DEBUGGING THE CFAA'S HYBRID STRUCTURE

Andrew Sgarro*
April 2020

* J.D. Candidate 2021, Columbia Law School. I would like to thank Professor Daniel Richman for his invaluable guidance, and AJ Howard and Christine Rua for their helpful comments.

INTRODUCTION

For years, lawyers, technologists, and digital rights activists have denounced the Computer Fraud and Abuse Act ("CFAA") as vague, dangerous, and overbroad.[1] Courts have struggled to interpret its imprecise language,[2] prosecutors have grappled with how vigorously to enforce it,[3] private plaintiffs have attempted to shape it for their own ends,[4] and defendants, along with open-Internet advocates, have pushed back against its expansion.[5]

Broad interpretations of the CFAA criminalize a wide range of everyday computer conduct.[6] Prosecutors have already used this overbreadth to bring disproportionate charges against politically unpopular individuals for minor misconduct.[7] The most famous CFAA prosecution ended in 2013, when Internet activist Aaron Swartz committed suicide three months before his trial, at which he would have faced up to fifty years in prison for publicly releasing millions of academic papers that most university affiliates could already read for free.[8] Threat of prosecution still deters cybersecurity research, making the Internet less safe.[9] It also discourages the work of

1 *See, e.g.*, Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), https://www.newyorker.com/news/news-desk/fixing-the-worst-law-in-technology (calling the CFAA "the most outrageous criminal law you've never heard of"); Jack Detsch, *Influencers: Antihacking Law Obstructs Security Research*, PASSCODE, CHRISTIAN SCIENCE MONITOR (July 14, 2016), https://www.csmonitor.com/World/Passcode/Passcode-Influencers/2016/0714/Influencers-Antihacking-law-obstructs-security-research (relating that 75% of "Passcode's group of digital security and privacy experts" stated that the CFAA "overly restricts necessary security research"); Rebecca Jeschke, *EFF Asks the Supreme Court to Put a Stop to Dangerously Broad Interpretations of the Computer Fraud and Abuse Act*, ELECTRONIC FRONTIER FOUNDATION (Jan. 27, 2020), https://www.eff.org/deeplinks/2020/01/eff-asks-supreme-court-put-stop-dangerously-broad-interpretations-computer-fraud (describing the CFAA as "vague and draconian—putting people at risk for prison sentences for ordinary Internet behavior").

2 *See infra* Section I.B.

3 *See infra* Section II.B.2.

4 *See infra* Section II.C.3.ii.

5 *See supra* note 1.

6 Tor, Ekeland, *How to Reform the Outdated Federal Anti-Hacking Law*, PASSCODE, CHRISTIAN SCIENCE MONITOR (Mar. 24, 2017) (stating that "the CFAA . . . criminalizes what many consider normal behavior").

7 *See* Kim Zetter, *The Most Controversial Hacking Cases of the Past Decade*, WIRED (Oct. 26, 2015), https://www.wired.com/2015/10/cfaa-computer-fraud-abuse-act-most-controversial-computer-hacking-cases/.

8 Peter Ludlow, *Aaron Swartz Was Right*, CHRONICLE REVIEW (Feb. 25, 2013), https://www.chronicle.com/article/Aaron-Swartz-Was-Right/137425 (arguing that Swartz was right to promote public access to academic information).

9 Joseph Lorenzo Hall & Stan Adams, *Taking the Pulse of Hacking: A Risk Basis for Security Research*, CTR. DEMOCRACY & TECH. 9 (Mar. 2018), https://cdt.org/files/2018/04/2018-03-27-Risk-Basis-for-Security-Research-

journalists and academics, inhibiting the Internet's potential to promote public interest projects.[10] And it subjects all of us who share Netflix passwords, or browse Facebook during work hours in violation of company policy, to the mercy of prosecutors, which makes the Internet less free.[11]

The CFAA also has a civil provision, which powerful companies have used as a tool to suppress competition and innovation.[12] By filing civil CFAA suits against competitors using automated scripts to access their public websites, private companies have eroded the open access norms that have made the Internet such a useful tool for journalists, researchers, and activists, among others.[13] These civil CFAA suits also strengthen the monopolies held by large technology companies and restrict employee mobility.[14]

Most CFAA scholarship has focused exclusively on the statute's criminal enforcement.[15] In contrast, this Note analyzes how the CFAA's hybrid structure—its combination of criminal and civil provisions—has contributed to its overbroad reach and overzealous use in both criminal and civil contexts. This Note argues that implementing criminal-specific and civil-specific narrowing measures could counteract the overbreadth and overuse caused by the statute's hybrid structure.

Part I of this Note presents an overview of the CFAA. Part I relates the CFAA's legislative history, describes how judges interpret the statute inconsistently, and surveys how it is used in practice. Part II investigates how the CFAA's hybrid structure has influenced its development. Part II first introduces the theory behind hybrid statutes and the problems that these statutes tend to create. Then, Part II identifies what prosecutors and judges have already done to mitigate the

FNL.pdf (noting that "[u]ncertainty potentially resulting in steep criminal penalties creates a significant chilling effect for [cybersecurity] researchers").

[10] Jamie L. Williams, *Automation is Not "Hacking": Why Courts Must Reject Attempts to Use the CFAA as an Anti-Competitive Sword*, 24 B.U. J. SCI. & TECH. L. 416, 448 (2018).

[11] *See infra* notes 72–75 and accompanying text.

[12] *See infra* Section I.C, Section II.C.3.ii.

[13] Williams, *supra* note 10, at 416–22.

[14] *Id.*

[15] Andrea M. Matwyshyn & Stephanie K. Pell, *Broken*, 32 HARV. J.L. & TECH. 479, 492 (2019).

dangers posed by the CFAA's hybrid structure. Lastly, Part II explains why the CFAA's hybrid structure has continued to expand the statute. Part III offers four solutions aimed at reducing the negative effects generated by the CFAA's hybrid structure. Part III proposes that Congress amend the civil provision to prohibit claims that arise out of contract breaches or business torts and to give judges the option to award attorneys' fees to victorious defendants. Part III also recommends that Congress heighten the CFAA's mens rea requirement for criminal liability, and it suggests that the Department of Justice ("DOJ") require prosecutors to obtain its approval before charging CFAA crimes.

I. AN OVERVIEW OF THE CFAA

This Part describes the CFAA's legislative history, judicial interpretation, and practical application. Section I.A tracks the history of Congress' expansion of the CFAA over the course of twenty-four years.[16] Section I.B demonstrates how federal courts struggle to interpret and apply the CFAA. And Section I.C relays data on how often prosecutors and plaintiffs bring cases under the CFAA.

A. The CFAA's Legislative History

In October of 1984, in response to "a flurry of electronic trespassing incidents" and the techno-thriller movie *WarGames*,[17] Congress enacted the first federal computer crime statute, and the precursor to the CFAA: the "Counterfeit Access Device and Computer Fraud and Abuse Act" ("CADCFAA").[18]

[16] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563 (2010) ("The law that began as narrow and specific has become breathtakingly broad.").

[17] 21 H.R. REP. No. 98-894, at 8–10 (1984); *see also* Williams, *supra* note 10, at 438 ("Congress was concerned about nightmare scenarios like that depicted in *WarGames* . . . which it (incorrectly) viewed as [realistic]").

[18] Kerr, *supra* note 16, at 1564.

The CADCFAA was a narrow statute designed to criminalize hacking.[19] Congress trusted that established criminal laws would cover established crimes—such as fraud, theft, and destruction of property—committed via computer.[20] But Congress also recognized that established criminal laws could not encompass computer abuse crimes that involved only "magnetic impulses" and "intangible property."[21] So it passed the CADCFAA to address those new crimes.[22] Codified at 18 U.S.C. § 1030, the CADCFAA proscribed "knowingly accesses[ing] a computer without authorization, or having accessed a computer with authorization, us[ing] the opportunity such access provides for purposes to which such authorization does not extend"[23] to obtain national security secrets ((a)(1)),[24] to obtain personal financial records ((a)(2)),[25] or to hack into a U.S. government computer((a)(3)).[26] The statute did not cover computer crime outside of these narrow parameters.

[19] *See* David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*, 103 J. CRIM. L. & CRIMINOLOGY 907, 913 (2013) ("According to one of its leading sponsors, Representative William J. Hughes, the CFAA's primary focus was 'technologically sophisticated criminal[s] who break[] into computerized data files.'"); Dennis Longley & Michael Shain, DICTIONARY OF INFORMATION TECHNOLOGY 146 (2d ed. 1986) (defining a "hacker" as: "a computer enthusiast. The term is normally applied to people who take delight in experimenting with system hardware, software and communication systems. Sometimes used with the connection of illegality, especially in reference to unauthorized access to data.").

[20] Samantha Jensen, Note, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81, 86 (2014).

[21] 21 H.R. REP. No. 98-894, at 9–12 (1984) ("People can relate to mugging a little old lady and taking her pocketbook, but the perception is that perhaps there is not something so wrong about *taking information* by use of a . . . computer even if it costs the economy millions now and potentially billions . . . .") (emphasis added).

[22] *Id.*

[23] 18 U.S.C. § 1030(a)(1)–(3) (Supp. II 1985); Kerr, *supra* note 16, at 1564.

[24] 18 U.S.C. § 1030(a)(1) (Supp. II 1985) (making such conduct a felony when done to obtain protected government information "with the intent or reason to believe that such information so obtained is to be used to the injury of the United States, or to the advantage of any foreign nation").

[25] 18 U.S.C. § 1030(a)(2) (Supp. II 1985) (making such conduct a misdemeanor when done to obtain "information contained in a financial record of a financial institution . . . or contained in a file of a consumer reporting agency on a consumer").

[26] 18 U.S.C. § 1030(a)(3) (Supp. II 1985) (making such conduct a misdemeanor when done to use, modify, destroy, or disclose information in, or prevent authorized use of, a U.S. government computer, if such conduct affects the computer's operation).

This limited construction left the CADCFAA ineffectual; it was only used to prosecute one person.[27] As a result, Congress both refined and expanded the CADCFAA in 1986, with an amendment that also shortened the Act's name to the "Computer Fraud and Abuse Act."[28]

First, the 1986 amendment sharpened the CFAA's first three provisions. The amendment heightened the intent requirement of (a)(2) and (a)(3) from "knowingly" to "intentionally,"[29] to reflect the statute's purpose, and to avoid subjecting to prosecution "those who inadvertently 'stumble into' someone else's computer file or computer data."[30] The amendment also changed (a)(3) to a "simple trespass offense" that applied to anyone who accesses a Federal government computer without authorization.[31] To protect whistleblowers, however, Congress exempted Federal employees from this provision.[32] Additionally, the amendment replaced (a)(1) and (a)(2)'s wordy formulation, "having accessed a computer with authorization, us[ing] the opportunity such access provides for purposes to which such authorization does not extend," with the more concise phrase, "exceeds authorized access."[33]

The amendment also added three new provisions to the CFAA, thereby increasing its reach. The first two of these provisions involved the term "Federal interest computer," which the statute

[27] Frank P. Andreano, *The Evolution of Federal Computer Crime Policy: The Ad Hoc Approach to an Ever-Changing Problem*, 27 AM. J. CRIM. L. 81, 86 (1999).

[28] Jensen, *supra* note 20, at 88.

[29] 18 U.S.C. § 1030(a)(2)–(3) (Supp. IV 1987).

[30] S. REP. 99-432, at 5–6 (1986) (explaining that "intentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones—are precisely what the Committee intends to proscribe" and that the "knowingly" standard "might be inappropriate for cases involving computer technology . . . particularly . . . in those cases where an individual is authorized to sign onto and use a particular computer, but subsequently exceeds his authorized access by mistakenly entering another computer file").

[31] *Id.* at 7.

[32] *Id.*; Andreano, *supra* note 27, at 88 ("With regard to federal employees who were not motivated by such high ideals [as whistleblowing], Congress felt that administrative sanctions would be sufficient to deter internal misconduct.").

[33] S. REP. 99-432, at 9 (1986). The new version of the Act defined this phrase at § 1030(e)(6). *See* 18 U.S.C. § 1030(e)(6) (Supp. IV 1987) ("the term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled so to obtain or alter"); *see also* S. REP. 99-432, at 21 (1986) (noting that replacing the original language "removed from the sweep of the statute one of the murkier grounds of liability, under which a[n] . . . employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances").

defined as a computer used by a financial institution or the government, or a computer which "is one of two or more computers used in committing the offense, not all of which are located in the same State."[34] These provisions prohibited: accessing without authorization, or exceeding authorized access to, a Federal interest computer, "knowingly and with intent to defraud" ((a)(4));[35] and intentionally accessing a Federal interest computer without authorization, and thereby damaging or destroying information in it, or preventing its authorized use ((a)(5)).[36] The third new provision targeted trafficking in computer passwords ((a)(6)).[37]

Congress next amended the CFAA in 1994, when it added a civil provision at § 1030(g).[38] Congress introduced this provision in response to an increase in computer crime that outpaced the resources and attention that law enforcement agents could devote to it.[39] This remedy enabled victims harmed by § 1030 crimes to sue the perpetrators for damages, injunctive relief, and other equitable relief.[40] Congress noted that private litigation under the new provision would not only

[34] 18 U.S.C. § 1030(e)(4) (Supp. IV 1987). In 1986, because the Internet was still new and limited, few crimes would have involved Federal interest computers of the latter kind. Kerr, *supra* note 16, at 1565.

[35] 18 U.S.C. § 1030(a)(4) (Supp. IV 1987) (requiring, also, that "such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer").

