations involving damage to or impairment of the protected computer.").

Circuits[131] have evaluated plaintiffs' loss allegations under existing circuit precedent, with some favorably citing the dicta in support of their analyses.

[44] Similarly, in the Eighth Circuit, where district courts "restrict[] the CFAA 'loss' requirement to actual computer impairment[,]" a Missouri district court approvingly quoted the *Van Buren* dicta in deciding that a plaintiff that had very briefly lost control of its social media accounts and website had not adequately alleged $5,000 in cognizable loss.[132]

[45] In the Third Circuit, as in the Eighth, district courts generally require that loss allegations be tied to damage or impairment to the protected computer.[133] In a dispute over web scraping, a Delaware federal court disagreed (in a cursory footnote) with the defendants' argument that the plaintiff had not suffered "technological harms" under *Van Buren*.[134] The court found that the plaintiff's alleged expenditure of "'considerable

[131] Saffron Rewards, Inc. v. Rossie, No. 22-CV-02695, 2022 U.S. Dist. LEXIS 131613, at *22 (N.D. Cal. July 25, 2022) (citing *Van Buren* dicta, seemingly as binding precedent, and *Andrews* in dismissing a CFAA claim for inadequate loss allegations); Fraser v. Mint Mobile, LLC, No. C 22-00138, 2022 U.S. Dist. LEXIS 76772, at *15 (N.D. Cal. Apr. 27, 2022) (citing *Van Buren* dicta and *Andrews* in dismissing CFAA claim because plaintiff's stolen cryptocurrency was not related to a computer or system). *See also* Fish v. Tesla, Inc., No. 21-cv-60, 2022 U.S. Dist. LEXIS 87065, at *22–25 (C.D. Cal. May 12, 2022) (citing *Andrews*, 932 F.3d at 1263); United Fed'n of Churches, LLC v. Johnson, No. 20-cv-509, 2022 U.S. Dist. LEXIS 69983, at *22–25 (W.D. Wash. Apr. 15, 2022) (citing *Andrews*, 932 F.3d at 1263); Biesenbach v. Doe, No. 21-cv-8091, 2022 U.S. Dist. Court LEXIS 12686, at *17–18 (N.D. Cal. Jan. 24, 2022) (citing *Andrews*, 932 F.3d at 1263).

[132] Burnett v. Grundy, No. 14-CV-00301, 2014 U.S. Dist. LEXIS 192624, at *5 (W.D. Mo. Oct. 28, 2014); Pipeline Prods. v. S&A Pizza, Inc., No. 20-CV-00130, 2021 U.S. Dist. LEXIS 197991, at *18–19 (W.D. Mo. Oct. 14, 2021).

[133] Volpe v. Abacus Software Sys. Corp., No. 20-10108, 2021 U.S. Dist. LEXIS 112641, at *15–16 (D.N.J. June 16, 2021).

[134] Ryanair DAC v. Booking Holdings Inc., No. 20-1191, 2021 U.S. Dist. LEXIS 246386, at *12 n.8 (D. Del. Dec. 27, 2021).

resources, in excess of five thousand dollars ($5,000), to find, diagnose, and block access' to its website" fit within the statutory definition of "loss."[135]

[46] Occasionally, recent decisions from these circuits have dismissed plaintiffs' CFAA claims on the merits without needing to rely on the Court's "loss" dicta, generally because *Van Buren* foreclosed the plaintiffs' interpretation of the CFAA.[136] Otherwise, in these "narrow reading" circuits, *Van Buren*'s language limiting "loss" to "technological harms" has served, at best, to reinforce the conclusion the court would have reached anyway under those courts' pre-*Van Buren* interpretation of "the cost of responding to an offense."

2. Broad Reading of "Cost of Responding to an Offense"

[47] In the Eleventh Circuit, which adopted a broader reading of "the cost of responding to an offense" in a case called *Brown Jordan*, district courts

[135] *Id.*; *see also* Ryanair DAC v. Booking Holdings Inc., No. 20-1191, 2022 U.S. Dist. LEXIS 193027, at *18–20 (D. Del. Oct. 24, 2022) (again denying motion to dismiss CFAA claim and citing *Van Buren* dicta; finding that plaintiff had alleged "damage or loss" by pleading that defendants' "scraping activities" had caused increased queries to the plaintiff's website, slower website response time, and other errors) (quoting *Van Buren*, 141 S. Ct. at 1660).

[136] *E.g.*, Rodgers Grp., LLC v. Lewis, No. 22-482, 2022 U.S. Dist. LEXIS 161607, at *19 (D.N.J. Sept. 7, 2022) (dismissing plaintiff's CFAA claim for failing to allege facts suggesting damage or impairment to its computer systems, and rejecting business damages as insufficient); Pinebrook Holdings, LLC v. Narup, No. 19-CV-1562, 2022 U.S. Dist. LEXIS 97578, at *33 n.17, *35–36 (E.D. Mo. June 1, 2022) (declining to decide whether to adopt *Van Buren*'s "technological harms" language; finding that plaintiffs' losses no longer met the $5,000 threshold after excluding investigatory costs tied to "misuse of information" theory which *Van Buren* rejected); Databaseusa.Com, LLC v. Van Gilder, 17-CV-386, 2022 U.S. Dist. LEXIS 112530, *32–33 (D. Neb. May 24, 2022) (finding no CFAA violation where an employee took and transferred documents to which he had authorized access). *Cf.* Acrison, Inc. v. Rainone, No. 22-1176, 2022 U.S. Dist. LEXIS 200868, at *21–25 (D.N.J. Nov. 3, 2022) (quoting *Van Buren*'s "loss" dicta favorably but dismissing CFAA claim as time-barred).

have relied on that precedent rather than *Van Buren* when evaluating plaintiffs' loss allegations in CFAA cases.[137]

[48] One Georgia district court concluded that the plaintiff had adequately alleged $5,000 in loss under *Brown Jordan* by adding together the direct costs of repairs plus the value of the time the plaintiff spent addressing the issue instead of working.[138] The court deemed *Van Buren* irrelevant because *Van Buren* was an "exceeds authorized access" case whereas the plaintiff's claim was brought under the CFAA's "without authorization" prong.[139]

[49] Similarly, a different Georgia court declined to apply *Van Buren* to the plaintiff's CFAA claim, conducting its "loss" analysis under *Brown Jordan* without acknowledging the *Van Buren* dicta.[140] The court ruled that the plaintiff failed to meet the loss threshold by alleging that it had hired an expert for litigation purposes, rather than to assess damages or restore data as in *Brown Jordan*.[141] Likewise, another court rejected a plaintiff's allegations of investigatory efforts as too conclusory where there was no

[137] *See* Brown Jordan Int'l, Inc. v. Carmicle*,* 846 F.3d 1167, 1173–75 (11th Cir. 2017) (rejecting a narrower reading of the CFAA requiring that loss be the result of an "interruption of service," holding instead that "'[l]oss' includes the direct costs of responding to the [alleged] violation," and therefore allowing as "losses" plaintiff's cost of hiring two firms to "engage in an extensive forensic and physical review of Brown Jordan's systems to determine the extent of Carmicle's hacking activity.").

[138] Bowen v. Porsche Cars, N.A., Inc., 561 F. Supp. 3d 1362, 1371 (N.D. Ga. Sept. 20, 2021) (citing *Brown Jordan*, 846 F.3d at 1174).

[139] *Id.* at 1370.

[140] Amerair Indus. of Del., LLC v. Indus. Accessories Co., No. 20-CV-01736, 2022 U.S. Dist. LEXIS 81405, at *13–14 (N.D. Ga. Mar. 30, 2022) (citing *Brown Jordan*, 846 F.3d at 1173–74).

[141] *Id.* at *17.

"evidence of actual loss," such as receipts showing payments to outside consultants as in *Brown Jordan*.[142]

[50] In Alabama, a CFAA claim survived summary judgment because "[h]iring a forensic analyst to investigate the extent of unauthorized email access is a loss 'incurred in the course of responding to the offense'" under *Brown Jordan*.[143] Finally, a Florida district court, invoking *Brown Jordan*'s holding about what constitutes cognizable loss, dismissed a CFAA claim because the alleged losses stemmed from an improper-use theory now foreclosed by *Van Buren*.[144]

[51] In the Fourth Circuit, which considers the "loss" definition a "broadly worded provision [that] plainly contemplates . . . costs incurred as part of the response to a CFAA violation, including the investigation of an offense,"[145] a district court relied on *Van Buren* to reject the plaintiff's loss allegations, but not because of the dicta. Rather, as in the Florida case, the court held that the defendant's alleged misuse of information did not violate the CFAA under both *Van Buren* and existing circuit precedent.[146]

[142] Castellano Cosm. Surgery Ctr., P.A. v. Doyle, No. 21-CV-1088, 2021 U.S. Dist. LEXIS 140610, at *27 n.5, *29 (M.D. Fla. July 28, 2021) (citing *Brown Jordan*, 846 F.3d at 1172–74; distinguishing *Van Buren* for being decided under "exceeds authorized access" provision).

[143] Gemstone Foods, LLC v. AAA Foods Enters., No. 15-CV-02207, 2022 U.S. Dist. LEXIS 83369, at *117–124, 124–130 (N.D. Ala. Apr. 27, 2022) (narrowing plaintiff's CFAA claim to exclude improper-use theory pursuant to *Van Buren*; cautioning that the plaintiff would have to tie its forensic analysis costs to the alleged CFAA violation at trial in order to recover damages).

[144] Trump v. Clinton, No. 22-CV-14102, 2022 U.S. Dist. LEXIS 163507, at *79–81 (S.D. Fla. Sept. 8, 2022) ("Plaintiff's single reference to 'the cost of investigating and responding to the unauthorized access' is conclusory and unsupported by factual allegations").

[145] A.V. *ex rel.* Vanderhye v. iParadigms, LLC, 562 F.3d 630, 646 (4th Cir. 2009).

[146] OSI Sys. v. KM-Logix, LLC, No. 20-CV-1577, 2022 U.S. Dist. LEXIS 112386, at *5–8 (E.D. Va. June 24, 2022) (citing *Van Buren*, 141 S. Ct. at 1653, 1654–55;

Consequently, the cost of reconfiguring the plaintiff's website in response to that non-violation "would not meet the CFAA qualifying loss standard."[147]

[52] Although some of the foregoing cases used *Van Buren*'s substantive ruling to narrow or dismiss the plaintiffs' CFAA claims, none quoted *Van Buren*'s dicta to reach their conclusions as to the sufficiency of the plaintiffs' loss allegations. Rather, as in the "narrow reading" circuits, they looked to "loss" caselaw that pre-dated *Van Buren*.