[36] 18 U.S.C. § 1030(a)(5) (Supp. IV 1987) (defining damaging conduct as that which: (A) "causes loss to one or more others of a value aggregating $1,000 or more during any one-year period;" or (B) "modifies or impairs, or potentially modifies or impairs, the medical examination, medical diagnosis, medical treatment, or medical care of one or more individuals").

[37] 18 U.S.C. § 1030(a)(6) (Supp. IV 1987) (prohibiting such trafficking if it is done with intent to defraud and "affects interstate or foreign commerce" or involves a government password).

[38] Kerr, *supra* note 16, at 1565.

[39] S. REP. 101-544, at 1 (1990) ("Businesses, industry, researchers and government increasingly rely on computers. In light of rapid developments in computer technology, it is necessary to revise existing laws governing computer security and abuse to ensure that novel forms of computer abuse are prohibited."); *id.* at 8 (describing computer crime as "an area that law enforcement has sometimes been reluctant to investigate or prosecute"); *see also* Jensen, *supra* note 20, at 92 ("[T]he civil provision was a reaction to a dramatic rise in the number of computer crime cases and the government's inability to pursue all of these claims.").

[40] Kerr, *supra* note 16, at 1566; *see also* Andreano, *supra* note 27, at 96–97 (arguing that the civil provision does not adequately compensate victims or deter violators because it does not allow awarding of attorney's fees nor statutory damages).

redress otherwise unpunished wrongs, but also increase the CFAA's deterrence value without significant governmental expense.[41]

Two years later, Congress expanded the CFAA again.[42] The 1996 amendment replaced the term "Federal interest computer" with "protected computer," which it defined as any computer used by a financial institution or the government, or any computer "used in interstate or foreign commerce or communication."[43] The amendment extended § 1030(a)(2) to prohibit accessing without authorization, or exceeding authorized access to, any protected computer, through interstate or foreign communication, to obtain *any* kind of information.[44] The amendment also recognized new harms that constituted "damage" under § 1030(a)(5), [45] added a felony enhancement to § 1030(a)(2),[46] and appended a computer extortion provision at § 1030(a)(7).[47] Congress maintained that it intended the CFAA to "address[] in a single statute the problem of computer crime."[48]

[41] S. REP. 101-544, at 8 (1990) ("Deterrence is another goal"); *id.* at 11 ("S. 2476 would result in no significant cost to the federal government"). The 1994 amendment also broadened § 1030(a)(5), the computer damage statute, to hold defendants liable for harm resultant from transmissions of destructive computer programs or codes, in addition to harm resultant from unauthorized computer access. *Id.* at 5; Deborah F. Buckman, *Validity, Construction, and Application of Computer Fraud and Abuse Act*, 174 A.L.R. FED. 101, § 2[a] (2001) ("[T]he post–1994 statute broadened the proscribed range of conduct to include transmissions.").

[42] Kerr, *supra* note 16, at 1566.

[43] 18 U.S.C. § 1030(a)(2) (Supp. II 1996); *see also* Kerr, *supra* note 16, at 1568 (noting that a "'Federal interest' computer . . . required computers in two or more states, while [a 'protected computer'] merely required a machine 'used' in interstate commerce" and extrapolating that "[b]ecause every computer connected to the Internet is used in interstate commerce or communication, . . . every computer connected to the Internet is a 'protected computer'").

[44] Kerr, *supra* note 16, at 1567 ("Prior legislative history emphasized the tremendous reach of this new amendment by clarifying that obtaining information included simply reading it. . . . [Therefore,] the new § 1030(a)(2) effectively criminalized all interstate hacking.").

[45] 18 U.S.C. § 1030(a)(e)(8)(A)–(D) (Supp. II 1996) (counting as "damaging" conduct that: causes loss of more than $5,00 in any one-year period; impairs a medical diagnosis or treatment; causes "physical injury to any person"; or "threatens public health or safety").

[46] 18 U.S.C. § 1030(c)(2)(B)(i)–(iii) (Supp. II 1996) (escalating 1030(a)(2) conduct to a felony if: it was done in furtherance of any crime or tort; it was done for financial gain; or it obtained information valued at more than $5,000).

[47] 18 U.S.C. § 1030(a)(7) (Supp. II 1996).

[48] S. REP. 104-357, at 5 (1996) ("As intended when the law was originally enacted, the [CFAA] facilitates addressing in a single statute the problem of computer crime . . . . Congress must remain vigilant to ensure that the [CFAA] is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime.").

The two latest amendments to the CFAA further widened its scope.[49] Most importantly, the latter, in 2008, removed the interstate or foreign communication requirement from § 1030(a)(2),[50] and loosened the definition of "protected computer" to include computers "used in *or affecting* interstate or foreign commerce."[51] Due to the vast scope of the modern Commerce Clause,[52] this change makes every computer connected to the Internet, and arguably every computer, a "protected computer."[53]

The accumulation of these amendments has turned the CFAA into a statute that the 1984 legislature could not have fathomed. The CADCFAA criminalized a narrowly defined set of actions[54]; now, the CFAA creates criminal liability for accessing without authorization, or exceeding authorized access to, *any* computer, to obtain *any* kind of information.[55] And it creates civil liability for the same conduct if it results in the loss of at least $5,000, interference with medical care, physical injury, or a threat to public safety.[56]

[49] The first of these amendments was enacted under the U.S.A. Patriot Act of 2001, which was passed shortly after the September 11 terrorist attacks. This Act added to the class of "protected computers" those "located outside of the United States that [are] used in a manner that affects interstate or foreign commerce or communication of the United States." 18 U.S.C. §1030(e)(2)(B) (Supp. II 2004). It also made damaging any computer "used by or for a government entity in furtherance of the administration of justice, national defense, or national security" a felony under § 1030(a)(5). 18 U.S.C. §1030(a)(5) (Supp. II 2004).

[50] *See* Kerr, *supra* note 16, at 1569.

[51] 18 U.S.C. §1030(e)(2)(B). The 2008 amendment also added more harms to § 1030(a)(5). *See* Kerr, *supra* note 16, at 1569 (explaining that the amendment created misdemeanor liability for harms under $5,000, and felony liability for harming ten or more computers).

[52] *See generally* John-Michael Seibler, *Commerce Clause Just Keeps On Expanding*, WASH. TIMES (Apr. 2, 2018), https://www.washingtontimes.com/news/2018/apr/2/commerce-clause-just-keeps-on-expanding/.

[53] *See* Kerr, *supra* note 16, at 1571 ("[It] may be no exaggeration to say that a 'protected computer' now just means a 'computer.' Computers are ubiquitous as tools of modern commerce, and intrastate use of computers often has interstate effects. . . . If limits exist, . . . they likely are very narrow ones."); *see also* TJ Wong, *Is My Toaster a Computer? The Computer Fraud and Abuse Act's Definition of "Protected Computer in the Age of the Internet of Things*, J. L. & SOC. PROBLEMS (Mar. 30, 2019), http://jlsp.law.columbia.edu/2019/03/30/is-my-toaster-a-computer-the-computer-fraud-and-abuse-acts-definition-of-protected-computer-in-the-age-of-the-internet-of-things/ ("courts across the country have since interpreted 'protected computer' to encompass any computer with an internet connection").

[54] *See supra* notes 17–26 and accompanying text.

[55] *See supra* notes 51–52 and accompanying text; 18 U.S.C. § 1030(a)(2) (2019).

[56] 18 U.S.C. § 1030(g) (2019).

B. How Courts Interpret The CFAA

As the CFAA has become broader and broader, it has raised a number of unsettled legal questions.[57] One of the most ubiquitous and contentious of these questions is how to interpret the statute's "access without authorization" and "exceeds authorized access" clauses.[58] Because "millions of computer users *access* millions of computers every day," this particular question arises often in both civil and criminal suits.[59] Accordingly, the circuit split over this question provides a prime example of how courts, struggling to interpret the CFAA across civil and criminal contexts, have expanded and muddled the statute.

The first appellate decisions to address this question arose in civil cases in the First and Seventh Circuits, and broadly construed the scope of the two "access" clauses.[60] Neither of these opinions gave much consideration to the fact that the CFAA is primarily a criminal statute.[61] First, in *Ef Cultural Travel BV v. Explorica*, the First Circuit held that Explorica "exceeded authorized access" to Cultural Travel's website by using a web scraper[62] that was enhanced by confidential Cultural Travel information, even though the data scraped from Cultural Travel's website was

[57] *See, e.g.*, Paul Spellings, *On Whose Authority? Authorized Access and Criminalized Computer Use Under The CFAA*, SUNDAY SPLITS, EMORY LAW (Nov. 19, 2017), http://sundaysplits.com/2017/11/19/on-whose-authority-authorized-access-and-criminalized-computer-use-under-cfaa/ (describing a circuit split over how to interpret the CFAA's "authorized access language"); ORIN S. KERR, COMPUTER CRIME LAW 114–18 (4th ed. 2018) (describing judicial uncertainty over what constitutes "damage" under the CFAA).

[58] KERR, *supra* note 57, at 39 ("Perhaps the most complex issues raised by computer misuse statutes concern authorization. . . . Given that millions of computer users access millions of computers every day, finding the line between authorized and unauthorized access obviously is quite important.").

[59] *Id.*

[60] *See* Ef Cultural Travel BV v. Explorica, 274 F.3d 577 (1st Cir. 2001); International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006).

[61] Both the First and Ninth Circuits have acknowledged that the CFAA is "primarily a criminal statute." *See Ef Cultural Travel*, 274 F.3d at 581 n.8; LVRC Holdings LLC v. Brekka 581 F.3d 1127, 1134 (9th Cir. 2009). Presumably, this label comes from the facts that the CFAA began as a solely-criminal statute, the civil provision was added to reinforce the statute's purpose of combatting computer *crime*, and most of the statute's provisions still discuss criminal, rather than civil, liability. *See supra* notes 17–26, 38–41 and accompanying text; 18 U.S.C. § 1030 (2019).

[62] For a brief description of web scraping, *see* Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372, 373 (2018) ("Web scraping generally refers to the retrieval of content posted on the [Internet] through the use of a program other than a web browser . . . . In most cases this is done through a computer script that will send tailored queries to websites to retrieve specific pieces of content.").

public.[63] Then, in *International Airport Centers, L.L.C. v. Citrin*, the Seventh Circuit held that Citrin accessed his company laptop "without authorization" when he deleted incriminating files from it, because in doing so he breached his "duty of loyalty," and thereby "terminated his agency relationship [with his company] . . . and with it his authority to access the [company] laptop."[64] Together, these decisions established a construction of "unauthorized access" that forbids not only hacking into another's computer or its restricted files, but also *misusing* access for ends unintended by the authorizer.[65] Both decisions have had their statutory interpretations cited in subsequent criminal (and civil) cases in the First, Seventh, and other circuits.[66]

The Ninth Circuit has developed a narrower interpretation of the "access" clauses, starting with its first encounter with those clauses in *LVRC Holdings LLC v. Brekka*, another civil case.[67] Declining to follow *Citrin*'s precedent, the court in *Brekka* held that the defendant did not act "without authorization," nor did he "exceed authorization," when he emailed LVRC documents from his work computer to his personal one while he was still employed by LVRC, but was planning to quit and use the documents to start a competing company.[68] The court emphasized that the CFAA is "primarily a criminal statute," and thus the court's interpretation would control subsequent criminal, as well as civil, cases.[69] Therefore, the court followed the rule of lenity, a criminal law canon that commands courts to interpret statutes strictly and resolve ambiguities in

[63] *See Ef Cultural Travel*, 274 F.3d at 582–83.
[64] *Citrin*, 440 F.3d at 420–21.
[65] *See id.*
[66] *See, e.g.*, United States v. Phillips, 477 F.3d 215, 220 (5th Cir. 2007) (citing *EF Cultural Travel* for the proposition that "conduct is unauthorized for § 1030 purposes 'if it is not in line with reasonable expectations of the website owner and its users'").
[67] LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009).
[68] *See id.* at 1129.
[69] *See id.* at 1134–35.

favor of defendants, to prevent conviction without adequate warning.[70] This led the court to conclude that the CFAA's access clauses do not prohibit *misuse* of authorization; instead, the court held, an individual accesses a computer "without authorization" only when they have not received permission to use it, or when their permission has been explicitly revoked.[71]

But even the Ninth Circuit has left open the possibility of widespread criminal and civil liability under the CFAA. In *United States v. Nosal* ("Nosal II"), the court held that former employees of Korn/Ferry accessed the company's computers "without authorization" when, after Korn/Ferry revoked their accounts, they logged on using the credentials of their former assistant, who still worked at Korn/Ferry.[72] In dissent, Judge Reinhardt argued that this prohibition on password sharing, dictated by the company's terms, "would criminalize the ordinary conduct of millions of citizens" who consensually share, for example, Facebook passwords, in violation of Facebook's user policies.[73] This kind of omnipresent liability invites arbitrary and selective

[70] *Id.* at 1135 ("in consideration of notice, [the rule of lenity] requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government") (quoting United States v. Romm, 455 F.3d 990, 1001 (9th Cir. 2006)).

[71] *Id.* ("Nothing in the CFAA suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer."). The Ninth Circuit elaborated on *Brekka*'s holding in a subsequent criminal case: *United States v. Nosal* ("Nosal I"). United States v. Nosal, 676 F.3d 854 (9th Cir. 2012). In Nosal I, the court held that a company's employees had not accessed their company computers "without authorization," nor "exceeded their authorized access" to the computers, by downloading proprietary data from them and sending the data to an employee of a competing firm, in violation of company policy. *Id.* at 856. The court cautioned that construing the CFAA to target misuse and misappropriation of information would criminalize any violation of a private computer-use policy, and thus "transform whole categories of otherwise innocuous behavior into federal crimes," which would "invite arbitrary and discriminatory enforcement." *Id.* at 860–63 ("The government assures us that, whatever the scope of the CFAA, it won't prosecute minor violations. But we shouldn't have to live at the mercy of our local prosecutor.").

[72] United States v. Nosal, 844 F.3d 1024, 1029 (9th Cir. 2016) (reiterating the court's holding in *Brekka*: "'[A] person uses a computer "without authorization" under [the CFAA] . . . when the employer has rescinded permission to access the computer and the defendant uses the computer anyway.' This straightforward principle embodies the common sense, ordinary meaning of the 'without authorization' prohibition.") (citations omitted) (quoting *Brekka*, 581 F.3d at 1135).

[73] *Id.* at 1049–51 (Reinhardt, J., dissenting) (labelling such password sharing "ubiquitous, useful, and generally harmless"). The majority argued that the "intent to defraud" mens rea requirement of § 1030(a)(4) would limit criminal liability. *Id.* at 1032–33. But § 1030(a)(2) contains the same "without authorization" language, and no such mens rea requirement. *See* 18 U.S.C. § 1030(a)(2).

enforcement by prosecutors and private citizens alike.[74] "Broadly interpreted," Reinhardt warned, "the CFAA is a recipe for giving large corporations undue power over their rivals, their employees, and ordinary citizens, as well as affording . . . indiscriminate power to the Justice Department."[75]

As Reinhardt predicted, corporations in the Ninth Circuit have indeed brought CFAA claims against their rivals, to mixed results. In *Facebook, Inc. v. Power Ventures*, the court held that Power did not have authorization to access Facebook's profiles via automated scripts after Facebook sent Power a cease and desist letter prohibiting such conduct.[76] On the other hand, in *hiQ Labs v. LinkedIn Corp.*, the court found that hiQ likely had authorization to automate scraping of LinkedIn profiles, even after hiQ received a cease and desist letter from LinkedIn, because, unlike Facebook, LinkedIn leaves its profiles public.[77] While failing to clarify what exactly the CFAA prohibits, these cases have introduced the threat of criminal and civil liability for the type of scraping commonly undertaken in the public interest by journalists and security researchers.[78]

[74] *See* United States v. Kozminski, 487 U.S. 931, 952 (1988) (referring to the possibility of selective or arbitrary criminal enforcement); James Vorenberg, *Decent Restraint of Prosecutorial Power*, 94 HARV. L. REV. 1521, 1555 (1981) ("Giving prosecutors the power to invoke or deny punishment at their discretion raises the prospect that society's most fundamental sanctions will be imposed arbitrarily and capriciously and that the least favored members of the community – racial and ethnic minorities, social outcasts, the poor – will be treated most harshly."). Civil plaintiffs are even more likely to act based on motivations that differ from those that inspired the legislature to enact the statute. *See infra* Section II.C.3.ii.

[75] *Nosal*, 844 F.3d at 1056 (Reinhardt, J., dissenting).

[76] Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1067–68 (9th Cir. 2016) ("Power deliberately disregarded the cease and desist letter and accessed Facebook's computers without authorization to do so."); *see also id.* at 1068–69 (distinguishing Nosal I).

[77] hiQ Labs, Inc. v. LinkedIn Corp., 938 F.3d 985, 999–1003 (9th Cir. 2019) ("In sum, Nosal II and Power Ventures control situations in which authorization generally is required and has either never been given or has been revoked. As Power Ventures indicated, the two cases do not control the situation present here, in which information is 'presumptively open to all comers.'") (quoting *Power Ventures*, 844 at 1067 n.2).

[78] Trevor Collins, *9th Circuit Court of Appeals Makes CFAA Law More Confusing*, SECPLICITY (Sept. 12, 2019), https://www.secplicity.org/2019/09/12/9th-circuit-court-of-appeals-makes-cfaa-law-more-confusing/; Sellars, *supra* note 62, at 412–15.

CFAA case law remains unresolved and convoluted. The statute's scope has been expanding erratically.[79] And the Supreme Court has refused opportunities to provide clarity.[80]

C. How The CFAA Is Used In Practice

The legislature's amendments to the CFAA, and the judiciary's loose interpretations of it, have informed how the statute is used in practice. Although the legislature created the CFAA to combat hackers breaking into strangers' computers, most CFAA prosecutions and civil claims no longer involve such conduct, in large part because sophisticated hackers are often judgment proof or live beyond the reach of U.S. courts.[81] More often, CFAA cases address employment or commercial disputes that only incidentally involve computers.[82]

An empirical analysis—published by law professor Jonathan Mayer in 2016—of all CFAA cases through 2012 demonstrated that CFAA prosecutions span a much broader range of activities than those initially imagined.[83] The analysis concluded that prosecutors "routinely" press charges for "minor misconduct," such as information misappropriation.[84] It found that most criminal charges targeted one-time, technically unsophisticated misconduct.[85] And it calculated that about half of all CFAA prosecutions did not involve a defendant circumventing a technical barrier.[86]

[79] *See supra* Section I.B.

[80] *See* Nosal v. United States, 138 S. Ct. 314 (2017) (denying certiorari); Power Ventures, Inc. v. Facebook, Inc., 138 S. Ct. 313 (2017) (denying certiorari). *But see* Van Buren v. United States, 940 F.3d 1192 (11th Cir. 2019), *petition for cert. filed* (U.S. Dec. 18, 2019) (No. 19-783) (pending decision on certiorari).

[81] *See infra* notes 83–92; Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453, 1501 (2016).

[82] *See* Mayer, *supra* note 81, at 1480–85; Matwyshyn & Pell, *supra* note 15, at 557.

[83] *See* Mayer, *supra* note 81, at 1480–85. The analysis found that, as of 2013, prosecutors bring about 100 CFAA cases a year, and obtain about 90 convictions. *Id.* at 1475–86.

[84] *Id.* at 1485, 1502 (citing 51 employee information misappropriation cases, which constituted 39% of the dataset, while also noting that "[t]here is . . . a meaningful subset of prosecutions that involves serious computer abuse").

[85] *Id.* at 1484 ("[T]he majority [76 cases, which constituted 57% of the dataset] of criminal charges relate to an employment or commercial dispute. These findings squarely deflate the myth that most cybercrime defendants align with hacker archetypes (i.e., repeat offenders motivated by sport, profit, or national pride).").

[86] *Id.* (citing 65 such cases, which constituted 49% of the data set, and adding that "among those cases that do involve a circumvention of a technological protection, many of the fact patterns do not reflect technical sophistication but rather password theft").

The same 2016 analysis, and an analysis of all civil CFAA filings in 2018—published by law professors Andrea M. Matwyshyn and Stephanie K. Pell—revealed that civil CFAA claims are even less likely to involve the type of hacking that inspired Congress to create the statute. The 2016 analysis observed that the volume of civil CFAA cases "exploded" between 2002 and 2012, such that civil cases now make up the majority of CFAA cases.[87] It determined that an "overwhelming majority" of civil CFAA actions stemmed from business disputes that "look nothing like 'hacking,' even construed broadly."[88] It also found that civil CFAA claims are usually redundant with conventional contract or business tort claims.[89] Similarly, the 2018 analysis found that a majority of civil CFAA claims in 2018 comprised "companies suing employees, contractors, or competitors, or business partners suing each other."[90] Additionally, the 2018 analysis noted that, in a majority of these competition-related cases, the CFAA claim was nonviable and dismissed or dismissed without prejudice.[91] The viable CFAA claims had alternative means of redress "in almost all cases."[92]

In sum, the CFAA has expanded well beyond the narrow statute that Congress intended to target criminal computer hacking.[93] Some courts have interpreted the statute's vague language so

[87] *Id.* at 1472, 1501; *see also id.* at 1476 ("[T]he [more modest] surge in criminal litigation predated the surge in civil litigation by about a decade . . . [which] suggests that prosecutors initially paved the way for broad applicability of cybercrime law, and civil litigants only later took advantage."); *id.* at 1473 (noting that, as of 2013, courts issue about 150 written opinions in civil CFAA cases a year).

[88] *Id.* at 1481 (citing 238 cases that arose from business disputes, which constituted 73% of the data set, and adding that most of these "follow from previous employment" and only "a small minority . . . are filed against strangers").

[89] *Id.* at 1490 ("This result is consistent with the theory that courts have adapted conventional tort and property claims to technology, making dedicated, computer-specific causes of action less necessary. The leading civil coclaims also reinforce the conclusion that civil cybercrime mediates commercial grievances, not sophisticated computer intrusions.").

[90] Matwyshyn & Pell, *supra* note 15, at 557.

[91] *Id.* This affirms that courts do (at least somewhat) limit the civil provision's scope. But it also suggests that private parties view the CFAA as a wide-ranging catchall cause of action, and that these parties will continue to pressure the courts to interpret it accordingly.

[92] *Id.*

[93] *See supra* Section I.A.

broadly that prosecutors could charge almost anyone with a federal criminal violation of the CFAA.[94] This invites arbitrary and discriminatory enforcement, diminishes citizens' trust in the justice system, and discourages online innovation and participation.[95] Furthermore, civil plaintiffs have taken advantage of broad interpretations of the CFAA to file frivolous and redundant claims, which stifle competition, increase wealth concentration, and disempower employees.[96]

II. THE CFAA'S HYBRID STRUCTURE

This Part examines how and why the CFAA's hybrid structure contributed to its devolution into the unstable and overbroad statute that exists today. Section II.A provides a short introduction to hybrid statutes. Section II.B identifies what courts and prosecutors have already done to account for the CFAA's hybrid structure and guard against inflation. Section II.C analyzes why, despite the safeguards of Section II.B, the CFAA remains particularly vulnerable to the dangers posed by hybrid construction, and explains how the CFAA's hybrid construction has precipitated overexpansion on both its criminal and civil sides.

A. Hybrid Statutes

1. Bridging The Criminal/Civil Divide

Criminal law and civil law have distinct goals, forms of punishment, burdens of proof, procedural rules, and modes of interpretation.[97] Criminal statutes address wrongs that harm the public as a whole.[98] They bring moral condemnation, and with it, a punishment that often includes

[94] *See supra* Section I.B.

[95] *See supra* notes 6–11, 72–75 and accompanying text.

[96] *See supra* notes 12–14, 87–92 and accompanying text.

[97] *See* Mary M. Cheh, *Constitutional Limits on Using Civil Remedies to Achieve Criminal Law Objectives: Understanding and Transcending the Criminal-Civil Law Distinction*, 42 HASTINGS L.J. 1325, 1325–27 (1991) ("The Constitution, statutes, and the common law all draw fundamental distinctions between criminal proceedings . . . and civil proceedings.").

[98] Henry M. Hart, Jr., *The Aims of the Criminal Law*, 23 L. & CONTEMP. PROBS., 401, 404–05 (1958) ("The commands of the criminal law are commands which the public interest requires people to comply with."); Kenneth W. Simons, *The Crime/Tort Distinction: Legal Doctrine and Normative Perspectives*, 17 WIDENER L.J. 719, 720 (2008) ("criminal law prohibits 'public' wrongs and tort law 'private' wrongs").

imprisonment.[99] Because of these high stakes, prosecutors must meet a high burden of proof to secure a criminal conviction, and courts afford criminal defendants many procedural safeguards, such as the right to counsel.[100] Furthermore, courts interpret criminal statutes narrowly, in order to protect defendants' due process rights.[101]

In contrast, civil law generally facilitates the redress of private injuries that do not substantially impact the wider community's interest.[102] The burden of proof is lower, parties have fewer procedural protections, and courts can order only monetary or injunctive relief, not prison sentences.[103] Courts interpret civil statutes more liberally, to promote remediation.[104]

The distinction between criminal law and civil law is imperfect, and subject to debate, but it is also widely recognized.[105] By providing for both criminal and civil enforcement, hybrid statutes bridge this distinction.[106] Hybrid statutes are fairly common, and most of them are

[99] Pamela H. Bucy, *Moral Messengers: Delegating Prosecutorial Power*, 59 SMU L. REV. 321, 342 (2006) ("'Guilty' . . . communicates that citizens have determined that a defendant . . . deserves the community's condemnation. . . . Convicted defendants go to prison. Their assets are forfeited. They suffer public scorn, . . . emotional pain, [etc.]."); Hart, *supra* note 98, at 404–05.

[100] Cheh, *supra* note 97, at 1329 (enumerating some of the "rigorous constitutional protections associated with criminal trials, such as proof beyond a reasonable doubt, trial by jury, and appointment of counsel").

[101] Lawrence M. Solan, *Statutory Inflation and Institutional Choice*, 44 WM. & MARY L. REV. 2209, 2212 (2003).

[102] Thaw, *supra* note 19, at 934–35 ("Private liability established under tort or contract law generally concerns circumstances under which one individual's actions cause redressable harm to another. . . . Neither [tort nor contract law] . . . focuses on the general prevention of socially undesirable activities or activities for which compensation cannot be provided."). This is the general, traditional distinction between criminal and civil law; but it is far from absolute. For example, in practice, torts often allow private citizens to redress public wrongs. *See, e.g.*, Benjamin C. Zipursky, *Torts as Wrongs*, 88 TEX. L. REV. 917, 918 (2010) (conceding that, "[o]f course, tort law is in many ways public"); John C.P. Goldberg, *The Constitutional Status of Tort Law: Due Process and the Right to a Law for the Redress of Wrongs*, 115 YALE L.J. 524, 530 (2005) (noting the tendency of many "modern scholars to treat tort law as an instrument for attaining *public* goals such as loss-spreading or efficient precaution-taking" (emphasis added)).