3. No Circuit Precedent

[53] Some circuits lack extensive CFAA case law, meaning their district courts must turn elsewhere for persuasive authority regarding the interpretation of "loss." *Van Buren*'s dicta has rarely influenced these courts' CFAA decisions to date.

[54] In the Tenth Circuit, where "[t]here is little . . . authority interpreting the CFAA," a federal district court in Utah, after extensively reviewing other courts' CFAA decisions post-*Van Buren*, ultimately treated *Van Buren*'s "loss" discussion as non-binding.[148] It rejected the defendant's argument "that the *Van Buren* court's observation in dicta about damage and loss limits those provisions to *exclusively* technological harms."[149] Previously, another Utah district court concluded there was a triable factual

iParadigms, 562 F.3d at 646; WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 203, 207 (4th Cir. 2012)).

[147] *Id.* at *8.

[148] ACI Payments, Inc. v. Conservice, LLC, No. 21-CV-00084, 2022 U.S. Dist. LEXIS 38222, at *26 (D. Utah Mar. 3, 2022).

[149] *Id.* at *33 n.135 (declining to choose between narrower and broader interpretations of "cost of responding to an offense" because plaintiff had not sufficiently alleged either one). The plaintiff subsequently dropped the CFAA claim from its amended complaint. Amended Complaint, *ACI Payments*, 2022 U.S. Dist. LEXIS 38222 (No. 21-CV-00084).

dispute on the CFAA claim under *Van Buren*, but it did not mention the Court's "loss" dicta in finding the $5,000 threshold satisfied by the plaintiff's computer audit costs.[150]

[55] The Fifth Circuit has not directly addressed the scope of "the cost of responding to an offense,"[151] but district courts post-*Van Buren* have had no trouble finding that the costs of investigating an intrusion, and in some cases hiring an outside forensic investigator, satisfy the $5,000 bar.[152] These cases cite *Van Buren* for its substantive holding only, with no mention of the dicta.[153]

[56] In circuits without a precedential interpretation of "loss," the dicta's greatest impact so far came in a Washington, D.C., district court decision.

[150] Vox Mktg. Grp. v. Prodigy Promos, 556 F. Supp. 3d 1280, 1285 (D. Utah Aug. 20, 2021). Curiously, the court cited no case law (in or out of circuit) construing the definition of "loss," although it did express skepticism that any of the plaintiff's other alleged costs could be recoverable as damages. *Id.* at 1288–90.

[151] It might interpret the term broadly if the issue arose. In a criminal sentencing appeal, it upheld (on plain-error review) a restitution award that included both the hacking victim's damage assessment costs and its costs of notifying individuals whose personal information the defendant had accessed. United States v. Phillips, 477 F.3d 215, 218, 224–25 (5th Cir. 2007).

[152] Philips N. Am. LLC v. Image Tech. Consulting LLC, No. 22-CV-147, 2022 U.S. Dist. LEXIS 133234, at *17–18 (N.D. Tex. July 26, 2022) (allegations of lost revenue and expenditure of over $5,000 investigating defendants' conduct satisfied the "loss" requirement); EthosEnergy Field Servs., LLC v. Axis Mech. Grp., Inc., No. 21-CV-3954, 2022 U.S. Dist. LEXIS 123586, at *17 (S.D. Tex. June 10, 2022) ("[Plaintiff] alleged that it expended more than $75,000 conducting an investigation and damage assessment that required forensic examinations and the reassignment of executives, attorneys, and other employees from their normal duties."); Cantu v. Guerra, No. 20-CV-746, 2021 U.S. Dist. LEXIS 119681, at *13-15 (W.D. Tex. June 28, 2021) ("Dr. Guerra alleges that she has suffered loss of at least $5,000, including engaging [a digital forensics firm], investigating the intrusion of the iPad and other computers, assessing the damage, and attempting to restore security to various intruded-upon systems.").

[153] *Philips N. Am.*, 2022 U.S. Dist. LEXIS 133234, at *15–17; *EthosEnergy*, 2022 U.S. Dist. LEXIS 123586, at *16; *Cantu*, 2021 U.S. Dist. LEXIS 119681, at *10.

The dicta appears to have prompted the court *sua sponte* to raise the statutory standing issue when ruling on the defendant's motion to dismiss.[154] The court cautioned the plaintiff that, at summary judgment, it would be expected to tie its remediation efforts to cognizable harms.[155] Those harms, the court said, may include the alleged damage to the plaintiff's computer systems and the "impair[ment] and corrupt[ion]" of the plaintiff's "efforts to measure and analyze legitimate subscriber traffic," but could not include the value the defendant derived from its unauthorized access to the plaintiff's database.[156]

V. THE "SHOOTING THE MESSENGER" PROBLEM

[57] The CFAA's substantive offenses, coupled with courts' willingness to include remediation costs as "loss," open a channel for civil litigation by vendors against researchers who responsibly disclose security vulnerabilities to them. Litigious vendors can sue over security research that prompted a bug fix, but did not harm any data, devices, programs, or systems. So long as the vendor spends just $5,000 remediating the disclosed vulnerability, it meets the jurisdictional "loss" threshold.[157]

[58] A vendor displeased by security research (either because the findings are unflattering or because it happened at all) can accuse the

[154] CoStar Grp., Inc. v. Leon Cap. Grp., Inc., No. 21-CV-2227, 2022 U.S. Dist. LEXIS 101663, at *26–28, *27 n.4 (D.D.C. June 7, 2022) (discussing "the statute's loss requirement" as "[an] issue with CoStar's claim that Leon Capital does not raise, but that may be dispositive at summary judgment").

[155] *Id.* at *28.

[156] *Id.* at *27 n.4 ("The statute's focus on 'technological harms,' as well as the $5,000 minimum loss standard, will necessarily limit claims to large-scale business misconduct affecting a victim's computer systems or data.").

[157] 18 U.S.C. § 1030(g); Kilovaty, *supra* note 41, at 503 ("loss" includes patching costs).

researcher of violating the CFAA.[158] The easiest subsection for a "vengeful vendor" to invoke is subsection 1030(a)(2)(C), under which Mr. Van Buren was charged.[159] To recap: subsection (a)(2)(C) requires that the defendant "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."[160] If a researcher intentionally accesses a vendor's "protected computer" and obtains "*any* information," the vendor can allege that such access was unauthorized and thus an (a)(2)(C) violation.[161]

[59] The vendor can then frame its remediation costs for fixing the vulnerability as a "loss" the researcher supposedly "caused" by finding and reporting the vendor's flaw. "Loss" means "any reasonable cost to any victim, including the cost of responding to an offense[.]"[162] Here, the

[158] *See* Kilovaty, *supra* note 41, at 488–89 ("Not all tech companies encourage an active hunt for bugs in their software, and some would even be quite unwelcoming of any vulnerabilities reported, whether due to reputational or cost-associated reasons, and might claim such vulnerability collection to be in breach of contract or in violation of the law.").

[159] United States v. Van Buren, 940 F.3d 1192, 1205 (11th Cir. 2019), *rev'd*, 141 S. Ct. 1648 (2021).

[160] 18 U.S.C. § 1030(a)(2)(C).

[161] Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, supra note 17, at 1578; *see also* Sandvig v. Sessions, 315 F. Supp. 3d 1, 3 (D.D.C. 2018) (subsection (a)(2)(C) "applies to anyone who purposely accesses an Internet-connected computer without authorization, or uses a legitimate authorization to receive or change information that they are not supposed to, and thereby obtains information from the computer.").

[162] 18 U.S.C. § 1030(e)(11). For purposes of this Article, where the phrase "remediation costs" appears in reference to "shooting the messenger" situations, it refers only to costs associated with *fixing* a vulnerability, such as investigating to confirm the vulnerability exists, determining how many resources are affected by it (*e.g.*, how many computers on a network, how many users of a version of software), and writing, testing, and deploying code to close the vulnerability. "Remediation costs" does not mean the costs associated with remediating harms arising from *exploitation* of a vulnerability, such as the costs arising from an interruption in service due to an attack, the cost of restoring the integrity of data that was deleted or altered by the attacker, legal costs, etc. The term also, as will

offense is the research that allegedly violates (a)(2)(C). Courts may recognize vulnerability remediation costs as a cognizable loss.[163]

[60] Because loss is a prerequisite for statutory standing but neither damage nor loss is an element of an (a)(2)(C) offense, spending $5,000 (by the plaintiff's own count[164]) on remediation will get the vendor into court without ever needing to show, for either standing or merits purposes, that the "protected computer" in question was at all harmed by the defendant's research. In this way, the vendor can shoot the proverbial messenger for inducing it to remediate a vulnerability it failed to discover or fix on its own—by suing the researcher and attempting to stick her with the bill for the patch.

[61] *Van Buren* does not dictate a result in cases where, although they arise from a plaintiff's security vulnerabilities, "no actual damage was inflicted and loss alone is alleged[.]"[165] As said, *Van Buren*'s language about limiting "loss" to "technological harms"[166] in civil cases is non-

be explained herein, excludes the costs to fix damage caused inadvertently by a well-intentioned research experiment gone awry.

[163] *E.g.*, Meta Platforms, Inc. v. BrandTotal Ltd., No. 20-CV-07182, 2022 U.S. Dist. LEXIS 100679, at *85–88 (N.D. Cal. June 6, 2022) (discussing *Van Buren* dicta; rejecting defendant's argument that *Van Buren* and *hiQ* require excluding investigative costs, stating, "There is no indication that the *Van Buren* Court would place investigative costs as falling outside the scope of 'the cost of responding to an offense' that the statute specifically incorporates."); Integrated Waste Sols., Inc. v. Goverdhanam, No. 10-2155, 2010 U.S. Dist. LEXIS 127192, at *26 (E.D. Pa. Nov. 30, 2010) ("The Court finds that [security enhancements], incurred in the course of assessing and responding to alleged violations of the CFAA, constitute cognizable damages under the Act."); *see also* Kilovaty, *supra* note 41, at 503 ("Losses also include the cost of patching a vulnerability, which would have taken place even in absence of the crime.").

[164] *See* Graves et al., *supra* note 33, at 318.

[165] Vasiu & Vasiu, *supra* note 37, at 200; *see also id.* at 188–89 (reviewing cases involving or hypothesizing such a fact pattern).