[103] Simons, supra note 98, at 719–25 (cataloguing the differences between criminal law and tort law).

[104] Solan, *supra* note 101, at 2212.

[105] *See generally* Simons, *supra* note 98 (listing all of the similarities and differences between the doctrine, structure, and normative perspectives of criminal law and civil law); Jerome Hall, *Interrelations of Criminal Law and Torts*, 43 COLUM. L. REV. 753 (1943) (discussing the distinctions between criminal law and tort drawn by a variety of legal philosophers, including Blackstone, Bentham, Austin, and Holmes).

[106] *See* Stephen Wills Murphy, *The Rule of Lenity and Hybrid Statutes:* WEC Carolina Energy Solutions LLC v. Miller, 64 S.C. L. REV. 1129, 1130 (2013) ("The typical 'hybrid' scheme is as follows: Section One prohibits certain conduct; Section Two creates a private cause for damages for such conduct; and Section Three makes a particular subclass of conduct—such as a willful or knowing violation—a crime."). The Supreme Court upheld the constitutionality of hybrid statutes in 1895. *See In re* Debs, 158 U.S. 564, 599 (1895).

enforced primarily through their civil provisions[107]; but others, like the CFAA, are primarily enforced through their criminal provisions.[108] Typically, legislatures construct hybrid statutes to effect maximum deterrence.[109] Indeed, this goal inspired the addition of the civil provision to the CFAA in 1994: the legislature believed that providing for civil suits would deter the criminal conduct that the statute was created to combat.[110]

But the differences between criminal and civil causes of action raise difficult interpretative questions[111]: Should hybrid statutes have one uniform interpretation, or separate interpretations in the alternate realms? Should courts consider a statute's hybrid structure when interpreting it? And how, if at all, should courts distinguish cases brought by the government from cases brought by private citizens? The answers to these questions can determine the outcome of both criminal and civil cases. Without focusing specifically on the CFAA, scholars have offered guidance for the courts, and framed the problems that hybrid statutes can generate.[112]

2. Interpreting Hybrid Statutes

Law professor Margaret Sachs articulated a "core principle" for interpreting hybrid statutes: courts should limit a statutory provision to one, consistent interpretation.[113] She offered

[107] Murphy, *supra* note 106, at 1130 (noting that "examples [of hybrid statutes primarily enforced through civil actions] include the Sherman Act, . . . the Bankruptcy Code, and . . . the Clean Water Act").

[108] *Id.*

[109] Judge Jed S. Rakoff, Speech at Conference on Corporate Crime and Financial Misdealing at New York University Law School (Apr. 17, 2015) ("The central idea behind . . . hybrid statutes is to provide maximum deterrence for the misconduct in question by making it subject to every weapon the legal system can bring to bear."); *see generally* Zachary D. Clopton, *Redundant Public-Private Enforcement*, 69 VAND. L. REV. 285 (2016) (discussing the possible benefits of redundant public-private enforcement, and analyzing how to order public and private claims to reduce excess costs and maximize intended effects).

[110] *See supra* notes 38–41 and accompanying text.

[111] *See, e.g.*, Rakoff, *supra* note 109 (asserting that the creation of hybrid statutes "has created more problems than it has solved," and that "[i]t is time to eliminate hybrid statutes and restore the legitimate distinction between the civil and criminal law").

[112] See *infra* Section II.A.2.

[113] Margaret V. Sachs, *Harmonizing Civil and Criminal Enforcement of Federal Regulatory Statutes: The Case of the Securities Exchange Act of 1934*, 2001 U. ILL. L. REV. 1025, 1029 (2001).

four reasons for this directive.[114] First, it respects Congressional intent.[115] Second, it accounts for the fact that some hybrid statutes have separate intent requirements for criminal enforcement.[116] Third, it follows from the convention that language repeated in a statute has a single meaning that language appearing only once has a single meaning too.[117] Fourth, it avoids the unstable alternative of creating multiple constructions out of a single text and legislative history.[118] For these reasons, among others, courts generally abide by the core principle.[119]

Sachs also recommended that courts follow three rules when interpreting hybrid statutes in accordance with the core principle.[120] The All Contexts Rule directs a court interpreting a hybrid statute in a criminal case to consider how its interpretation will apply in future civil cases, and vice versa.[121] The Default Fair Warning Rule directs courts to apply the rule of lenity to civil cases[122]; but the Alternative Fair Warning Rule provides that courts can abandon strict construction, without raising warning concerns, when a hybrid statute has a criminal intent requirement that precludes

[114] *Id.* at 1031–33.

[115] *Id.* at 1031–32 (observing that, if Congress wanted to enact different provisions, it could have done so explicitly).

[116] *Id.* at 1032 (explaining that, "[b]y singling out intent as the distinctive feature of criminal actions, Congress implies that the prohibitions are otherwise identical").

[117] *Id.* (noting that the presumption that "language appearing repeatedly in a statute has one meaning throughout" is "'virtually impossible' to rebut when the language is repeated within . . . a single sentence" (citing Brown v. Gardner, 513 U.S. 115, 118 (1994))).

[118] *Id.* (explaining that multiple constructions of a hybrid statute share "origination points," which "may propel the constructions toward convergence," and cautioning that "preserving the distinctiveness of a prohibition's multiple-constructions may prove more difficult than it first appears").

[119] Solan, *supra* note 101, at 2218 ("Courts . . . do not impose two separate interpretations on the same words, depending on whether the case is civil or criminal."); *see also* Leocal v. Aschcroft, 543 U.S. 1, 11 n.8 (2004) (holding—in a civil case involving a statute with "criminal and noncriminal applications"—that "because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies").

[120] *See* Sachs, *supra* note 113, at 1033–40.

[121] *Id.* at 1033–34 (explaining that the All Contexts Rule's import "becomes apparent upon considering what would happen if courts rejected it while at the same time accepting the core principle. Under these circumstances, a prohibition's meaning would be determined by the nature of the lawsuit that addressed it first, thereby precipitating a race to the courthouse door.").

[122] *Id.* at 1035–36 ("[b]y mandating strict construction, the rule strips courts of the flexibility to interpret ambiguities in accordance with the policies that prompted the hybrid statute's enactment"); *see also* Solan, *supra* note 101, at 2224 ("The primary justifications for the rule [of lenity] are fair notice to defendants and separation of powers.").

prosecution unless the defendant had "either knowledge of illegality or knowledge of wrongfulness sufficient to make illegality likely."[123] Finally, the Differentiated Intent Rule instructs courts to enforce *any* heightened criminal intent requirement, and thus bolsters Congressional attempts to reduce criminalization of minor misconduct.[124] The core principle, and these complementary rules, can guide courts toward a consistent mode of interpreting hybrid statutes that maintains judicial order, respects legislative intent, and provides clarity and predictability for citizens.

Shortly after Sachs published these prescriptions, law professor Lawrence Solan published a descriptive account of the different ways that courts can and actually do interpret hybrid statutes.[125] Solan identified four approaches: the Inflationary Model; the Lenity Model; the Standard Model; and the Law Enforcement Model.[126]

Only the first two of these approaches comply with Sachs' core principle. In the Inflationary Model, courts interpret statutes broadly in both criminal and civil cases.[127] This approach allows courts to combat harmful conduct aggressively, even in an ever-changing society.[128] But it also carries the greatest risk of over-inflation, wherein a statute becomes so broad, usually through civil-case interpretations, that it creates criminal liability for innocuous conduct that the legislature did not intend to criminalize.[129] On the civil side, overbroad interpretations can

[123] Sachs, *supra* note 113, at 1037–38 ("[a] criminal intent requirement . . . would render strict construction inapposite and thereby preserve the flexible judicial interpretation that the Court believed Congress wanted").

[124] *Id.* at 1038–39.

[125] *See* Solan, *supra* note 101.

[126] *See id.* at 2218–60.

[127] *Id.* at 2237–51 (discussing securities laws, antitrust laws, and environmental laws as examples of statutes that courts tend to interpret using this model).

[128] *Id.* at 2251.

[129] *Id.* at 2213. A criminal-specific mens rea requirement can limit the expansion of criminal liability. *See supra* note 123 and accompanying text. And prosecutorial discretion can limit the practical effect of this expansion, if not the looming threat of *possible* prosecution. *But see* Solan, *supra* note 101, at 2214; United States v. Nosal, 676 F.3d 854, 862–63 (9th Cir. 2012) ("[W]e shouldn't have to live at the mercy of our local prosecutor. . . . And it's not clear we *can* trust the government when a tempting target comes along."); McDonnell v. United States, 136 S. Ct. 2355, 2372–73 (2016) ("we cannot construe a criminal statute on the assumption that the Government will 'use it responsibly'" (citing United States v. Stevens, 559 U.S. 460, 480 (2010))).

inundate courts with frivolous suits, including anti-competitive actions designed to scare or overwhelm rivals, and overzealous good-faith claims that no government agent would pursue.[130]

The Lenity Model espouses the opposite approach: narrow construction in both criminal and civil cases.[131] This approach, which conforms to Sachs' Default Fair Warning Rule, presents less risk of overbreadth than the Inflationary Model does.[132] The tradeoff is that it also restricts a statute's ability to redress and deter misconduct, particularly in civil cases, which traditionally allow for broader interpretation to promote remediation.[133]

Solan's last two models run afoul of the core principle, and therefore rarely gain traction in practice.[134] In the Standard Model, courts simply maintain the default canons of interpretation: they construe hybrid statutes narrowly in criminal cases and broadly in civil cases.[135] Because courts observe stare decisis, this model results in path-dependence: the type of case in which courts first interpret the hybrid statute determines its breadth in future cases.[136]

Lastly, the Law Enforcement Model envisions broad statutory constructions in criminal cases and narrow constructions in civil cases.[137] Courts rarely, if ever, interpret individual language in this way.[138] However, courts have followed the general spirit of the Law Enforcement

[130] Sachs, *supra* note 113, at 1029 (noting that implied private rights of action, at least, "elicit considerable judicial antipathy because they are perceived as vexatious"); Blue Chip Stamps v. Manor Drug Stores, 421 U.S. 723, 742–43 (1975) (explaining that, in securities litigation, "the mere existence of an unresolved lawsuit has settlement value to the plaintiff not only because of the possibility that he may prevail on the merits . . . but [also] because of the threat of extensive discovery and disruption of normal business activities").

[131] Solan, *supra* note 101, at 2251–52.

[132] *Id.*

[133] *See supra* notes 102–105 and accompanying text; *see also* Jonathan Marx, Note, *How to Construe a Hybrid Statute*, 93 VA. L. REV. 235, 260–61 (2007) (describing a potential problem with narrowly interpreting civil provisions of hybrid statutes: "if the legislature passed a statute creating a private remedy addressing certain wrongs or 'mischief,' it viewed that mischief as inadequately remedied under prior law, and the statute should not be interpreted so stingily as to gut the intended new remedy").

[134] *See* Solan, *supra* note 101, at 2218–37, 2255–60.

[135] *Id.* at 2218.

[136] *Id.* at 2218, 2237–38 (stating that most often this scenario leads to a broad interpretation in both contexts, and so the Standard Model, in practice, turns into the Inflationary Model); *see also* Marx, *supra* note 133, at 236.

[137] *See* Solan, *supra* note 101, at 2255–60.

[138] *Id.* at 2255 ("I have found no instances in which a court interprets the same language broadly in criminal cases, and more narrowly in civil ones.").

Model in their treatment of the Racketeer Influenced and Corrupt Organizations Act ("RICO"), a primarily-criminal statute.[139] Courts have allowed broad constructions of RICO provisions used by prosecutors, while enforcing narrower constructions of RICO's civil standing provisions (which do not apply to criminal prosecutions) and other provisions used mostly by civil plaintiffs.[140] This practice gives prosecutors leeway to use their discretion to realize RICO's purpose, while also (theoretically) restraining private parties—who are unaccountable to the public and usually motivated by their own financial gain rather than a broader goal of eliminating racketeering—from co-opting a broad interpretation of RICO's language for their own ends.[141]

When tasked with interpreting a hybrid statute, courts must choose between these four models. Courts need to decide whether to abandon the core principle's guidance, or to heed it and risk either uncontrollable statutory inflation or inadequate redressal of civil wrongs. Solan found that most courts make this decision based on their perception of the legislature's intent.[142]

[139] *Id.* (citing Religious Tech. Ctr. v. Wollersheim, 796 F.2d 1076, 1084-87 (9th Cir. 1986)).