[166] Van Buren v. United States, 141 S. Ct. 1648, 1659–60 (2021).

binding dicta.[167] Courts may still accept that a vendor suffered cognizable "loss" for merely fixing a vulnerability that a researcher responsibly disclosed, even if the researcher's conduct, like Mr. Van Buren's, "did not impair the 'integrity or availability' of data, nor did it otherwise harm the [vendor's protected computer] itself."[168] Even in jurisdictions that ostensibly interpret "the cost of responding to an offense" narrowly, a court may choose to allow the plaintiff's patching costs to count toward the standing threshold notwithstanding *Van Buren*.[169]

[62] Bug bounties and vulnerability disclosure programs cannot fully mitigate the "shooting the messenger" threat either, even though their whole purpose is to encourage disclosure. Like the DOJ's CFAA charging policy, they are voluntary commitments, not legal requirements. Vendors are free to refuse to establish a bug bounty or VDP if they do not want external security research into their products.[170] What's more, even where vendors do establish such a program, they often set terms that give the vendor sole

[167] ACI Payments, Inc. v. Conservice, LLC, No. 21-CV-00084, 2022 U.S. Dist. LEXIS 38222, at *33 n.135 (D. Utah Mar. 3, 2022) ("The court reads the *Van Buren* decision to suggest a trend toward a narrower reading of the CFAA, including those provisions concerning damage and loss, but disagrees with Conservice that the *Van Buren* court's observation in dicta about damage and loss limits those provisions to *exclusively* technological harms.").

[168] *Van Buren*, 141 S. Ct. at 1660.

[169] *Meta Platforms*, 2022 U.S. Dist. LEXIS 100679, at *85–88 (declining to exclude "investigative costs" as out of scope of "the cost of responding to an offense," reasoning that neither *Van Buren*'s nor *hiQ*'s dicta requires such a limitation). That court, however, expressed skepticism that, where a defendant's conduct is ultimately found not to violate the CFAA, a plaintiff "can count costs to investigate *potential* violations that do not turn out to be violations towards the $5,000 threshold." *Id.* at *88–89. Second Circuit district courts post-*Van Buren* have reiterated that they count as "loss" the costs of investigations and damage assessment, even if they ultimately confirmed there had been no damage from the defendant's conduct. *Zap Cellular*, 2022 U.S. Dist. LEXIS 168735, at *31–32.

[170] Kilovaty, *supra* note 41, at 488–89 ("Not all tech companies encourage an active hunt for bugs in their software[.]").

discretion to determine whether to refrain from taking legal action against a participant.[171] If a vendor breaks its end of the agreement after a participant has submitted a bug, the consequences may be worse for the researcher than for the breaching vendor.[172]

[63] Put another way, bug bounties and VDPs tend to be burdensome on researchers and disproportionately favorable to vendors as-is, so they require good-faith behavior by both sides, researcher *and* vendor, in order to work. However, shooting the messenger is bad-faith behavior almost by definition, so it is not out of the question that a bad-faith vendor might sue a researcher just because the vendor offers a bug bounty or VDP.[173]

[64] As Voatz's mulish response to the Supreme Court's decision underscores, *Van Buren* will not deter vendors intent on continuing to limit and control research into their products' security and to prohibit or punish the publication of any unflattering results. Until something stronger than the dicta in *Van Buren* bars vengeful vendors from filing civil claims, researchers will remain vulnerable to "shooting the messenger" lawsuits under the CFAA.

---

[171] Arooni, *supra* note 60, at 454 ("This power imbalance is . . . a regular practice in the VDP industry today.").

[172] *Compare* Yael Grauer, *Voatz Bug Bounty Kicked Off of HackerOne Platform*, COINTELEGRAPH (Mar. 31, 2020), https://cointelegraph.com/news/voatz-bug-bounty-kicked-off-of-hackerone-platform [https://perma.cc/542G-X97W] (for its bad-faith behavior in referring a student researcher to the FBI, then changing the terms of its bug bounty to make it look like the student had violated the terms, the consequence Voatz incurred was being kicked off the third-party bug bounty platform), *with* Collier, *supra* note 113 (for the student in question, the consequence of Voatz's behavior was getting investigated by the FBI, including receiving "a search warrant for their phone").

[173] *See* Arooni, *supra* note 60, at 454–55 ("Voatz serves as an example of how even a safe harbor [from liability for submitting a bug] may derail the environment of trust between researchers and the host organization. For safe harbor provisions to work, host organizations must follow their own protocol.").

VI. FIXING THE "SHOOTING THE MESSENGER" RISK TO SECURITY RESEARCHERS

[65] How can policymakers mitigate the legal risk to researchers from "shooting the messenger" litigation? This section discusses two possible answers. The first is to exempt "good-faith security research" from liability, as other commentators have proposed. The second alternative approach is to statutorily restrict what type of "loss" can establish standing that gets a CFAA plaintiff through the courthouse door.

A. "Good-Faith Security Research" Safe Harbor

[66] This Article discussed the DOJ's recent adoption in the CFAA context of the DMCA's exemption from liability for "good-faith security research."[174] In addition, several commentators have also proposed their own versions of a safe harbor to protect researchers from legal risk. While these proposals vary in their level of detail and the kinds of legal claims to which they apply, they tend to have some elements in common. After reviewing several proposals, starting with the earliest framework and ending with the most recent one, this section explains the shortcomings inherent in trying to limit liability by defining "good-faith security research."

1. Commentators' Proposals

[67] Several commentators have proposed variations on a safe harbor for good-faith security research. These proposals tend to favor multi-factor tests that require the evaluation of several factors, including the responsible design and conduct of research to avoid harm and minimize the amount of data accessed, vendor notification of the vulnerability, "reasonable" time windows before public disclosure, and vulnerability classification. The

[174] *See supra* Section IV.A.

more complex the proposal, the more difficult it will be for any individual researcher to qualify for the safe harbor.

[68] In 2010, Derek Bambauer and Oliver Day were "the first to propose a set of reforms . . . to protect socially valuable security research [and] guide behavior of those searching for vulnerabilities."[175] Writing about the threats posed by the DMCA and other intellectual property regimes to researchers who test software for flaws, Bambauer and Day set forth five rules for security researchers to follow in exchange for immunity from civil IP claims: "tell the vendor first, don't sell the bug, test on your own system, don't weaponize, and create a trail."[176] Bambauer and Day's proposals proved influential over the next decade: variations on these five rules recur throughout subsequent proposals for limiting researchers' legal liability. However, Bambauer and Day chose to exclude the CFAA from their discussion, on the rationale that the law "contains a built-in limitation on civil liability that offers protection to security researchers."[177] As discussed above, though, security researchers themselves view the CFAA as a source of significant liability exposure,[178] so this proposal is not fully responsive to the problem it sought to address.

[69] Next, in a 2014 article about "gray hat hackers," Cassandra Kirsch suggested that lawmakers enact a safe harbor provision specifically for "this sub-group of the hacking community" so that they "may research and report vulnerabilities without fear of legal repercussion."[179] Kirsch's discussion is

[175] Derek E. Bambauer & Oliver Day, *The Hacker's Aegis*, 60 EMORY L.J. 1051, 1055 (2010).

[176] *Id.* at 1088–92 (explaining each rule in more depth).

[177] *Id.* at 1103–04.

[178] *See supra* Section III.B.

[179] Kirsch, *supra* note 45, at 400 (explaining how "gray hat" hackers "operate with unclear motivations," so their conduct in any given situation cannot be relied upon to be

brief but sets forth the main points that a safe harbor should entail. These include limiting the intrusion on consumers' private information to the minimum necessary, "reasonable measures to put the vendor on notice," a vendor notification period of 24 to 48 hours after discovery of the flaw (during which the gray hat "cannot take any action"), and a one-week window (or "other reasonable time period") for the vendor to respond, after which, if there is no response, the gray hat may disclose the flaw publicly.[180]

[70] This model, Kirsch claims, strikes a balance between hackers' legal concerns and vendors' concerns about having sufficient time to fix the vulnerability before its public disclosure.[181] Kirsch cautions that her protocol will have low odds of success unless lawmakers also impose more stringent data security requirements on vendors; otherwise, if gray hat hackers see vendors escaping liability for breaches or dragging their feet on repairing flaws, they will abandon the protocol.[182]

[71] A 2018 paper by Daniel Etcovitch and Thyla van der Merwe set forth the most complicated safe harbor framework that has been proposed to date.[183] The authors noted that they were not the first to propose such a safe harbor but claimed theirs was "the most comprehensive so far" and the first to finally get into "the specifics of such a statutory reform."[184]

---

either predictably beneficial or predictably malicious); *see* Kilovaty, *supra* note 41, at 480–83 (explaining "white," "black," and "gray hat" terms).

[180] Kirsch, *supra* note 45, at 400.

[181] *Id.*

[182] *Id.* at 400–01.

[183] ETCOVITCH & VAN DER MERWE, *supra* note 58.

[184] *Id.* at 20–21.

[72] For a researcher to qualify for safe harbor eligibility, the "key condition" is to follow the authors' "specific implementation of responsible disclosure," which requires vendor disclosure within two days of confirmed discovery, in a particular two-part format which makes the researcher classify the vulnerability (according to the authors' classification) and give the vendor all information "reasonably necessary" to find and fix the vulnerability.[185] The researcher must also participate in a dispute process with the vendor if the vendor disputes the researcher's classification, comply with a prescribed process for communication, and refrain from public disclosure until the expiration of a time period for final classification of the vulnerability.[186] While the authors' proposal is quite extensive compared to the broad-stroke generalities of Kirsch's, both pieces describe their respective regimes similarly: as striking a balance between researchers' and vendors' needs.[187]

[73] Subsequently, in 2019, Ido Kilovaty set forth a number of case- and fact-specific factors that "distinguish between malicious and benign hackers."[188] This is not so much a formal statutory safe harbor proposal (although Kilovaty stressed the "immense[] importan[ce]" of "[c]larifying the boundaries of the CFAA . . . as pertaining to security researchers"[189]) as a list of considerations to help identify good-faith security testers who should be granted some legal "freedom to hack."[190] The dividing "red line"

[185] *Id.*

[186] *Id.*

[187] *See* ETCOVITCH & VAN DER MERWE, *supra* note 58, at 20.

[188] Kilovaty, *supra* note 41, at 506.

[189] *Id.* at 509.

[190] *Id.* at 506 ("The main difficulty with the proposition that security research should not be impeded by legal hurdles is that it is somewhat burdensome to draw a clear line between benign and malicious activities in cyberspace.").

between "ethical hacking" and "malicious hacking" is whether the hacker weaponizes and exploits the vulnerability to cause harm.[191]

[74] Kilovaty's assessment takes into account whether the hacker's tools and techniques minimized harm or instead caused "damage beyond what is required to identify the flaw."[192] The assessment also considers "the nature of the vulnerability," since different vulnerabilities enable different levels of damage, the amount of time and resources the hacker expended (which could be indicative of malicious intent), cooperation with law enforcement, whether there is disclosure to the vendor and the amount of time it takes the hacker to do so, and the amount of information provided to relevant agencies where applicable.[193]

[75] Finally, immediately following the *Van Buren* decision in 2021, the cybersecurity firm Rapid7 published a proposed safe harbor for security researchers, which it limited to civil claims under the CFAA.[194] Rapid7's proposed amendments would add an affirmative defense to civil actions brought under subsection 1030(4)(A)(i)(I), where "the defendant acted solely for the purpose of good faith security research," a term the proposal would define in a new subsection 1030(e)(13).[195] The proposed subsection (e)(13) imposes several eligibility requirements on the affirmative defense (several of which echo Kirsch and Kilovaty). These include responsible design and conduct of the research to avoid harm, minimizing the amount of data obtained, retained, and disclosed to what is "directly necessary" for

[191] *Id.*

[192] *Id.*

[193] *Id.* at 505–06.

[194] 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/E7NY-P8PU].

[195] *Id.*

the research, waiting a reasonable time (depending on several factors) before public disclosure of a security vulnerability, taking "reasonable steps" to disclose to the protected computer's owner or the Cybersecurity and Infrastructure Security Agency (CISA) prior to public disclosure, and until then, prohibiting commercialization of the findings, and prohibiting nonconsensual public disclosure of trade secrets or another person's personally identifiable information.[196]

[76] Rapid7 asserted that its proposed amendment, while complex, includes "safeguards to curb disingenuous misuse of the defense while providing appropriately scoped protection from federal anti-hacking laws for researchers acting responsibly to detect and disclose security vulnerabilities."[197]

2. Shortcomings of the Safe Harbor Approach

[77] The efforts by commentators (and the Department of Justice) to set forth precise safe harbor language are deserving of recognition. It is not easy to turn high-level guiding principles into actual, finalized policy language. Yet the difficulty of precisely defining a safe harbor, as evident from the number of proposals put forth over the years, illustrates the core problem with the safe harbor approach to protecting good-faith security research.

[78] A slippery concept like "good faith" evades easy definition in the first place. Reasonable minds may differ about where the line lies between research activities and responsible disclosure that are deserving of protection on the one hand, and malicious or reckless conduct that should remain exposed to liability on the other.[198] In specific instances,

[196] *Id.*

[197] Geiger, *supra* note 194.

[198] *See* Kilovaty, *supra* note 41, at 505–06 (describing competing views of best practices for responsible disclosure).

determining which side of the line a researcher's work falls on may prove fraught with difficulty.

[79] What's more, even once a definition of "good faith" is chosen (such as the DMCA's), applying the definition to particular conduct will not be a friction-free process. It is one thing for commentators to have an academic disagreement about what conduct should qualify for a safe harbor; it is quite another thing when the disagreement is between a researcher and the U.S. government. Having oneself and one's work scrutinized by federal law enforcement personnel may be time-consuming, expensive, and stressful, even if the government ultimately agrees that the research in question was in good faith and thus should not be prosecuted.[199]

[80] The thorniest problem with nailing down safe harbor language is the potential for negative consequences if the safe harbor is either too generous or too stingy. As one DOJ official commented, "it is surprisingly hard to develop language that can both exempt legitimate security research and not create a loophole for bad-faith actors."[200] Threading that needle entails making policy trade-offs without losing sight of the greater goal of improving cybersecurity, and setting the line in the wrong place risks consequences that undermine the policy's purpose.

[81] Craft a baroque safe harbor that is too "tied down with detailed requirements and limitations,"[201] and white hat hackers may find it an unduly high bar to meet.[202] This approach treats impediments to white hat

[199] *See generally* Adams & Shin, *supra* note 96 ("How intrusive is it going to be into [researchers'] lives for [the government] to make that determination?").

[200] Johnson, *supra* note 99.

[201] Ed Felten, *The Chilling Effects of the DMCA*, SLATE (Mar. 29, 2013, 7:45 AM), https://slate.com/technology/2013/03/dmca-chilling-effects-how-copyright-law-hurts-security-research.html [https://perma.cc/HY25-HUT8].

[202] *See* ETCOVITCH & VAN DER MERWE, *supra* note 58, at 38 ("It is possible that the solution presented may be viewed as cumbersome and complicated by the parties wishing

participation as an acceptable trade-off for keeping black hats out. An onerous safe harbor, however, would be hard to distinguish from having no safe harbor at all, as it would still deter research (by those unable or unwilling to jump through all the hoops) or allow research to be punished after the fact (depending on implementation, *i.e.*, as a strict versus substantial compliance regime). Setting the bar too high would defeat the whole purpose of having the safe harbor, which is to encourage more socially desirable (and badly needed) research to happen than presently does under the current legal regime.

[82] On the other hand, if a safe harbor's eligibility requirements are too lax, there is a risk that black hats may take advantage of it to immunize their malicious activities.[203] This approach treats occasional abuse as an acceptable trade-off for incentivizing more research. Overall, this might be the better trade. The specter of CFAA liability has long chilled good-faith research,[204] but there are indications that it is not deterring malicious actors.[205] If attackers are already indifferent to legal consequences whereas

to engage in responsible disclosure."); Geiger, *supra* note 194 (conceding that Rapid7's proposal "is… admittedly complex!") (ellipsis in original).

[203] Geiger, *supra* note 194 ("Cyber criminals will claim to have good intent to confound prosecution or civil lawsuits, and CFAA liability protection should not shield security researchers that act recklessly and cause harm."); ETCOVITCH & VAN DER MERWE, *supra* note 58, at 30 ("The argument that malicious actors will use a responsible disclosure regime to acquire a legal safe harbor for their activity is rebutted by carefully considered definitions that make clear that only designated research activities are captured within the scope of the safe harbor.").

[204] *See supra* Section III.B (arguing that white-hat researchers will be deterred from their work by fear of criminal prosecution or civil suit under the CFAA).

[205] Thompson, *supra* note 74, at 540 ("[C]urrent laws and developing trends within the law may be inhibiting the white hats without sufficiently deterring cybercriminals and other assorted black hats."); Pfefferkorn, *supra* note 96 ("U.S. authorities have begun to acknowledge that 'black hat' hackers (particularly those overseas) appear largely unmoved by the threat of prosecution. That is, the specter of liability may be discouraging white hats from doing innocuous or beneficial security research, without meaningfully deterring malicious hacking."); Joseph Marks & Aaron Schaffer, *The*

researchers are risk-averse, then the addition of a readily-accessible safe harbor might have little effect on attacker behavior while clearing the way for more research that improves security (which, in turn, helps stymie the attackers). True, some attackers might still try to invoke the safe harbor if they get caught. But, as explained below, they will not necessarily succeed. It is more economical overall to impose a safe harbor with relatively low compliance costs for both supplicants (*i.e.*, researchers) and gatekeepers (*i.e.*, prosecutors). All told, the optimal level of abuse of a safe harbor system is probably not zero.[206]

[83] The idea that bad-faith actors would try to cloak their behavior in the mantle of "security research" is not an illusory concern. At her criminal trial, accused Capital One hacker Paige Thompson's defense counsel claimed that her actions were no different from those of ethical hackers who responsibly disclose the vulnerabilities they find.[207] Thompson's alleged

Cybersecurity 202: DOJ's future is in disrupting hackers, not just indicting them, WASH. POST (July 1, 2021, 7:18 AM), https://www.washingtonpost.com/politics/2021/07/01/cybersecurity-202-dojs-future-is-disrupting-hackers-not-just-indicting-them/ [https://perma.cc/QS26-TDVY].

[206] DAN DAVIES, LYING FOR MONEY: HOW LEGENDARY FRAUDS REVEAL THE WORKINGS OF THE WORLD 17 (Scribner 2021) ("We can't check up on everything, and we can't check up on nothing, so one of the key questions that a[] [system] has to make is how much effort to spend on checking. . . . [S]ince checking costs money and trust is really productive, the optimal level of fraud is unlikely to be zero."); *cf.* Kwame Anthony Appiah, *What Can You Do When Cheaters Take Advantage of Charity?*, N.Y. TIMES MAG. (July 13, 2022), https://www.nytimes.com/2022/07/12/magazine/food-donations-ethics.html [https://perma.cc/W992-575S] ("You think we could help more of those requiring assistance if we screened out those who don't. That's not necessarily the case. The optimal system — the one that does the most good — might tolerate a certain margin of abuse.").

[207] Kate Conger, *Ex-Amazon Worker Convicted in Capital One Hacking*, N.Y. TIMES (June 17, 2022), https://www.nytimes.com/2022/06/17/technology/paige-thompson-capital-one-hack.html [https://perma.cc/Z3E3-8R9M] [hereinafter *Ex-Amazon Worker Convicted*]; Kate Conger, *Fraud and Identity Theft Trial to Test American Anti-Hacking Law*, N.Y. TIMES (June 8, 2022), https://www.nytimes.com/2022/06/08/technology/

conduct included downloading the data of over 100 million Capital One customers and installing cryptocurrency-mining software on the company's servers.[208] According to a cybersecurity expert who commented on the case, these are "intentionally malicious actions that do not happen in the course of testing security."[209] Thompson's behavior is hard to square with the DOJ's definition of "good-faith security research" (announced about three weeks before her trial began),[210] and the jury didn't buy it. The jury found Thompson guilty of multiple counts of violating the CFAA.[211] The effort to paint Thompson as a white hat hacker failed, indicating that it is possible to see through bad-faith claims and tell the true color of someone's proverbial hat without resorting to "detailed requirements and limitations."[212]

[84] The perfect is the enemy of the good enough. The foregoing proposals show longstanding agreement that something more must be done to exempt security researchers from legal liability, along with simultaneous disagreement about what exactly to do. Between Bambauer and Day's proposal and the DOJ's new policy, a dozen years elapsed. Now that the DOJ has decided the current DMCA definition of "good-faith security

---

capital-one-hacker-trial.html [https://perma.cc/69JS-VVMF] [hereinafter *Fraud and Identity Theft*] (quoting Thompson's lawyers as saying her conduct was that of a "novice white-hat hacker").

[208] Maya Miller, *Ex-Amazon worker convicted in massive Capital One hack*, SEATTLE TIMES (June 17, 2022, 8:51 PM), https://www.seattletimes.com/business/ex-amazon-worker-convicted-in-massive-capital-one-hack/ [https://perma.cc/5TLT-VJQ3].

[209] *Fraud and Identity Theft*, *supra* note 207 (quoting Chester Wisniewski, principal research scientist at cybersecurity firm Sophos, who contrasted Thompson with "[l]egitimate people" who "will push a door open if it looks ajar").

[210] *DOJ Press Release*, *supra* note 88 ("[T]he new policy acknowledges that claiming to be conducting security research is not a free pass for those acting in bad faith.").

[211] Miller, *supra* note 208.

[212] Felten, *supra* note 201.

research" is good enough, maybe we will see a drop-off in commentator proposals for safe harbors; on the other hand, maybe future DMCA rulemakings will keep refining the definition of "good-faith security research."

[85] The difficulty of defining a safe harbor suggests that this is not the optimal means of protecting good-faith research, and so policymakers should turn elsewhere. The next section suggests an alternative approach to separating good-faith wheat from malicious chaff in the civil litigation context.