[140] *Id.*

[141] *Id.* at 2255–60. Despite these interpretive maneuvers, RICO's civil provision has expanded well beyond the legislature's intent. The legislature enacted RICO primarily to fight organized crime, and phrased the statute broadly because it expected prosecutors to choose cases based on that stated purpose. (To reinforce that end, the Justice Department adopted formal prosecution guidelines, which include "careful monitoring and centralized control," to prevent overzealous prosecutions.) The legislature also added a provision for private civil suits, with the intent that these would further deter organized crime. But because of the statute's broad, ambiguous language, and the civil provision's inclusion of treble damages and attorneys' fees for victorious plaintiffs, civil plaintiffs began bringing RICO claims in all sorts of commercial disputes involving legitimate businesses and no organized crime issues. In fact, the statute's civil provision has had the exact opposite effect of its intended purpose. Most private plaintiffs would not dare sue a powerful criminal organization. Still, the statute's harsh damages regime allows these private plaintiffs to themselves extort civil defendants, who settle to avoid outsized penalties and any association with a court case branding them as criminals. *See* Philip A. Lacovara & Geoffrey F. Aronow, *The Legal Shakedown of Legitimate Business People: The Runaway Provisions of Private Civil RICO*, 21 NEW ENG. L. REV. 1, 1 (1985); DANIEL C. RICHMAN, KATE STITH, & WILLIAM J. STUNTZ, DEFINING FEDERAL CRIMES 511 (2d ed. 2018).

[142] *See* Solan, *supra* note 101, at 2223 ("Even when it is not mentioned, courts routinely state that their goal is to interpret the statute in such a way as to carry out the will of the legislature."). In his student Note, Jonathan Marx recommended that courts also consider how a statute is actually enforced. Marx suggests that courts interpret narrowly statutes enforced mostly through their criminal provisions, and interpret broadly statutes enforced mostly through their civil provisions. *See* Marx, *supra* note 133, at 281–82. Of course, neither Solan's nor Marx's approach will always generate a clear answer. Some hybrid statutes were passed for a mix of remedial and penal purposes, and spawn a roughly equal amount of criminal and civil cases. Marx advised that courts interpret these statutes as "evenhandedly as possible," with an emphasis on consistency, and a focus on the statute's plain meaning. *Id.* at 282–86.

B. How Courts And Prosecutors Already Account For the CFAA's Hybrid Structure

Those interpreting and enforcing the CFAA have already resisted its over-inflation in at least two ways: by embracing the Lenity Model,[143] and by creating a Charging Policy that discourages prosecutors from bringing CFAA charges for computer crimes of little federal relevance.[144]

1. Applying The Lenity Model

Recognizing the importance of the core principle, and that the CFAA is primarily a criminal statute, many circuit courts have explicitly invoked the rule of lenity when interpreting the CFAA, even in civil cases. For example, in the first Ninth Circuit case to interpret the phrase "without authorization," the court emphasized that "[f]irst, and most important, § 1030 is primarily a criminal statute," and thus the court's interpretation in its present civil case would be "equally applicable in the criminal context."[145] Therefore, the court resolved to follow the "well established" principle that "ambiguity concerning the ambit of criminal statutes should be resolved in favor of lenity."[146] In so doing, the Ninth Circuit rejected the Seventh Circuit's expansive interpretation of "without authorization" because it did not "comport with the plain language of the [statute]."[147]

[143] *See infra* Section II.B.1.

[144] See *infra* Section II.B.2.

[145] LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134 (9th Cir. 2009) (citing Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004)).

[146] *Id.* (citing United States v. Carr, 513 F.3d 1164, 1168 (9th Cir. 2008) (quoting Rewis v. United States, 401 U.S. 808, 812 (1971))).

[147] *Id.* (holding that an individual using a computer that they are authorized to use for an unauthorized purpose is not accessing the computer without authorization). Other circuits have also employed the Lenity Model in their interpretations of the CFAA. *See, e.g.*, WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 204 (4th Cir. 2012); Murphy, *supra* note 106, at 1129 (praising the Fourth Circuit's use of the Lenity Model); United States v. Valle, 807 F.3d 508, 526–28 (2d Cir. 2015) ("[C]ourts that have adopted the broader construction 'looked only at the culpable behavior of the defendants before them, and failed to consider the effect on millions of ordinary citizens caused by the statute's unitary definition of "exceeds authorized access."'" (quoting United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012))).

If the court had not considered this phrase's importance to future criminal cases, it might have facilitated a major CFAA expansion by interpreting the language broadly in an effort to redress a minor civil wrong and to avoid upsetting inter-circuit precedent.[148] Instead, the court asserted that the rule of lenity, a well-established tenet of criminal law,[149] should also apply to hybrid statutes, to protect future criminal defendants from prosecutions based on ambiguous statutory language.[150] This limits anti-competitive civil misuse of the CFAA too.[151]

2. Promoting Prosecutorial Discretion

The DOJ has also taken a step toward taming the statute's overbreadth by providing CFAA enforcement guidelines for prosecutors. Prosecutors are particularly likely to consult the DOJ when working on CFAA cases, because the DOJ's Computer Crime and Intellectual Property Section ("CCIPS") offers a wealth of technical expertise that is uncommon amongst lawyers.[152] The Office of the Attorney General's 2014 "Intake and Charging Policy for Computer Crime Matters" advises United States Attorneys that they should prosecute CFAA violations only when "a substantial federal interest would be served by prosecution" and the available, admissible evidence is likely "sufficient to sustain a conviction."[153]

[148] *See infra* Section II.C.2.

[149] *See, e.g.*, United States v. Bass, 404 U.S. 336, 347–48 (1971) (noting that the rule of lenity stems from fair warning concerns and a reluctance to impose harsh punishments).

[150] Warren Thomas, Note, *Lenity on Me: LVRC Holdings LLC v. Brekka Points the Way Toward Defining Authorization and Solving the Split Over the Computer Fraud and Abuse* Act, 27 GA. ST. U. L. REV. 379, 407–08 (2011) (noting that "[t]he narrow interpretation of without authorization limits the overuse of the CFAA in criminal prosecutions and inappropriate use of the federal courts as a preferred forum for trade secret litigation").

[151] *See infra* Section II.C.3.ii (describing how civil plaintiffs take advantage of broad interpretations of the CFAA).

[152] *See infra* Section II.C.3.i.

[153] Memorandum from The Attorney General to The United States Attorneys and Assistant Attorney Generals for the Criminal and National Security Divisions on Intake and Charging Policy for Computer Crime Matters 1 (Sept. 11, 2014), https://www.justice.gov/criminal-ccips/file/904941/download [hereinafter "CCIPS Memorandum"]. The Department of Justice website uploaded the memorandum and a press release in 2016, shortly after the government submitted the memorandum as evidence of prosecutorial restraint in a case brought by the ACLU that challenged the CFAA on First Amendment grounds. *See* Press Release, Assistant Attorney General Leslie R. Caldwell, Criminal Division, Department of Justice, Department Releases Intake and Charging Policy for Computer Crime Matters (Oct. 25, 2016), https://www.justice.gov/archives/opa/blog/department-releases-intake-and-charging-policy-computer-crime-matters. The ACLU's case is ongoing. *See* Sandvig v. Barr, No. 1:16-cv-01368 (D.D.C. filed June 29, 2016);

The Policy recommends that prosecutors weigh a variety of considerations when deciding whether a substantial federal interest is at stake: the sensitivity of the affected computers and the information stored therein; the degree to which the violation implicates national security, public health, or critical infrastructure concerns; the harm suffered by victim(s); whether the violation was in furtherance of a larger criminal scheme; and whether "any other jurisdiction is likely to prosecute the conduct effectively."[154] The Policy also provides that U.S. Attorneys should only prosecute "exceeds-authorized-access violation[s]" when "the defendant *knowingly* violated restrictions on his authority to obtain or alter information stored on a computer."[155] And it cautions that "prosecution may not be warranted" if the "defendant exceeded authorized access solely by violating an access restriction contained in a contractual agreement or term of service with an Internet service provider or website."[156] These guidelines imply that the DOJ does not intend to argue for the criminalization of innocuous CFAA violations, no matter how broadly a court interprets the CFAA in civil (or criminal) case precedent. Therefore, they are a step in the right direction.[157]

see also Challenge to CFAA Prohibition on Uncovering Racial Discrimination Online, ACLU (last updated May 22, 2019), https://www.aclu.org/cases/sandvig-v-barr-challenge-cfaa-prohibition-uncovering-racial-discrimination-online (providing case updates).

[154] CCIPS Memorandum, *supra* note 153, at 1–2.

[155] *Id.* at 4 (emphasis added).

[156] *Id.* at 4–5 (explaining that prosecution of unauthorized or excessive access violations is more likely to serve a substantial public interest if the defendant abused a position of trust, or if the conduct threatened national or economic interests).

[157] Still, the Policy does have shortcomings. It is not binding on prosecutors, and it does not "create a right or benefit . . . enforceable at law by a party to litigation with the United States." *Id.* at 2. It also suggests that "advancements in technology generally weigh in favor of more federal prosecutions—and more serious prosecutions." *See* Jamie Williams, *New Federal Guidelines For Computer Crime Law Do Nothing To Reign In Prosecutorial Overreach Under Notoriously Vague Statute*, ELECTRONIC FRONTIER FOUNDATION (Oct. 31, 2016), https://www.eff.org/deeplinks/2016/10/what-were-scared-about-halloween-prosecutorial-discretion-under-notoriously-vague. Furthermore, U.S. Attorneys could use the Policy's emphasis on the "deterrent value" of CFAA prosecutions to justify especially aggressive enforcement against defendants whose cases involve the use of a new technology—to "make an example" out of them. *See id.*; CCIPS Memorandum, *supra* note 153, at 2 (listing deterrence as a factor for CFAA charging decisions, including considerations of: "whether the need for deterrence is increased because the activity involves a new or expanding area of criminal activity, a recidivist defendant, use of a novel or sophisticated technique, or abuse of a position of trust or . . . because the conduct is particularly egregious"). Also, the DOJ has argued for the expansion of the CFAA in other instances. *See, e.g.*, King & Spalding, *DOJ Asks Senate*

C. How The CFAA's Hybrid Structure Contributes To Its Overbreadth

Despite these attempts at limiting the CFAA's scope, the CFAA's hybrid structure continues to advance its overexpansion. There are a few, compounding reasons for this. First, the CFAA's drafters neglected to differentiate the statute's criminal and civil components.[158] Second, some courts have failed to apply the Lenity Model.[159] And third, the statute's evolving, technical subject matter destabilizes its position in society.[160]

1. The CFAA's Overlapping Criminal And Civil Provisions

Although Congress added a civil provision to the CFAA to increase its ability to combat computer crime, rather than to change its primary character,[161] Congress has done little to confine this new provision's influence on the statute's development as a whole.[162] The civil addition provides that "[a]ny person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator," as long as the conduct involves one of a set of four factors.[163] Three of these factors target conduct that interferes with medical care, causes physical injury, or threatens public safety.[164] The last of these factors[165]—"loss to 1 or more persons during any 1-year period . . . aggregating at least $5,000 in value"—has been interpreted so broadly,[166] and manipulated by civil plaintiffs so thoroughly,[167] that nearly any victim of a crime that falls

to Reform CFAA to Help Deter Insider Threats, JD SUPRA (Aug. 29, 2018), https://www.jdsupra.com/legalnews/doj-asks-senate-to-reform-cfaa-to-help-34028/.

158 *See infra* Section II.C.1.

159 *See infra* Section II.C.2.

160 *See infra* Section II.C.3.

161 *See supra* notes 38–41 and accompanying text.

162 *See infra* Section II.C.1.

163 18 U.S.C. § 1030(c)(4)(A)(i)(I)–(V) (2019).

164 *Id.*

165 *Id.*

166 KERR, *supra* note 57, at 127–29 (detailing how the CFAA's definition of loss "is quite broad"); Ekeland, *supra* note 6 ("[C]osts associated with 'loss' include those incurred to investigate and restore a system, and those incurred from any interruption of service. . . . [T]he murkiness of the definition invites Enron-style accounting.").

167 KERR, *supra* note 57, at 79, 117.

under the CFAA can bring a civil action.[168] The civil provision adopts the language of the CFAA, which the legislature drafted solely for criminal use, without including any significant restrictions to account for courts' tendencies to interpret statutes more broadly in civil cases and civil litigants' disinclination to exercise the same discretion as prosecutors.[169]

Nor does the CFAA insulate its primary, criminal application from its secondary, civil application. The statute does not include any heightened criminal-specific intent requirement,[170] and therefore any conduct found to be a civil violation of the CFAA also becomes a criminal violation.[171] This means that the statute is at a high risk of criminal over-inflation, unless courts follow the Default Fair Warning Rule and apply the Lenity Model.[172]

2. The Limits Of Lenity

But some circuits have not applied the Lenity Model and instead largely ignored the CFAA's hybrid structure.[173] This is not unusual; federal judges often ignore the rule of lenity because they trust their own interpretations and rarely view statutes as ambiguous enough to trigger the rule.[174] If these judges first interpret the CFAA in a civil case, then a broad construction of the

[168] In contrast, RICO puts a somewhat more meaningful restraint on its secondary civil provision by qualifying that: "no person may rely upon any conduct that would have been actionable as fraud in the purchase or sale of securities to establish a violation of section 1962." 18 U.S.C. § 1964(c). While civil RICO has still over-expanded, this limitation does have some effect. *See supra* note 141 (describing the expansion of civil RICO); Peter J. Henning, *RICO Lawsuits Are Tempting, But Tread Lightly*, N.Y. TIMES (Jan. 16, 2018), https://www.nytimes.com/2018/01/16/business/dealbook/harvey-weinstein-rico.html ("[I]f the alleged violations involve securities fraud, they cannot survive a motion to dismiss even if they could constitute mail or wire fraud.").

[169] *See supra* Section II.A.1 (outlining the ways in which civil remedies differ from criminal remedies).

[170] For a counterexample, the Copyright Act establishes civil liability for copyright infringement, but specifies that criminal liability will only attach if the infringement is *willful*. *See* 17 U.S.C. § 506 (2019).