B. A New Proposal: Exclude Remediation Costs and Shift Fees

[86] This Article's approach to amending the CFAA would protect harmless research by reducing civil litigation over it instead of creating a carve-out from liability for it. We can put aside hand-wringing over the optimal definition of "good-faith security research" in favor of a simpler strategy: follow the money. This Article proposes (1) amending the CFAA's "loss" definition to prevent vulnerability remediation costs alone from satisfying the $5,000 statutory standing threshold in the absence of any other alleged loss, and (2) adding a fee-shifting provision that courts can apply in civil cases where the plaintiff does not allege qualifying losses that meet that threshold.

[87] The DOJ's recent choice in its new CFAA charging policy to endorse the DMCA definition of "good-faith security research" does not undermine this stance; to the contrary, the DOJ's decision bolsters this proposal. The DOJ has decided to address (however imperfectly) the criminal side of the statute's threat to security research.[213] With that

[213] *DOJ Press Release, supra* note 88. The process of determining to the DOJ's satisfaction that research counts as "in good faith" may itself prove to be an intrusive and stressful experience for the researcher. The DOJ's adoption of the DMCA definition from among those proposed does not cure the challenges of *applying* the definition in particular circumstances, which this Article's approach sidesteps entirely.

commitment in place, reining in civil litigation becomes the most impactful locus for reform efforts.[214]

1. Amend the Definition of "Loss"

[88] To foreclose "shooting the messenger" civil lawsuits against good-faith security researchers under the CFAA, this Article proposes amending the law so that the cost to remediate a vulnerability, standing alone, cannot satisfy the statute's $5,000 jurisdictional threshold. Tightening up the "loss" calculus would stymie retaliatory litigation against socially beneficial (or at least benign) security research. At the same time, it would preserve victims' ability to seek redress in cases where well-intended research activities (or instances of intentional malice) do cause harm—an avenue that would be unavailable if, as some commentators have recommended,[215] the Act's private cause of action were eliminated entirely.

[89] This Article suggests the following addition to the definition of "loss" in section 1030(e)(11) (in underline):

> the term "loss" means any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any

[214] *See* Geiger, *supra* note 194 ("In our estimation, the threat of private lawsuits against legitimate security researchers for 'loss' is much more common than federal criminal prosecution.").

[215] *E.g.*, Mayer, *supra* note 66, at 1501–02; Matwyshyn & Pell, *supra* note 35, at 552–557; Eric Goldman, *Online Trespass to Chattels Needs Structural Reform (Forbes Cross-Post)*, TECH. & MKTG. L. BLOG (Apr. 4, 2013), https://blog.ericgoldman.org/archives/2013/04/rethinking_onli.htm [https://perma.cc/7RFT-5NTM]; Orin Kerr, *Proposed Amendments to 18 U.S.C. 1030*, VOLOKH CONSPIRACY (Jan. 20, 2013, 1:10 PM), https://volokh.com/2013/01/20/proposed-amendments-to-18-u-s-c-1030/ [https://perma.cc/S389-A35C].

> revenue lost, cost incurred, or other consequential damages incurred because of interruption of service; except that for purposes of bringing a civil action for conduct involving the factor set forth in subclause (I) of subsection (c)(4)(A)(i), "loss" shall not include a victim's cost of testing, investigation, and/or correction of a security vulnerability as defined in 6 U.S.C. § 1501(17), where such cost is not reasonably necessary to prevent the offender from committing another offense under this section or causing additional damage or loss (as defined in this subparagraph) to any victim.

[90] This language borrows wording from the DMCA "good-faith security research" definition used in the DOJ's new CFAA charging policy and incorporates an existing statutory definition of "security vulnerability," as inspired by Rapid7's proposal.[216]

[91] The proposed amendment is also inspired by a 2000 Ninth Circuit case, *United States v. Middleton*,[217] which was decided under an earlier version of the CFAA that required a causal link between "damage" and "loss."[218] *Middleton* stated that the $5,000 loss calculation could not include the cost of making improvements that rendered the plaintiff's computer system *more* secure than it had been prior to the alleged violation.[219] More recent cases have not always agreed. [220] The costs of "security

[216] Geiger, *supra* note 194; *see also* 6 U.S.C. § 1501(17) ("The term 'security vulnerability' means any attribute of hardware, software, process or procedure that could enable or facilitate the defeat of a security control.").

[217] 231 F.3d 1207, 1208, 1212 (9th Cir. 2000).

[218] *Id.* at 1211 (citing 18 U.S.C. § 1030(e)(8)(A) (1996)).

[219] *Id.* at 1212–13 (citing legislative history).

[220] *See, e.g.*, M-I LLC v. Stelly, 733 F. Supp. 2d 759, 780 (S.D. Tex. 2010). This is not surprising; "[f]or each type of cost, with enough research, one can likely find case law

enhancements to Plaintiff's computer systems" and "the heightened security measures [plaintiff] put in place" have counted as loss in some cases,[221] whereas the costs of "prophylactic" measures that "sought to identify ways to improve the [plaintiff's] security systems" against prospective future intrusions have been discounted in others, even if they were prompted by the defendant's conduct.[222]

[92] The proposed statutory amendment aims to clarify that the rule should be that the cost to patch a security vulnerability should count as "loss" for standing purposes only where patching is needed to stop this defendant — not some prospective future attacker — from continuing to break the law, do damage, and/or increase losses to the victim.[223] Phrased another way, the cost of patching the vulnerability must be both reasonable and directly caused by the defendant's alleged CFAA violation.[224] Where the researcher was the one who disclosed the vulnerability to the plaintiff in the first place, precisely in the expectation that the plaintiff *would* patch said vulnerability, it will be difficult for the plaintiff to show that the patch was

---

that permits it to qualify and case law that holds it does not." Tuma, *supra* note 35, at 186.

[221] Integrated Waste Sols., Inc. v. Goverdhanam, No. 10-CV-2155, 2010 U.S. Dist. LEXIS 127192, at *26 (E.D. Pa. Nov. 30, 2010); Ticketmaster LLC v. Prestige Ent. W., Inc., 315 F. Supp. 3d 1147, 1173–74 (C.D. Cal. 2018).

[222] Univ. Sports Publ'ns Co. v. Playmakers Media Co., 725 F. Supp. 2d 378, 388 (S.D.N.Y. 2010). This language has been cited repeatedly by other Second Circuit district courts. *See* Cohen v. Gerson Lehrman Grp., Inc., No. 09-CV-4352, 2011 U.S. Dist. LEXIS 104551, at *23 (S.D.N.Y. Sept. 15, 2011); *see also* Millennium TGA, Inc. v. Leon, No. 12-CV-1360, 2013 U.S. Dist. LEXIS 150508, at *47 (E.D.N.Y. Sept. 24, 2013) (distinguishing between the "prospective" and "retrospective" audits undertaken by the plaintiff in *University Sports*, only the latter of which the court found cognizable as loss).

[223] *See Middleton*, 231 F.3d at 1213.

[224] *See* A.V. *ex rel.* Vanderhye v. iParadigms, LLC, 562 F.3d 630, 646 (4th Cir. 2009); Glob. Pol'y Partners, LLC v. Yessin, 686 F. Supp. 2d 642, 647 (E.D. Va. 2010).

anything other than a prophylactic measure against hypothetical future attacks.[225] Such prophylactic costs could not be used to establish standing to sue the researcher.

[93] This proposal is consistent with the Court's dicta in *Van Buren* about limiting the statutory meaning of "loss."[226] Under the Court's reading of "loss," civil plaintiffs would only be able to establish statutory standing under the CFAA if the defendant's actions caused "technological harms" that cost the plaintiff at least $5,000 to fix.[227] If the plaintiff's expenditures are not tied to some underlying "harm to computer data, programs, systems, or information services," then they are not "loss" and thus will not count towards the $5,000 threshold.[228] The current proposal, however, suggests amending the language of the statute, not relying on judge-made law or mere dicta, leaving less interpretive wiggle room for courts.

[94] This approach is intended to place a vendor that receives a responsible vulnerability disclosure from an outsider on the same footing as a vendor whose internal security team identifies a vulnerability. In the latter situation, the vendor is not a "victim," it has suffered no "loss," and there is nobody for the vendor to sue; fixing what the internal team found is just the cost of doing business. If the vendor's response to a good-faith researcher's responsible disclosure is to treat the research activity like a malicious hack and run up a huge bill investigating it, only to confirm the researcher caused no damage, the vendor risks having those costs deemed ineligible as a type of loss for being unreasonable and unnecessary. This proposed statutory

[225] The prospect of fee-shifting might help dissuade the plaintiff from trying to push this narrative where the evidence of the researcher's good-faith conduct will disprove it. *See infra* Section VI.B.2.

[226] *See* discussion *supra* Section IV.B.

[227] *See* Van Buren v. United States, 141 S. Ct. 1648, 1653, 1660 (2021).

[228] *Id.* at 1659–60 ("[Petitioner's] run of the license plate did not impair the 'integrity or availability' of data, nor did it otherwise harm the database system itself.").

amendment also mirrors the existing practice of judges who, bucking historical trend,[229] closely scrutinize plaintiffs' claimed losses.[230] A vendor might be able to externalize the task of bug-*hunting* onto outsiders, but it could not externalize the expense of bug-*fixing* onto them too.

[95] Disallowing plaintiffs from using vulnerability remediation costs alone to establish statutory standing might initially seem like it could help bad-faith actors escape accountability. Nevertheless, secret malicious hacks will do harm (above and beyond vulnerability patching costs alone) that good-faith research and responsible disclosure should not, enabling courts to draw a line between the former and the latter. This Article's proposal therefore will not let bad-faith actors off the hook by undermining hacking victims' ability to meet the $5,000 loss threshold.

[96] Recent CFAA litigation against "spyware" maker NSO Group shows that, as in Paige Thompson's case, accused bad actors will argue that they should not be held accountable for their conduct that brought others' security flaws to light.[231] At first glance, this Article's argument appears distressingly similar to the one NSO Group has repeatedly pushed in court. On closer examination, however, NSO's argument is distinguishable—and, like Thompson's, it did not hold up in court.

[97] NSO became notorious after its Pegasus malware, which it licenses to governments around the world, was attributed to the hacking of devices

[229] *See supra* notes 33–34 and accompanying text.

[230] *See* InfoTek Corp. v. Preston, No. 18-1386, 2022 U.S. Dist. LEXIS 163364, at *12, *14 (D. Md. Sept. 9, 2022) ("Victims of CFAA violations may neither make a mountain out of a molehill when investigating intrusions, nor use summary judgment to rubberstamp expenses toward the jurisdictional loss threshold. There remains a genuine dispute about whether InfoTek's costs were 'reasonably necessary' under the circumstances.").

[231] *See* WhatsApp Inc. v. NSO Grp. Techs., Ltd., 472 F. Supp. 3d 649, 683 (N.D. Cal. 2020).

belonging to hundreds of journalists, human rights activists, political dissidents, politicians, and government officials, among others.[232] The human rights abuses enabled by NSO's phone-hacking tools led the U.S. government to put the company under sanctions in late 2021.[233]

[98] Facebook/WhatsApp and Apple each sued NSO (together with its corporate parent during the relevant time period) in Northern California federal court for allegedly leveraging security flaws in Facebook's WhatsApp and Apple's iMessage to surreptitiously install the Pegasus spyware on victims' devices.[234] The WhatsApp complaint alleged that "Defendants' actions caused Plaintiffs to incur a loss as defined in 18 U.S.C. § 1030(e)(11), including the expenditure of resources to investigate and remediate Defendants' fraud and unauthorized access."[235] In nearly identical language, Apple's complaint alleged that "Defendants' actions caused Apple to incur a loss as defined by 18 U.S.C. § 1030(e)(11), in an amount in excess of $5,000 during a one-year period, including the expenditure of resources to investigate and remediate Defendants' conduct."[236]

---

[232] *See* The Associated Press, *Journalists, activists among firm's spyware targets, nonprofits say*, NBC NEWS (July 19, 2021, 11:38 AM), https://www.nbcnews.com/tech/security/journalists-activists-firms-spyware-targets-nonprofits-say-rcna1449 [https://perma.cc/RV8X-77RH].

[233] Drew Harwell, et al., *Biden administration blacklists NSO Group over Pegasus spyware*, WASH. POST (Nov. 3, 2021, 2:30 PM), https://www.washingtonpost.com/technology/2021/11/03/pegasus-nso-entity-list-spyware/ [https://perma.cc/J6GV-SG5R].

[234] *See* Complaint at 1–2, WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d 649 (N.D. Cal. 2020) (No. 19-CV-07123) [hereinafter WhatsApp Complaint]; Complaint at 1–2, Apple Inc. v. NSO Grp. Techs. Ltd., No. 21-CV-9078 (N.D. Cal. Nov. 23, 2021) [hereinafter Apple Complaint]. Note that the WhatsApp complaint pre-dates, and the Apple complaint post-dates, the Supreme Court's decision in *Van Buren*.

[235] WhatsApp Complaint, *supra* note 234, at ¶ 57; *see also id.* at ¶¶ 56, 73 (additional loss allegations).

[236] Apple Complaint, *supra* note 237, at ¶ 72.

[99] NSO responded in both cases by moving to dismiss the respective CFAA claims, asserting that the costs to "investigate and remediate" a pre-existing vulnerability were not cognizable "losses" under the CFAA.[237] In *WhatsApp*, NSO pointed to the Ninth Circuit's "narrow conception of 'loss'"[238] in challenging the plaintiffs' "theory of the case" that

> they incurred losses because [NSO] allegedly exploited a "vulnerability" in WhatsApp's product. That vulnerability . . . is what Plaintiffs had to "investigate and remediate." And the disclosure of that vulnerability—not [NSO's] mere[] access to user's [*sic*] devices—was responsible for any loss to Plaintiffs. Plaintiffs' alleged losses, therefore, were not "caused by" [NSO's] alleged intrusions into WhatsApp's users' devices . . . and they cannot sue [NSO] for [them].[239]

[100] Put another way, NSO seems to be saying that secretly exploiting a WhatsApp flaw to hack users' phones did no harm, and any "loss" WhatsApp incurred was WhatsApp's own fault for patching the vulnerability instead of letting NSO continue exploiting it. This is a bold argument to make, and the *WhatsApp* court rejected it.[240] The court found that the plaintiffs' allegations "that they incurred costs responding to the unauthorized access to users' phones by upgrading the WhatsApp system in response to defendants' intrusion" were "sufficient to state a claim for

[237] *See* Motion to Dismiss at 22–23, WhatsApp Inc. v. NSO Grp. Techs. Ltd., 472 F. Supp. 3d 649 (N.D. Cal. 2020) (No. 19-CV-07123) [hereinafter WhatsApp Motion to Dismiss]; Motion to Dismiss at 11, Apple Inc. v. NSO Grp. Techs Ltd., No. 21-CV-09078 (N.D. Cal. Nov. 3, 2021) [hereinafter Apple Motion to Dismiss].

[238] WhatsApp Motion to Dismiss, *supra* note 237, at 22 (citing *Andrews*, 932 F.3d at 1262-63).

[239] *Id.* at 22–23.

[240] *WhatsApp*, 472 F. Supp. 3d at 683.

loss based on responding to an offense on a third party's device."[241] The court refuted NSO's argument that WhatsApp's "loss derived from responding to a *vulnerability* in the WhatsApp system," not from WhatsApp's "expenditure of resources to investigate and remediate" NSO's "accessing of information on individual users' devices."[242]

[101] Despite failing to persuade the *WhatsApp* court, NSO later made the same argument when pushing for the dismissal of Apple's lawsuit. It said its "alleged interactions with Apple — finding flaws in Apple's iMessage program — are comparable to the activities of 'researchers' to whom Apple pays substantial 'bounties' for discovering security issues and vulnerabilities."[243] NSO asked the court to disregard Apple's costs of "investigating and remedying self-created vulnerabilities in [Apple's] software that pre-dated NSO's alleged conduct."[244] Even if NSO's alleged access to Apple's servers "exposed a preexisting vulnerability in Apple's software, which Apple then investigated and repaired," NSO argued, "[t]hat does not qualify as 'loss' under the CFAA," because "investigating the preexisting vulnerability in its software . . . is not the sort of 'damage' or 'loss' the CFAA covers."[245] "The CFAA is not a cost-shifting statute that allows a tech company . . . to investigate possible vulnerabilities and update its software at somebody else's expense," NSO added.[246]

---

[241] *Id.* (denying defendants' motion to dismiss CFAA claim).

[242] *Id.* at 683.

[243] Reply in Support of Motion to Dismiss at 1, Apple Inc. v. NSO Grp. Techs. Ltd., No. 21-CV-09078 (N.D. Cal. Nov. 3, 2021). By this rationale, Hannibal Lecter is "comparable" to an oncologist.

[244] *Id.* at 1.

[245] *Id.* at 6–7 (citing hiQ Labs, Inc. v. LinkedIn Corp., 31 F.4th 1180, 1195 n.12 (9th Cir. 2022); Phreesia, Inc. v. Certify Glob., Inc., No. 21-678, 2022 WL 911207, at *8 (D. Md. Mar. 29, 2022)).

[246] *Id.* at 7. This line in particular is gallingly similar to this Article's argument at first glance, although the resemblance dissipates when viewed up close.

[102] Again, victim-blaming is a bold litigation tactic to choose, and the Ninth Circuit shot down this very argument back in 2004. In *Creative Computing v. Getloaded.com LLC*,[247] the defendant argued that it did not "cause" (and thus should not have to pay damages for) the plaintiff's computer upgrades, because if the plaintiff had timely patched its system like it should have done anyway, that would have prevented the defendant's hack.[248] This did not go over well with the court, which called the argument "analogous to a thief arguing that 'I would not have been able to steal your television if you had installed deadbolts instead of that silly lock I could open with a credit card.'"[249] "A causal chain from the thief to the victim is not broken by a vulnerability that the victim negligently leaves open to the thief," the court chided.[250]

[103] This trespass metaphor reveals why NSO's argument that pre-existing vulnerabilities fall outside the CFAA's purview is nonsensical. The ability to hack into a computer system necessitates that some vulnerability (such as a weak lock) must already have existed which the hacker could exploit. If the metaphorical door were securely bolted, there could be no break-in; if a system's security were flawless, it could not get hacked. If there could be no liability for abusing a pre-existing security vulnerability to gain unauthorized access, there would be precious little left of the CFAA.

[104] Applying that rationale to the *Apple* case, by the same "causal chain" reasoning, Apple "suffer[ed] . . . loss by reason of" NSO's conduct for purposes of bringing a civil action.[251] The supposedly poor quality of the

[247] 386 F.3d 930, 935–36 (9th Cir. 2004).

[248] *Id.* at 935.

[249] *Id.* at 936.

[250] *Id.*

[251] 18 U.S.C. § 1030(g).

iMessage software code that NSO had the chutzpah to criticize is irrelevant, because the CFAA presupposes the existence of some weakness that gave rise to damage or loss when exploited. However, the *Apple* court never had occasion to evaluate NSO's arguments because the case was administratively closed in June 2022, terminating NSO's pending motion to dismiss.[252] We therefore do not know whether NSO's theory would have fared better than it did in *WhatsApp*. Still, it seems likely that the *Apple* court would have reached the same conclusion based on *Creative Computing* as well as the *WhatsApp* order and the cases it cited.

[105] Whether it is sincere or self-serving, NSO's stance — that the plaintiffs should not be allowed to sue NSO just because they spent money fixing their own pre-existing security flaws — sounds a lot like this Article's thesis. In a rejection of NSO's position, the *WhatsApp* court interpreted the cost of responding to an offense to encompass the cost of upgrading software to patch a security vulnerability[253] — precisely what this Article suggests should not, on its own, establish standing. Yet the court's decision to let the CFAA claim against NSO proceed is not contrary to this Article's proposal.

[106] NSO's actions are easily distinguishable from the good-faith security research this Article seeks to protect. In each lawsuit, stressing the plaintiff's "pre-existing vulnerability" was a way for NSO to gloss over all the parts of the complaint that described how it allegedly abused that vulnerability to covertly spy on users on an ongoing basis, through malware it had installed on their phones by sending malicious code over the

[252] Order to Administratively Close, Apple Inc. v. NSO Group Techs. Ltd., No. 21-CV-09078-JD (N.D. Cal. June 23, 2022), Dkt. No. 40, https://www.courtlistener.com/docket/61570971/apple-inc-v-nso-group-technologies-limited/ ("At the parties[']joint request . . . the stay is extended until the Supreme Court decides whether to issue a writ of certiorari . . . . All hearings are vacated, the motion to dismiss . . . is terminated without prejudice, and the case is administratively closed.").