[171] Sometimes courts will read a criminal-specific mens rea requirement into a hybrid statute even if the statute's language does not contain one. *See, e.g.*, United States v. U.S. Gypsum Co., 438 U.S. 422, 435–43 (1978) (construing the Sherman Act to require "knowledge of probable consequences"). But "courts have interpreted the CFAA's mens rea element to be nearly tautological[:] . . . it fails to separate the intent to commit the act that constitutes or results in unauthorized access from the intent actually to disregard authorization or access restrictions." Thaw, *supra* note 19, at 945.

[172] *See supra* notes 122–123 and accompanying text.

[173] *See supra* notes 60–66 and accompanying text.

[174] RICHMAN, STITH, & STUNTZ, *supra* note 141, at 88 (explaining that federal courts often ignore the rule of lenity because "[t]he rule matters only when judges conclude both (1) that all things considered, the government's

language will dictate future civil and criminal cases alike.[175] In *Ef Cultural Travel*, a civil case, the First Circuit did not even mention the rule of lenity, and only briefly noted that the CFAA has a criminal provision.[176] This led the court to interpret the CFAA's language broadly.[177] Five years later, the Seventh Circuit cited and built upon *Ef Cultural Travel*'s holding in *Citrin*, another civil case, and the first case to interpret "exceeds authorized access" in its circuit.[178] Again, the court did not invoke the rule of lenity, and again, the court interpreted the language broadly.[179] Together, these two early cases set a strong precedent that remains in the First and Seventh Circuits, and that has infiltrated some other circuits, even when those circuits first interpret the language in criminal cases.[180]

And even when courts purport to follow it, the rule of lenity has limits: it cannot negate every difference between criminal and civil litigation.[181] Inescapably, these realms have different

interpretation is at least as good as the defendant's, and (2) that the case is close enough to trigger the rule" and "[t]hose conclusions sit uncomfortably together").

[175] *See supra* notes 135–136 and accompanying text.

[176] In fact, the word "criminal" only appears in the opinion three times. *See* Ef Cultural Travel BV v. Explorica, 274 F.3d 577, 580 (1st. Cir. 2001) ("[T]he district court granted a preliminary injunction against Explorica based on the CFAA, which criminally and civilly prohibits certain access to computers."); *id*. at 584 (claiming that "[i]f the loss to the victim meets the required monetary threshold, the conduct should be criminal, and the victim should be entitled to relief" (quoting S. Rep. No. 104-357, at 11 (1996))); *id.* at 581 n.8 (acknowledging that "[a]lthough the CFAA is primarily a criminal statute, under § 1030(g), any person who suffers damage or loss . . . may maintain a civil action . . . for compensatory damages and injunctive relief or other equitable relief").

[177] *See id.* at 583 (holding that a defendant exceeds authorized access to information when he or she abuses a privacy policy protecting that information).

[178] *See* International Airport Centers, L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006).

[179] *See id.* In its discussion of the CFAA's transmission provision, the court at least hesitated to "stretch[] the statute too far . . . especially since it provides criminal as well as civil sanctions for its violation." *Id.* at 419. This was the opinion's sole mention of the CFAA's criminal character.

[180] *See, e.g.*, United States v. Phillips, 477 F.3d 215, 220 (5th Cir. 2007) (citing *EF Cultural Travel* for the proposition that "conduct is unauthorized for § 1030 purposes 'if it is not in line with reasonable expectations of the website owner and its users'"). Other circuits have rejected the broad construction of the First and Seventh Circuits. *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1135 (9th Cir. 2009) ("Citrin does not comport with the plain language of the CFAA, and given the care with which we must interpret criminal statutes to ensure that defendants are on notice as to which acts are criminal, we decline to adopt [Citrin's] interpretation of 'without authorization.'"); WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199, 206 (4th Cir. 2012) ("We recognize that the Seventh Circuit applied its reasoning to egregious behavior that clearly violated the duty of loyalty. . . . Nevertheless, we believe that the theory has far-reaching effects unintended by Congress." (citation omitted))

[181] *See infra* notes 182–185 and accompanying text.

fact-patterns and sanctions.[182] Different stakes, procedural safeguards, and client demands will also affect how lawyers present their cases—including statutory interpretation arguments—before a trial or appellate judge.[183] Judges can attempt to apply the Lenity Model, but they are not immune to the influence of these differences, because they are not immune to human bias.[184] These biases likely leave judges more inclined to construct a statute narrowly in a hard-fought criminal case in which a broad construction will imprison the defendant for a minor crime than in a less contentious civil case in which the broad construction will redress a minor wrong, and not devastate the defendant.[185]

3. The Challenges Of Legislating And Litigating Computer Misconduct

The CFAA's subject matter amplifies the statutory inflation that results from its hybrid structure. Legislatures and judges struggle to control the CFAA because technology is not well understood throughout the legal system,[186] evolves unpredictably,[187] and destabilizes legal norms.[188]

[182] *See supra* notes 97–105.

[183] *See id.*

[184] *See, e.g.*, Andrew J. Wistrich, Jeffrey J. Rachlinski & Chris Guthrie, *Heart Versus Head: Do Judges Follow the Law or Follow Their Feelings?*, 93 TEX. L. REV. 855, 911 (2015) ("Most judges try to faithfully apply the law, even when it leads them to conclusions they dislike, but when the law is unclear, the facts are disputed, or judges possess wide discretion their decisions can be influenced by their feelings about litigants. This may occur without their conscious awareness and despite their best efforts to resist it. In such circumstances, where the judge is in equipoise and judicial head does not plainly indicate which decision is correct, if the case creates a strong affective response, judicial heart can carry the day. . . . Judges are not computers."); *see generally* William N. Eskridge Jr. & John Ferejohn, *Structuring Lawmaking to Reduce Cognitive Bias: A Critical View*, 87 CORNELL L. REV. 616 (2002) (discussing how judges and legislatures are vulnerable to cognitive bias).

[185] *See supra* notes 181–184 and accompanying text. Powerful corporate plaintiffs can use their experience and wealth to make a favorable outcome even more likely. *See infra* note 214 and accompanying text.

[186] *See infra* Section II.C.3.i.

[187] *See infra* Section II.C.3.ii.

[188] *See infra* Section II.C.3.iii .

i. Technology Is Not Well Understood Throughout The Legal System

Legislatures', judges', and attorneys' limited familiarity with computers adds to the difficulty of drafting, interpreting, and enforcing the CFAA across the criminal/civil divide.[189] In 1994, when Congress appended the civil action, many legislative officials lacked technical expertise[190] that could have prompted creative solutions for combating statutory inflation—or at least ensured a greater understanding of computer hacking—and thus steered them away from implementing such an unconstrained civil provision.[191]

Judges then and now often reveal a similar unfamiliarity with technology,[192] which hinders their ability to interpret the CFAA, a statute that already presents interpretive challenges due to its hybrid structure.[193] Uneven lawyering can further obfuscate the judges' job: while DOJ policies require the Assistant United States Attorneys ("AUSAs") prosecuting CFAA cases to be "technically qualified," [194] attorneys representing civil parties or criminal defendants are not

[189] *See infra* Section II.C.3.i.

[190] *See* Andrea M. Matwyshyn, *Cyber Harder*, 24 B.U. J. SCI.& TECH. L. 450, 460 ("While some members arrive in Congress with a background in computer science or professional experiences working in technology-related fields, the majority of members of Congress do not."); Adam Keiper, *Science and Congress*, 2004 NEW ATLANTIS 19, 19 (2005) ("Aristocratic scientists and democratic policymakers—the nation's experts and the people's representatives—usually speak different languages and live in different worlds."). Congress still struggles to stay up to date on new technologies, perhaps even more so than in the early 1990s, because the Office of Technology Assessment was defunded in 1995. *See* Conor Cawley, *Politicians Are Too Out of Touch to Make Laws About Tech*, TECH.CO (Oct. 15, 2018), https://tech.co/news/politicians-out-of-touch-laws-regulate-tech-2018-10 (lamenting that "most politicians are too out of touch to even understand the problems facing the tech industry, let alone regulate them"); Keiper, *supra* note 190, at 19 (2005) (describing the rise and fall of the OTA, and its benefits and limitations); Kim Zetter, *Of Course Congress Is Clueless About Tech—It Killed Its Tutor*, WIRED (Apr. 21, 2016), https://www.wired.com/2016/04/office-technology-assessment-congress-clueless-tech-killed-tutor/.

[191] *See supra* Sections I.A, II.C.1; *see also* Cyrus Y. Chung, Note, *The Computer Fraud and Abuse Act: How Computer Science Can Help with the Problem of Overbreadth*, 24 HARV. J. L. & TECH. 233 (2010) (exemplifying how advanced technical knowledge could allow for new interpretations of the CFAA).

[192] *See* Jason Tahea, *Courts Need Help When It Comes to Science and Tech*, ABA JOURNAL (Nov. 2, 2017), http://www.abajournal.com/lawscribbler/article/courts_need_help_when_it_comes_to_science_and_tech ("Lawyers and judges often do not have the background to correctly assess data, scientific research or technology."); Trevor Timm, *Technology Law Will Soon be Reshaped by People Who Don't Use Email*, GUARDIAN (May 3, 2014), https://www.theguardian.com/commentisfree/2014/may/03/technology-law-us-supreme-court-internet-nsa.

[193] *See supra* II.C.1–2.

[194] U.S. Attorneys have "primary responsibility for implementing the CHIP program," which prepares prosecutors to effectively handle computer crime and intellectual property cases. *See* CHIP Guidance, THE UNITED STATES DEPARTMENT OF JUSTICE, https://www.justice.gov/jm/jm-9-50000-chip-guidance (stating that these responsibilities include "implementing the Department's cyber and intellectual property crime strategies; ensuring that

subject to such a requirement, and thus might overlook important technical arguments for their side.[195]

ii. Technology Evolves Unpredictably

The rapid, unpredictable evolution of technology makes drafting, interpreting, and enforcing the CFAA across the criminal/civil divide even more difficult.[196] In 1984, when Congress passed the CADCFAA, the Internet was just one year old and "today's interconnected, networked world" was unimaginable.[197] This might explain why Congress felt capable of addressing all "computer abuse" in a single statute.[198] In 1986, when Congress expanded the CADCFAA into the CFAA, only about two thousand computers were online.[199] By 1994, when Congress introduced the civil provision, that number was about two million, but the first commercial web browser had not yet launched, and the first online transaction had just taken place.[200] Today, in contrast, about four point five billion people use the Internet,[201] and it plays a

experienced and technically-qualified [AUSAs] serve as the district's CHIP prosecutors" and adding that CHIP coordinators "should also ensure that the USAO notifies and coordinates with other USAOs and [CCIPS]" when computer crime and intellectual property cases come up). *But see* Matwyshyn, *supra* note 190, at 479 ("Although regional offices currently conduct CFAA prosecutions in consultation with [CCIPS], CCIPS attorneys are not always staffed on these local prosecutions and appear not to retain veto power in their handling.").

195 Tahea, *supra* note 192 ("Lawyers and judges often do not have the background to correctly assess data, scientific research or technology."). Expert witnesses (which can be called by either party, or the court) may provide some clarity for the record, but they can only opine on the case on trial, not on other consequences that might arise from an appellate court's statutory interpretation. *See* FED. R. EVID. 401; FED. R. EVID. 402; FED. R. EVID. 702. And judges cannot always distinguish between good and bad expert testimony. Paul C. Gianelli, *Forensic Science: Daubert's Failure*, 68 CASE W. RES. L. REV. 869, 937 (2018) (arguing that the judiciary has failed "to fulfill its gatekeeper role" by refusing "to demand and properly evaluate foundational research," and suggesting that "the justice system may be institutionally incapable of applying Daubert . . . because it does not have access to independent scientific expertise on an ongoing basis").

196 *See infra* Section II.C.3.ii.

197 Williams, *supra* note 10, at 437–38.

198 *See supra* Section I.A.

199 Williams, *supra* note 10, at 438.

200 Geoff Herbert, *1994 in Technology: What the Internet, Computers, and Phones Were Like 20 Years Ago*, SYRACUSE (Mar. 22, 2019), https://www.syracuse.com/news/2014/11/technology_history_internet_computers_phones_1994.html (noting that the first major internet-based companies—including Amazon and Yahoo!—were "in beginning stages" in 1994, and explaining that "[u]ntil the mid-'90s, the Internet was mostly used by scientists and scholars").

201 J. Clement, *Global Digital Population as of October 2019*, STATISTA (Nov. 20, 2019), https://www.statista.com/statistics/617136/digital-population-worldwide/.

critical role in journalism, business, and everyday life.[202] This evolution of computers and the Internet into all-encompassing business tools has, at least in part, led to the CFAA civil provision's expansion well beyond its intended supplemental role.[203]

Now that most businesses depend on computers,[204] broad interpretations of the CFAA's unauthorized access provisions give powerful corporations vast, unforeseen opportunity to use the statute's civil action to punish disloyal employees and to deter competition.[205] These private plaintiffs do not have the same incentives to exercise discretion as do prosecutors, who serve the public and have been advised by the DOJ to limit their use of the CFAA.[206] Therefore, corporations often use the CFAA as an alternative to state trade secret laws, because it has simpler pleading standards and accords federal jurisdiction, which allows plaintiffs to sue the defendant's new

[202] Williams, *supra* note 10, at 416–17 (adding that even the Supreme Court has recognized the Internet serves as our "modern public square" (citing Packingham v. North Carolina, 137 S. Ct. 1730, 1732 (2017))); *see also* Timothy H. Gray, Ethan Kisch, & Michael F. Buchanan, *Capital One Hack Prosecution Raises New and Old Questions About Adequacy of CFAA*, DATA SECURITY LAW BLOG, PATTERSON BELKNAP (Sept. 9, 2019), https://www.pbwt.com/data-security-law-blog/capital-one-hack-prosecution-raises-new-and-old-questions-about-adequacy-of-cfaa ("In 1989 . . . only about 15% of American households owned a personal computer. Today three-fourths of Americans own smartphones, which are . . . [much] more powerful than the personal computers of the late 1980s.").