[253] *WhatsApp*, 472 F. Supp. 3d at 683.

plaintiffs' servers, until the plaintiffs found out and put a stop to it.[254] When those allegations stay in the picture, as they do in the *WhatsApp* court's ruling, it is evident that NSO's conduct looks nothing like "good-faith security research," irrespective of one's preferred definition of that term.[255] Rather, secretly hacking users' phones by exploiting a previously-unknown WhatsApp or iMessage vulnerability looks a lot more like Paige Thompson's "intentionally malicious actions" far afield from normal security testing, for which she was convicted.[256]

[107] After all, whatever one thinks "responsible disclosure" means,[257] at a minimum it requires *disclosure* — something NSO conveniently elided when comparing itself to the researchers who submit bugs to Apple's bug bounty program.[258] NSO hid its knowledge of the apps' vulnerabilities from WhatsApp and Apple, allegedly in order to make hundreds of millions of dollars exploiting them on behalf of NSO's clients.[259] That is not "good

[254] There's a certain "*Scooby Doo* ending" energy to NSO's argument: "And I would've gotten away with it too, if it weren't for you meddling kids!" *See List of 'And I Would Have Gotten Away With It Too, If It Weren't For You Meddling Kids' Quotes*, SCOOBYPEDIA, https://scoobydoo.fandom.com/wiki/List_of_%22And_I_Would_Have_Gotten_Away_With_It_Too,_If_It_Weren%27t_For_You_Meddling_Kids%22_Quotes [https://perma.cc/EHJ4-BYQS].

[255] *See supra* Sections IV.A, VI.A (discussing the DOJ's new charging policy and commentators' proposals for research safe harbor).

[256] *Fraud and Identity Theft*, *supra* note 207.

[257] *See supra* Section III.A.

[258] NSO Reply in Support of Motion to Dismiss at 1, Apple v. NSO Grp. Techs., Ltd., No. 21-CV-09078 (N.D. Cal. May 18, 2022).

[259] Apple Complaint, *supra* note 234, at ⁋⁋ 48–53, 55, 59-60 (noting that Apple was notified by academic researchers of the vulnerabilities at issue and claiming to be "in a continual arms race" with NSO); WhatsApp Complaint, *supra* note 237, at ⁋⁋ 44–45 (stating that Facebook discovered WhatsApp's vulnerability on its own); *see also CVE-2019-3568 Detail*, NAT'L INST. OF STDS. & TECH., https://nvd.nist.gov/vuln/detail/CVE-2019-3568 [https://perma.cc/YWL3-Q3Z9].

faith" behavior.[260] This distinction makes quick work of the cynical claim that a theory of CFAA liability that covers NSO's or Thompson's conduct would also cover legitimate security research.

[108] The fact patterns alleged in the *WhatsApp* and *Apple* lawsuits also illustrate why the *WhatsApp* court's finding that the plaintiff had met the $5,000 loss threshold is not at odds with the idea of excluding remediation costs from counting toward that threshold. The goal of this proposal is to protect research activity that is both good-faith and harmless (and indeed, often beneficial). The proposed amendment does *not* exclude the cost to remediate a security vulnerability where, as with NSO, the defendant is the one actively exploiting the vulnerability and patching is necessary to stop the attack. By contrast, had Apple attempted to sue Citizen Lab, the academic security-research organization that discovered NSO's iMessage exploit and reported it to Apple, the proposed amendments to the CFAA would prevent Apple from establishing standing to sue Citizen Lab just because Apple undertook "extensive research, engineering, and testing around the clock" upon receiving Citizen Lab's report.[261] Citizen Lab was the one to report the iMessage exploit to Apple, but Citizen Lab was not the one allegedly secretly exploiting iMessage to hack Apple users. The expense of stopping NSO's surreptitious hacking activities cannot be laid at Citizen Lab's feet, even though Citizen Lab's report prompted a costly frenzy of activity at Apple (and even though Citizen Lab studied the exploit by forensically analyzing iPhones,[262] over which Apple asserted in its complaint that it retains ownership of the operating system software[263]).

[260] *See supra* Section IV.A.

[261] Apple Complaint, *supra* note 234, at ⁋⁋ 48–53.

[262] Complaint Exhibit 3 at 2, Apple v. NSO Grp. Techs., Ltd., No. 21-CV-09078 (N.D. Cal. Nov. 23, 2021) (displaying a Citizen Lab report dated Sept. 13, 2021, describing Citizen Lab's analysis of the iPhone of a Saudi activist that had been infected with NSO's spyware program "Pegasus").

[263] Apple Complaint, *supra* note 234, at ⁋ 70 & n.27.

[109] Apple did not patch the iMessage vulnerability because Citizen Lab's report raised the hypothetical possibility that someone might exploit it in the future. It patched it because NSO was allegedly actively exploiting it already, to the detriment of Apple's users. There is a clear difference between security research that is done in good faith and causes no harm and bad actors' harmful, malicious conduct. This distinction has held up in court in the *WhatsApp* case and the *Thompson* case.

[110] Given NSO's notoriety, it is worth recognizing the risk that a desire to see NSO held accountable might lead courts, counsel, or commentators to condone a broad interpretation of cognizable "loss" that would move the law in an undesirable direction. That is, bending over backwards to keep an unlikable defendant on the hook can have unintended consequences once that holding is later applied to good-faith actors.[264] But it was hardly novel for WhatsApp and Apple to include the cost of upgrading their software to stop NSO's attacks as part of their complaints' loss allegations (as evidenced by the *WhatsApp* court's citations to existing interpretations of "loss"[265]). Going forward, a stricter definition of "loss" for standing purposes would help to make sure good-faith actors do not get caught up in the liability net.

[111] *Van Buren* is not to the contrary. Since Apple's and WhatsApp's remediation costs were occasioned by the "technological harms" of NSO's

[264] *See* Andrea Peterson, *Hacker/Troll 'Weev' Will Walk Free. But the Court Didn't Rule on the Main Issue.*, WASH. POST (Apr. 11, 2014, 2:38 PM), https://www.washingtonpost.com/news/the-switch/wp/2014/04/11/hackertroll-weev-will-walk-free-but-the-court-didnt-rule-on-the-main-issue/ [https://perma.cc/LX4Y-65X7] (discussing the overturned CFAA conviction of Andrew "weev" Auernheimer, an Internet troll whose case drew the support of digital-rights groups despite his notoriety because his conduct resembled "the kind of thing that cybersecurity researchers and 'white hat' hackers do").

[265] WhatsApp, Inc. v. NSO Group Techs. Ltd., 472 F. Supp. 3d 649, 683 (N.D. Cal. July 16, 2020).

conduct, the *Van Buren* dicta would have provided additional support in either case for a finding that the plaintiffs had asserted sufficient losses tied to NSO's alleged conduct to establish standing to sue NSO.[266] The view of "loss" urged by *Van Buren* and by this Article, while narrow, still permits bad actors to be held accountable for the harms they cause.

2. Adding a Fee-Shifting Provision That Can Apply When the Loss Threshold is Not Met

[112] In addition to limiting the loss calculus to exclude remediation costs, this Article also proposes that the CFAA be amended to allow for the shifting of litigation fees from defendant to plaintiff in cases where the plaintiff proves unable to meet the revised $5,000 bar. Fee-shifting would act as a deterrent against asserting weak CFAA claims and would give the recipients of legal threats some leverage to fight back, even before a threat matured into a filed complaint.

[113] Under the "American rule," litigants in U.S. courts generally bear their own costs except where Congress has expressly provided otherwise.[267] Meanwhile, the cost of civil litigation puts a price tag on justice that is beyond most Americans' reach.[268] Taken in combination, the American rule and the costliness of litigation allow the legal system itself to be wielded as a weapon for inflicting pain on one's enemies, irrespective of the ultimate outcome of the case.[269] The specter of financial ruin from defending oneself

[266] Van Buren v. United States, 141 S. Ct. 1648, 1659–60 (2021).

[267] Key Tronic Corp. v. United States, 511 U.S. 809, 815 (1994).

[268] *See* Deborah Rhode, *Access to Justice: A Roadmap for Reform*, 41 FORDHAM URB. L.J. 1227, 1228 (2014) ("Over four-fifths of the poor's legal needs and two- to three-fifths of the legal needs of middle-income Americans remain unmet.").

[269] *See* Marie Gryphon, *Assessing the Effects of a "Loser Pays" Rule on the American Legal System: An Economic Analysis and Proposal for Reform*, 8 RUTGERS J.L. & PUB. POL'Y 567, 568 (2011) ("The American rule makes the civil justice system as a whole

in court makes the mere threat of a lawsuit a powerful cudgel for dissuading, punishing, or covering up behavior a vendor dislikes — such as the responsible public disclosure of a security vulnerability[270] by a researcher who is likely flying solo.[271]

[114] To deter such misuse of the legal system, this Article proposes adding a fee-shifting provision that can be invoked by researchers who prevail in lawsuits brought by vengeful vendors. Etcovitch and van der Merwe's safe harbor proposal made the same suggestion for similar reasons.[272] They did not suggest particular language, so this Article proposes adding the following sentence to the end of section 1030(g), the CFAA's private right of action provision:

> 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.

[115] This language borrows from section 285 of the Patent Act,[273] which is one of the more than 150 fee-shifting provisions found in federal law.[274]

---

unnecessarily costly by encouraging the filing of [abusive] lawsuits . . . [and] also makes most legal victories Pyrrhic ones.").

[270] *See* Thompson, *supra* note 74, at 567 ("[E]ven a settlement-focused litigation strategy provides another profound deterrent to unauthorized access for possible ethical hackers").

[271] *See* Gamero-Garrido et al., *supra* note 46, at 1501 (claiming that independent vulnerability researchers outnumber internal employees or contractors).

[272] ETCOVITCH & VAN DER MERWE, *supra* note 58, at 25.

[273] 35 U.S.C. § 285 ("The court in exceptional cases may award reasonable attorney fees to the prevailing party.").

[274] ETCOVITCH & VAN DER MERWE, *supra* note 58, at 25 (citing Robert R. Percival & Geoffrey P. Miller, *The Role of Attorney Fee Shifting in Public Interest Litigation*, 47 L. & CONTEMP. PROBS. 233 (1984)).

Of those, most exist to encourage public interest litigation.[275] Deterring and defending CFAA cases against researchers is in the same vein, since safeguarding cybersecurity research is in the public interest and the ability to recoup fees would encourage attorneys to defend accused researchers.[276]

[116] The intent in adding this language is for it to be interpreted as the Supreme Court interpreted the Patent Act provision in 2014: "an 'exceptional' case is simply one that stands out from others with respect to the substantive strength of a party's litigating position (considering both the governing law and the facts of the case) or the unreasonable manner in which the case was litigated."[277] In applying this standard, courts consider factors including "frivolousness, motivation, objective unreasonableness (both in the factual and legal components of the case) and the need in particular circumstances to advance considerations of compensation and deterrence."[278]

[117] Those are precisely the factors at play in "shooting the messenger" lawsuits by vengeful vendors. In such situations, the vendor has suffered no harm, yet it seeks to use the legal system punitively, both to shift the cost of fixing its vulnerability onto the good-faith actor who responsibly reported it and to scare off anyone else from researching its product's flaws. The court's finding that the plaintiff cannot establish $5,000 in loss (exclusive of vulnerability remediation costs) is relevant to the court's fee-shifting inquiry, as it can be considered probative of the frivolousness and objective

[275] *Id.*

[276] *Id.* ("We believe the important policy rationales for granting attorneys fees to the winners are present in this use case: it would deter baseless litigation that would create social detriment, the statute is designed to create public benefit, and the parties in potential litigation have vastly unequal access to resources.").

[277] Octane Fitness, LLC v. Icon Health & Fitness, Inc., 572 U.S. 545, 554 (2014).

[278] *Id.* at 554 n.6.

unreasonableness of asserting a CFAA claim for which the plaintiff lacks standing.[279]

[118] Moreover, the proposed fee-shifting provision is broadly worded enough that it could also be invoked in situations where a plaintiff does meet the revised $5,000 threshold — such as where a court allows a vendor's costs to investigate and confirm there has been no damage after the vendor receives a researcher's responsible vulnerability disclosure — but nevertheless merits sanctions for other reasons such as unreasonable or bad-faith behavior. A vengeful vendor who can establish standing but who nevertheless uses the legal system punitively against a researcher would still risk incurring fees under the proposed language.

[119] At the same time, the *Octane Fitness* test[280] should operate to prevent fee awards where the court's inquiry concludes that a plaintiff made its CFAA claim in good faith but simply pleaded it insufficiently. In those cases, as in patent disputes, the plaintiff should not generally be found to have advanced a frivolous claim.[281] As is, CFAA plaintiffs who initially fail to assert $5,000 in loss typically get a chance to amend their complaint to add the requisite allegations.[282] That would not change under this amendment.

---

[279] *See* JEROLD S. SOLOVY ET AL., SANCTIONS UNDER RULE 11 70–71 (2010), https://jenner.com/system/assets/assets/5514/original/Sanctions_20Under_20Rule_2011-Complete_2010.pdf?1323114005 [https://perma.cc/5YRE-74TL] (in the similar context of sanctions under Rule 11 of the Federal Rules of Civil Procedure, "[a]ssertion of a claim with a clear, insurmountable procedural or jurisdictional defect has been held to be sanctionable conduct.").

[280] *Octane Fitness*, 572 U.S. at 554, 558 n.6.

[281] *See* Hockeyline, Inc. v. STATS LLC, No. 13-CV-1446, 2017 WL 1743022, at *5 (S.D.N.Y. Apr. 27, 2017) ("[W]here a party has set forth some good-faith argument in favor of its position, it will generally not be found to have advanced 'exceptionally meritless' claims.").

[282] *E.g.*, Deck v. Courtney, No. 21-CV-1078, 2021 U.S. Dist. LEXIS 147768, at *5-6 (S.D. Ind. Aug. 6, 2021).

[120] The specter of being liable for a defendant's fees and costs — which rise in tandem with the duration and intensity of the litigation — would help to deter would-be plaintiffs from ever filing suit in the first place.[283] Upon receiving a legal threat from a vengeful vendor over a disclosure of a vulnerability (whether before or after public disclosure is made), the threatened researcher (or her lawyer) could not only explain in response why vulnerability remediation costs alone do not create CFAA civil standing, but also cite the fee-shifting provision as a warning not to make good on the threat to sue. (Perhaps the chastened vendor would decide its money would be better spent on its security team than its outside counsel.)

[121] Adding fee-shifting to the CFAA would have other benefits. Coupled with the *Van Buren* decision narrowing the scope of permissible claims under the Act, these statutory changes would be felt beyond the context of vendor versus researcher. They would help rein in the CFAA's rampant misuse in civil litigation contexts far afield from the law's core anti-hacking purpose. Plaintiffs have been able to "craft a colorable [CFAA] claim from myriad modern fact patterns" that "look nothing like hacking."[284] This has prompted some commentators to call the private right of action "a failed experiment" and propose eliminating it entirely.[285] A fee-shifting amendment would target that misuse while preserving the private

[283] ETCOVITCH & VAN DER MERWE, *supra* note 58, at 25 ("[Fee shifting] alleviates some of the burden [on researchers] and possibly serves as a disincentive when vendors are deciding, ex ante, whether to file a lawsuit: as losers of the lawsuit, vendors would be forced to bear that cost, potentially making vendors more risk averse in filing suits against researchers on the margin.").

[284] Mayer, *supra* note 66, at 1457, 1506; *see also id.* at 1457 ("The overwhelming majority of civil claims arise from mundane employment and commercial disputes, not sophisticated computer intrusions.").

[285] *Id.* at 1453–1454, 1501; Goldman, *supra* note 215; Kerr, *Proposed Amendments to 18 U.S.C. 1030, supra* note 215; *see also* Eric Goldman, *The Computer Fraud and Abuse Act Is a Failed Experiment*, FORBES (Mar. 28, 2013, 4:21 PM), http://www.forbes.com/sites/ericgoldman/2013/03/28/the-computer- fraud-and-abuse-act-is-a-failed-experiment/ [https://perma.cc/Z8XU-E526].

right of action for appropriate cases, as explained below. Fee-shifting might also disincentivize civil plaintiffs from asserting novel legal interpretations that stretch the boundaries of the statute. *Van Buren* signaled that the law should be construed more narrowly than it has been over the years. Civil litigants may need a little prodding to take the hint.

3. Harmed Plaintiffs Would Still Have a Remedy

[122] The best-laid plans of mice and men often go awry.[286] So, too, can security research end up inadvertently harming the research target, as happened in the first-ever criminal CFAA prosecution.[287] The two proposed amendments to the CFAA would not leave plaintiffs without any recourse if they have a legitimate grievance against a security researcher. If well-intentioned research goes awry and causes enough harm, the CFAA will still be available.[288] If the harm falls below the $5,000 threshold, the plaintiff would be free to pursue other claims besides the CFAA.

[123] Even before *Van Buren*, plaintiffs frequently asserted a variety of other claims in addition to a CFAA cause of action, such as claims for breach of contract, intellectual property violations, and business torts, as well as claims under state-level computer trespass laws and the federal

[286] Robert Burns, *To a Mouse*, POETRY FDN., https://www.poetryfoundation.org/poems/43816/to-a-mouse-56d222ab36e33 [https://perma.cc/6EAP-8NYC] ("The best laid schemes o' Mice an' Men / Gang aft agley."). For a plan gone awry involving a different mouse, *see* FANTASIA (Walt Disney Prods. 1940).

[287] Kerr, *Norms of Computer Trespass, supra* note 64, at 1159.

[288] Criminal enforcement, not just civil action, could still be on the table in situations where research goes wrong. The DOJ's new CFAA charging policy does not precisely define what conduct the DOJ will or will not deem "good faith," but it does require research to be "carried out in a manner designed to avoid any harm to individuals or the public." *DOJ Charging Policy*, *supra* note 89.

Electronic Communications Privacy Act.[289] Now that *Van Buren* has narrowed the scope of permissible CFAA claims, those other causes of action will assume greater importance to plaintiffs.

[124] The sufficiency of alternative causes of action post-*Van Buren* is supported by two pre-*Van Buren* empirical studies of civil CFAA cases. From his analysis of non-CFAA claims in civil filings, Jonathan Mayer concluded that, "in civil litigation, CFAA and conventional bases of liability are usually redundant. Plaintiffs evidently believe they have a broad range of colorable theories for recovery."[290] Subsequently, Andrea Matwyshyn & Stephanie Pell published an analysis of civil CFAA cases decided in the year 2018.[291] They found that most were competition matters (*e.g.*, companies suing each other or their employees); of those, the CFAA claim was nonviable in the majority of cases.[292] Further, in the minority of potentially-meritorious claims, "alternative means of statutory or common law redress appeared to exist to compensate the claimant for any compensable harms in almost all cases."[293] On this basis, the authors recommended removing the CFAA's private right of action, as doing so "is

[289] Mayer, *supra* note 66, at 1489; Eric Goldman, *Do We Even Need the Computer Fraud & Abuse Act (CFAA)?–Van Buren v. US*, TECH. & MKTG. L. BLOG (June 9, 2021), https://blog.ericgoldman.org/archives/2021/06/do-we-even-need-the-computer-fraud-abuse-act-cfaa-van-buren-v-us.htm [https://perma.cc/9SSX-F3ME]; *see also* Kathleen C. Riley, Note, *Data Scraping as a Cause of Action: Limiting Use of the CFAA and Trespass in Online Copying Cases*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 245, 265–79 (2019) (studying the use of other claims alongside CFAA in data scraping disputes).

[290] Mayer, *supra* note 66, at 1489.

[291] Matwyshyn & Pell, *supra* note 35, at 557.

[292] *Id.*

[293] *Id.*

unlikely to significantly correlate with foreclosing civil redress for most plaintiffs currently including CFAA civil claims in their pleadings."[294]

[125] This Article does not go so far as to endorse eliminating section 1030(g), but these studies' findings support the proposed amendments in two ways. First, if a majority of civil CFAA claims are not meritorious, then it is desirable to discourage them from being filed by making it harder to satisfy the $5,000 loss threshold and adding a fee-shifting provision. Second, they indicate that plaintiffs could still obtain appropriate redress under other theories even if the CFAA were unavailable to them for whatever reason.

[126] To avoid fee-shifting, the choice for plaintiffs is simple: stop asserting dubious CFAA claims and focus instead on stronger legal theories with a greater likelihood of success. Minimizing weak claims conserves judicial economy by freeing up the parties and the court to focus on the most viable part of the dispute.[295] Presenting the strongest version of the plaintiff's case could also incentivize defendants to settle, enabling the plaintiff to get a remedy faster while reducing the court's caseload.

[127] Curtailing the Act's misuse in litigation as an impressive-looking but illusory cudgel to intimidate a (likely weaker) party would not put the law out of plaintiffs' reach in appropriate cases. If a plaintiff incurs more than $5,000 in losses from security research gone wrong, then a CFAA claim is still in-bounds. The plaintiff would of course still have to make its case on the merits, but statutory standing would not pose a problem.

VII. CONCLUSION

[294] *Id.* at 557–58.

[295] *Cf.* DocMagic, Inc. v. Ellie Mae, Inc., 745 F. Supp. 2d 1119, 1155 (N.D. Cal. 2010) ("Good lawyering does not require pleading every cause of action that may even remotely appear possible. Rather, it requires careful analysis and selectivity.").

[128] The time is ripe to make the legal landscape safer for security researchers. *Van Buren*'s "loss" dicta points to an encouraging direction for CFAA reform, and the DOJ's surprise policy shift indicates that such reforms are feasible and timely. For Congress to tighten up the statutory standing requirements and add a fee-shifting option in civil CFAA cases would help further the project of protecting security research that the executive and judicial branches have begun. Those who responsibly disclose security vulnerabilities are not like those who choose to exploit them. Federal computer trespass law should acknowledge the difference.