[203] *See infra* notes 204–217 and accompanying text.

[204] Jamie Konn & Matthew Engel, *Employment Law for the 21st Century: Litigating Computer Fraud and Abuse Act Claims*, BLOOMBERG LAW (Aug. 10, 2017), https://news.bloomberglaw.com/daily-labor-report/employment-law-for-the-21st-century-litigating-computer-fraud-and-abuse-act-claims ("The 'work computer' . . . is ubiquitous. And such devices are typically linked to a common network to allow for widespread and seamless access to all of a company's electronic systems and connected technology.").

[205] *See* Ekeland, *supra* note 6 ("There are hundreds of civil CFAA cases between companies . . . it has become a popular way for companies to attempt to enforce intellectual property rights. . . . It also allows companies to go after former employees who copy files on the way out the door."); *see, e.g.*, United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016) (suing a disloyal employee); Facebook, Inc. v. Power Venures, Inc., 844 F.3d 1058 (9th Cir. 2016) (suing a less powerful competitor); KERR, *supra* note 57, at 79–82 ("[b]ecause computers are integral to most businesses, a business can file a civil suit . . . whenever there is a claim of potential foul play by a competitor").

[206] *See* CCIPS Memorandum, *supra* note 153.

employer and seek injunctive relief.[207] This restrains employee mobility by shifting the balance of trade secret law too far to the side of protecting proprietary information.[208]

Powerful corporations also use the CFAA to sue their competitors directly, for conduct that does not at all resemble "computer hacking."[209] Facebook, for example, has already shut down a smaller competitor by holding them liable under the CFAA for making use of Facebook's public information.[210] Following a ruling in Facebook's favor, many other companies sent cease and desist letters to inhibit their competitors from using public information.[211] Often, these corporate plaintiffs use the CFAA to force a settlement.[212]

When unsettled suits arrive in court, the plaintiffs pressure the judge to interpret the CFAA increasingly broadly.[213] These well-resourced corporate plaintiffs have a number of distinct

[207] *See* Glenn R. Schieck, Note, *Undercutting Employee Mobility: The Computer Fraud and Abuse Act in the Trade Secret Context*, 79 BROOK. L. REV. 831, 843–45 (2014); Jensen, *supra* note 20, at 92 ("Employers enthusiastically embraced this civil remedy as a way to recapture compensatory damages or obtain injunctive relief against former employees."); KERR, *supra* note 57, at 79–82 (providing additional examples of employers suing "disloyal employees").

[208] Schieck, *supra* note 207, at 834; Matwyshyn & Pell, *supra* note 15, at 492 ("Fearing retribution in criminal law for an alleged civil transgression of an employee handbook technology use policy or other breach of contract, employees may alter their analysis of a job change decision.").

[209] Williams, *supra* note 10, at 419–20 ("[C]ompanies . . . are seeking to . . . transform the CFAA into a massive computer misappropriation statute—so that they can conduct anti-competitive behavior . . . [specifically,] restrict[ing] their competitors' access to information they've published publicly online for the rest of the world to see.").

[210] Corynne McSherry, *Want More Competition in Tech? Get Rid of Outdated Computer, Copyright, and Contract Rules*, ELECTRONIC FRONTIER FOUNDATION (Dec. 20, 2018), https://www.eff.org/deeplinks/2018/12/want-more-competition-tech-get-rid-outdated-computer-copyright-and-contract-rules.

[211] *Id.*; Williams, *supra* note 10, at 419–20 ("Within weeks, citations to the two cases—particularly Power Ventures—began appearing in cease and desist letters, purporting to revoke authorization to access publicly available data published on the open Internet.").

[212] Ekeland, *supra* note 6 ("On the civil side, [the CFAA] is usually used to bludgeon a defendant into a settlement.").

[213] *See, e.g.*, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058 (9th Cir. 2016) (adopting a broad interpretation of the CFAA); United States v. Nosal, 844 F.3d 1024 (9th Cir. 2016) (adopting a broad interpretation of the CFAA); *see also* Jeffrey S. Klein & Nicholas J. Pappas, *Using CFAA to Protect Confidential Information*, WEIL (Feb. 3, 2014), https://www.weil.com/articles/using-cfaa-to-protect-confidential-information (describing how companies can use the CFAA to protect trade secrets). Because they benefit so much from the current CFAA, large silicon valley companies have opposed narrowing reform proposals. *See* Fruzsina Eordogh, *Silicon Valley is Stonewalling Efforts to Amend the Law Imprisoning Hacktivists*, MOTHERBOARD, VICE (Jul. 16, 2014), https://www.vice.com/en_us/article/4x33zp/silicon-valley-is-stonewalling-efforts-to-amend-the-law-imprisoning-hacktivists ("[T]he CFAA makes it very easy for corporate giants to sue people—anyone from employees to users that violate Terms of Service agreements. Efforts to reform the law have been squashed by millions of dollars in lobbying funds from tech companies . . . .").

advantages that their individual ex-employee or smaller-competitor defendants often lack, including experienced lawyers and long-term strategies for molding the CFAA to their benefit.[214] As a result, these plaintiffs are likely to have an outsize influence on how judges interpret the CFAA, especially because of the statute's vulnerability to civil-side inflation.[215] The success of these plaintiffs leads not only to more civil suits, but also to a corresponding swell of criminal liability.[216] Well-resourced plaintiffs can then exploit this criminal expansion by investigating potential CFAA violations, preparing a legal strategy, and then proposing an attractive case to prosecutors, who often rely on these types of private investigations, especially in white-collar cases.[217]

iii. Technology Destabilizes Legal Norms

Another reason that the CFAA's hybrid construction has caused so much statutory inflation is that the lines defining criminal and civil wrongs in cyberspace are not yet well-established.[218] The Internet benefits from, and depends upon, a rapidly evolving open-access regime that diverges from the property norms of the physical world.[219] This dynamic requires those interpreting the

[214] *See* Marc Galanter, *Why the "Haves" Come out Ahead: Speculations on the Limits of Legal Change*, 9 L. & SOC. REV. 95, 125 fig.3 (1974).

[215] *Id.*; *supra* Section II.C.2.

[216] Matwyshyn & Pell, *supra* note 15, at 492 ("expansive CFAA use in civil cases simultaneously pushes the boundaries of CFAA application in criminal cases in more aggressive directions").

[217] *See* Lisa Kern Griffin, *Inside-Out Enforcement*, *in* PROSECUTORS IN THE BOARDROOM: USING CRIMINAL LAW TO REGULATE CORPORATE CONDUCT 110, 113–19 (Anthony S. Barkow & Rachel E. Barkow eds., 2011). For example, the government brought criminal CFAA charges against David Nosal *after* his former company investigated his alleged CFAA violation and contacted the government. *See Nosal*, 844 F.3d at 1031. Even the threat of criminal prosecution enhances the ability of unscrupulous plaintiffs to stifle competition and employee agency. *See* United States v. Nosal, 676 F.3d 854 (9th Cir. 2012) (noting that a broad interpretation of the CFAA that establishes liability for violating a company's work-computer policies, such as prohibitions on checking personal emails, could allow "[e]mployers wanting to rid themselves of troublesome employees . . . [to] threaten to report them to the FBI unless they quit"). A similar paradigm exists within copyright law: powerful lobbying and special interest groups have been known to influence how law enforcement wields its criminal copyright powers. *See* Eldar Haber, *The Criminal Copyright Gap*, 18 STAN. TECH. L. REV. 247, 279 (2015).

[218] *See* Thaw, *supra* note 19, at 947; Eordogh, *supra* note 213 ("[P]rofessor Orin Kerr . . . [says that] the legal system is 'still trying to figure out what's the line between less serious offenses and more serious offenses' when it comes to computer crimes and misuse and the CFAA.").

[219] *See* James Grimmelmann, *The Internet is a Semicommons*, 78 FORDHAM L. REV. 2799, 2799–80 (2010) (explaining Grimmelmann's theory that the Internet is a semicommons, which means that "[i]t mixes private property

CFAA to resist defining "*computer* trespass" as simply physical trespass in the digital realm.[220] But there is no clear alternative definition: society has not agreed on what constitutes computer trespass, or consent to access another's server, over the Internet.[221] In other words, the CFAA's vague access provisions do not criminalize conduct that society already condemns as a public harm; instead, these provisions leave (often technically inexpert[222]) judges and attorneys to decide what computer conduct is criminal.[223]

Because there is no guiding social consensus on computer norms, the CFAA is not constrained by the traditional limitation of criminal liability to conduct that society deems morally blameworthy.[224] The broad construction of the CFAA's "unauthorized access" provisions that has developed without this limitation—and due in large part to the statute's hybrid structure—gives prosecutors the latitude to criminally charge almost anyone, because most people in today's society access a computer "without authorization" at some point.[225] This increases the risk of arbitrary or excessive enforcement, exemplified by the Swartz prosecution.[226] And arbitrary, excessive, and

in individual computers and network links with a commons in the communications that flow through the network. Both private and common uses are essential. . . . [W]e should expect difficult tensions between these two very different ways of managing resources.").

220 Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1154 (2016) ("[T]respass norms of physical space are relatively clear . . . [but] trespass norms surrounding [the Internet and its] usage are contested and uncertain. . . . Without established norms to rely on, the application of a seemingly simple concept like "authorization" becomes surprisingly hard.").

221 *See* Matwyshyn & Pell, *supra* note 15, at 511–20. Neither do private terms of service agreements—drafted by social networks, streaming services, and online shopping services—establish uniform norms. "These contracts of adhesion are often difficult for consumers to find and are routinely ignored." Sheldon Whitehouse, *Hacking into the Computer Fraud and Abuse Act: The CFAA at 30*, 84 GEO. WASH. L. REV. 1437, 1438 (2016).

222 *See supra* Section II.C.3.i.

223 For an exploration of what computer conduct people in the United States consider unauthorized and/or worthy of criminal punishment, *see* Matthew B. Kugler, *Measuring Computer Use Norms*, 84 GEO. WASH. L. REV. 1568, 1588–90 (2016) (noting that "something more than mere unauthorized access is needed to make people willing to endorse criminal sanctions").

224 *See supra* notes 98–101, 218–223 and accompanying text.

225 *See supra* notes 72–78 and accompanying text (describing the Nosal II decision, which could "criminalize the ordinary conduct of millions of citizens," and thus does align with the (admittedly still developing) social understanding of morally blameworthy computer conduct that society at large has an interest in combatting). *But see* CCIPS Memorandum, *supra* note 153 (guiding prosecutors to use their discretion carefully).

226 *See supra* note 75 and accompanying text (noting that broad interpretations of the CFAA risk "affording . . . indiscriminate power to the Justice Department"); *see also* Ekeland, *supra* note 6 ("The DOJ has also used the

politically-directed prosecutions diminish the public's trust in government, chill technological innovation, and make the Internet less free.[227]

If the CFAA's hybrid structure is left unaltered, the statute will likely continue to enhance the power of the United States government and the country's biggest companies.[228] It will imprison people for minor misconduct, and bankrupt would-be technology innovators and thought-leaders.[229] It will also undermine the ideal of free and open Internet access.[230]

III. PROPOSED SOLUTIONS

Critics of the CFAA have already proposed removing the civil provision, [231] and rewriting the law entirely. [232] These major changes would eliminate the problems associated with the statute's hybrid structure, but they have not been implemented by Congress.[233]

CFAA to prosecute individuals whose activities were largely harmless, but whose views were politically unpalatable to them—even when the alleged 'victims' did not want a criminal prosecution. This happened most notably in the prosecution of the computer innovator and activist Aaron Swartz.").

[227] *See* Lawrence Lessig, *Aaron's Law: Violating a Site's Terms of Service Should Not Land You in Jail*, ATLANTIC (Jan. 16, 2013), https://www.theatlantic.com/technology/archive/2013/01/aarons-law-violating-a-sites-terms-of-service-should-not-land-you-in-jail/267247/ (arguing that our criminal law "depends upon our trusting the government" and the prosecution of Swartz "breached that trust" for an out-of-proportion case that "had nothing to do with keeping America safe from 'criminals.'"); Tim Wu, *How the Legal System Failed Aaron Swartz—And Us*, NEW YORKER (Jan. 14, 2013), https://www.newyorker.com/news/news-desk/how-the-legal-system-failed-aaron-swartzand-us ("In an age when our frontiers are digital, the criminal system threatens something intangible but incredibly valuable. It threatens youthful vigor, difference in outlook, the freedom to break some rules and not be condemned or ruined for the rest of your life."); Williams, *supra* note 10, at 417 ("Open [Internet] access is at risk, however, as a result of recent efforts by companies to use the [CFAA] . . . to block competitors from using automated scripts to access publicly available information on their websites.").

[228] *See supra* Section II.C.

[229] *See id.*

[230] *See id.*; Max Anderson, *Protect Open Internet in the US*, HUMAN RIGHTS WATCH (Dec. 13, 2017), https://www.hrw.org/news/2017/12/13/protect-open-internet-us (noting that constraints on open internet access in the United States—a repeal of net neutrality, in this case—damage human rights to freedom of expression and access to information).

[231] *See* Matwyshyn & Pell, *supra* note 15, at 552. Judge Rakoff has even called for the elimination of all hybrid statutes. *Supra* note 109.

[232] *See generally* Matwyshyn & Pell, *supra* note 15 (proposing that a new statute—the Computer Intrusion and Abuse Act—replace the CFAA); Parker Higgins, *Critical Fixes for the Computer Fraud and Abuse Act*, ELECTRONIC FRONTIER FOUNDATION (Jan. 29, 2013), https://www.eff.org/deeplinks/2013/01/these-are-critical-fixes-computer-fraud-and-abuse-act (summarizing "Aaron's Law," a proposed rewrite of the CFAA).

[233] *See* Freedom House, *Freedom on the Net 2018 - United States*, REFWORLD (Nov. 1, 2018), https://www.refworld.org/docid/5be16aeea.html (noting that Aaron's Law has not passed).

This Part suggests more modest improvements that specifically target the statutory inflation generated by the CFAA's hybrid structure. Section III.A proposes two ways to reign in the CFAA's civil provision: prohibiting civil actions based on conduct that could be redressed by contract or business tort claims, and empowering judges to award attorneys' fees to defendants who win their cases. Section III.B then proposes two ways to limit the CFAA's criminal applicability: adding a heightened criminal intent requirement, and requiring the DOJ to approve prosecutions based on its enforcement policy. Although these four solutions complement each other, any of them could also make a positive impact independently.

A. Limiting The CFAA's Civil Provision

Congress could make two changes to the civil provision to counteract its distorting influence on the larger statute: prohibit civil actions based on conduct that could be redressed by contract or business tort suits, and allow judges to award attorneys' fees to prevailing defendants.

1. Prohibiting Civil Actions Based On Breach Of Contract Or Business Misconduct

Congress would significantly reduce the number of frivolous and anti-competitive CFAA claims by adding to the CFAA a clause that bars any civil claims based on conduct that would be actionable as breach of contract or business tort claims, regardless of whether the conduct also constitutes hacking.[234] This clause would require judges to evaluate whether a breach of contract or business tort suit could provide redress for the conduct underlying a CFAA complaint; if so, the judge would have to dismiss the CFAA claim.[235] Congress could model this change on the Private

[234] *See supra* Section I.C (noting that most civil CFAA claims are based on business misconduct and not hacking); *supra* Section II.C.3.ii (describing how corporations use the CFAA to stifle competition and employee mobility).

[235] To narrow this restriction, Congress could clarify that it applies only to conduct that could actually, practically give rise to a breach of contract or business tort claim. In other words, conduct that involves business or contracts, but that could not sustain a contract or tort claim beyond the motion to dismiss stage, could still serve as the basis for a CFAA claim. *See* Eliza Clark Riffe, Note, *Actionability and Ambiguity: RICO after the Private Securities Litigation Reform Act*, 2012 U. CHI. L.F. 463, 463–65 (2012) (arguing that judges should interpret narrowly RICO's prohibition on civil claims, such that it does not impose a blanket bar on *any* "claims sounding in securities fraud").

Securities Litigation Reform Act, which prohibited civil RICO claims based on conduct also actionable as a securities violation.[236]

This restriction would prohibit a majority of the recent civil CFAA claims, most of which arise out of business disputes that do not involve hacking, are frivolous or redundant, and end in dismissal.[237] However it would not prevent the redress of any wrongs out of which these claims arise, because plaintiffs could still sue the perpetrators of these wrongs in state court for breach of contract, trade secret violations, or other business torts.[238] The restriction clause would not defeat any CFAA claims that do not have alternate means of redress.[239]

The benefits of this restriction would outweigh any marginal loss of deterrence. The disappearance of redundant CFAA claims would protect vulnerable defendants from being pressured into unfavorable settlements.[240] It would also lift a considerable administrative burden from the federal courts, especially considering the technical complexity and legal ambiguity endemic to CFAA cases.[241] Even more importantly, this restriction would refocus the CFAA on the hacking that it was created to redress.[242] Prohibiting CFAA claims aimed at business disputes would minimize the opportunities for powerful civil plaintiffs to pressure judges to stray from the rule of lenity and adopt broad interpretations of the statute.[243]

Therefore, this restriction could serve as a counter-measure against the vulnerability to overbreadth created by the CFAA's hybrid structure.[244] And it could do so without entirely

[236] *See id.*; *supra* note 168.
[237] *See supra* Section I.C.
[238] *See id.*
[239] *See supra* notes 234–235 and accompanying text.
[240] *See supra* Section II.C.3.ii.
[241] *See supra* Section II.C.3.i (noting that many judges and attorneys are not technology experts); *supra* Section II.C.3.iii (noting that Internet norms have not been fully established yet, which adds to the difficulty of deciding CFAA claims); *supra* Section I.B (demonstrating how courts struggle to interpret the CFAA).
[242] *See supra* notes 17–26.
[243] *See supra* Sections II.C.2, II.C.3.ii.
[244] *See supra* Section II.C.

eliminating the civil provision and its potential to complement, rather than commandeer, the larger statute.

2. Allowing Judges To Award Attorneys' Fees To Defendants

A second way that Congress could limit the civil provision's overuse and overexpansion would be to give judges the option of requiring losing plaintiffs to pay defendants' reasonable attorneys' fees. Most litigation in the United States falls under the "American Rule," which leaves each party to pay their own litigation expenses. But there are exceptions. Courts can use their equitable powers to compel attorneys to pay excessive fees that they have generated.[245] And Congress can add fee-shifting provisions that override the American Rule to individual statutes.[246] These provisions can *mandate* that a losing party pay a winning party's attorneys' fees, or they can give courts the *option* to order such payment.[247] They can institute a two-way fee-shifting scheme, in which the losing party pays regardless of which party loses, or a one-way fee-shifting scheme, in which only one favored side (either the plaintiff or defendant) pays upon losing, and not vice versa.[248] Congress most often employs one-way fee-shifting statutes that favor plaintiffs in order to encourage legitimate public interest claims from cash-strapped citizens and debtors against the government or wealthy creditors.[249]

[245] *See* 28 U.S.C. § 1927 (2019) (allowing that "any attorney . . . who so multiplies the proceedings in any case unreasonably and vexatiously may be required by the court to satisfy personally the excess costs, expenses, and attorneys' fees reasonably incurred because of such conduct").

[246] *See* Fox v. Vice, 563 U.S. 826, 832 (2011).

[247] *Compare* The Fair Labor Standards Act, 29 U.S.C. § 216(b) (2019) ("[t]he court . . . *shall*, in addition to any judgment awarded to the plaintiff or plaintiffs, allow a reasonable attorney's fee to be paid by the defendant" (emphasis added)) *with* The Copyright Act, 17 U.S.C. § 505 (2019) (providing that, in a copyright claim, "the court *may* . . . award a reasonable attorney's fee to the prevailing party as part of the costs" (emphasis added)).

[248] *See id.* (demonstrating that The Fair Labor Standards Act allows only *plaintiffs* to recover attorneys' fees while The Copyright Act allows *either party* to recover attorneys' fees).

[249] *See generally* Robert V. Percival & Geoffrey P. Miller, *The Role of Attorney Fee Shifting in Public Interest Litigation*, 47 L. & CONTEMP. PROBS. 233 (1984).

The civil CFAA, however, poses the opposite problem: it has allowed powerful plaintiffs to bring too many suits against weaker opponents, and to mold the statute in their own interests.[250] A discretionary, one-way fee-shifting provision that favors the defendants would reduce the unfair advantage conferred on these plaintiffs by their power and wealth because it would incentivize small businesses and individual employees to argue their case more vigorously, and not to settle for fear of litigation costs.[251] It would also discourage these plaintiffs from bringing cases that they might not win, both because they would face a stronger defense, and because they could suffer a financial penalty if they lost.[252] Therefore, these plaintiffs would bring less claims in which the law is uncertain, and would have less opportunity to pressure judges to adopt new, broader interpretations of the CFAA.[253] This would allow criminal cases to drive the CFAA's interpretation, which would mitigate the effects of the statute's civil provision.[254]

In many circumstances, a one-way fee-shifting provision could favor the defendant too much, and discourage meritorious civil claims.[255] But the CFAA's primarily criminal purpose,[256] hybrid structure, and focus on technology make the statute uniquely suited to this fee structure.[257] Additionally, the proposed fee-shifting provision would state that judges *may* award attorneys' fees to a victorious defendant, not that they *must*. The Supreme Court has advised judges deciding

[250] *See supra* Section II.C.3.ii.

[251] Filippo Roda, The Economic Analysis of the One-way Fee-shifting Rule in Litigation 40–102 (Jan. 25, 2019) (unpublished Ph.D. thesis, University of Rotterdam), https://repub.eur.nl/pub/114700/PROEF-Fillippo-Roda-BW-3.pdf (finding that one-way fee shifting can make litigation fairer because it "incentivizes the favoured litigant to exert more effort" and thereby increases their chances of winning); *see also* Galanter, *supra* note 214 (explaining how wealth disparities between parties influence litigation outcomes).

[252] Roda, *supra* note 251, at 64 (using a "general theoretical [economic] model" to demonstrate the "discouraging power of the one-way fee-shifting rule").

[253] *Id.*; *see also* Sections II.C.2., II.C.3.ii (discussing how civil plaintiffs can pressure judges to depart from the rule of lenity).

[254] *See supra* Part II.

[255] For example, that would certainly be the case for the statutes that Congress has identified as benefiting from one-way fee-shifting provisions that favor plaintiffs. *See supra* note 249 and accompanying text.

[256] *See supra* note 61.

[257] *See supra* Part II.

whether to award attorneys' fees to consider "the large objectives" of the Act that gives them the discretion to do so.[258] When amending the CFAA to include this fee-shifting provision, then, Congress could instruct judges to use it against plaintiffs filing anti-competitive suits that do not involve computer hacking. This would lead judges to award attorneys' fees often, for now.[259] If, in the future, the civil provision is used to deter hacking that prosecutors do not have the resources to address, then judges could award attorneys' fees less often.

B. Limiting The CFAA's Criminal Provision

Two more changes would insulate the CFAA from overbroad criminal application, notwithstanding its hybridity: Congress could modify the statute to state that a defendant only incurs criminal culpability if they act with knowledge of illegality, and the DOJ could forbid AUSAs from prosecuting CFAA violations without the DOJ's approval based on its Intake and Charging Policy.

1. Adding A Heightened Criminal Intent Requirement

To prevent the CFAA from criminalizing computer conduct that society does not recognize as morally blameworthy, Congress could add to the statute a criminal-specific mens rea requirement of "willfulness" that is met only if the defendant "voluntarily and intentionally" violates a "known legal duty."[260] A strong mens rea requirement would anchor the CFAA's criminal application in a familiar, well-developed component of criminal law.[261] This would give

[258] Kirtsaeng v. John Wiley & Sons, Inc., 136 S. Ct. 1979, 1986 (2016) (citing *Zipes*, 491 U.S. 754, 759 (1989)).

[259] *See supra* Section I.C (noting that most CFAA suits involve business disputes and not hacking).

[260] *See* Cheek v. United States, 498 U.S. 192, 201 (1991). To prevent this requirement from exonerating too many defendants, Congress could specify that it does not demand that the defendant know every detail of the CFAA, only that they know that their conduct is against the law. Even with this limitation, the new mens rea requirement would be significantly heightened, and unambiguous. *See supra* note 171 (describing the ineffectiveness of the statute's current mens rea requirement).

[261] *See* Thaw, *supra* note 19, at 945–48 (suggesting that legislative reform of the CFAA's mens rea element could diminish the risk of overbroad prosecution while still allowing the statute to combat serious cybercrime).

courts and prosecutors a straightforward limiting principle, even as technology continues to develop unpredictably, and the Internet's norms continue to evolve.[262] For example, this mens rea requirement would, in most cases, defeat criminal charges brought against an individual for sharing a Netflix password, because most people do not know that such conduct arguably breaks the law.[263] By focusing on defendants' minds, this requirement would shift the power to determine what counts as criminal on the Internet back to the broader public, and away from prosecutors and judges.[264] The public could preserve the Internet's open access norms, and thereby encourage public interest journalism, innovation, and information distribution.[265]

Furthermore, as Sachs observed in her articulation of the Default and Alternative Fair Warning Rules, this criminal-specific mens rea requirement would obviate the need for courts to follow the Lenity Model.[266] Civil precedent would not address this mens rea element, and thus could not on its own establish broad criminal liability.[267]

2. Requiring Prosecutors To Receive DOJ Approval Based On The DOJ's Intake And Charging Policy

Lastly, the DOJ could decrease the threat of prosecutorial indiscretion, and increase transparency, by requiring prosecutors to gain its approval before filing criminal CFAA charges. The authority of U.S. Attorneys' Offices predates that of the DOJ; U.S. Attorneys, like top DOJ

[262] *See supra* Sections II.C.3.ii–iii.

[263] *See supra* notes 72–78. To preempt this mens rea defense, prosecutors could try to alert everyone that the CFAA criminalizes this type of password sharing in some jurisdictions. This strategy could establish that future defendants have the requisite knowledge of illegality, but it might also inspire political action to change the law. In this way, the mens requirement would prevent the CFAA from creating criminal liability that significantly outstretches society's view of what should be criminal.

[264] *See supra* Section II.C.3.iii (describing how judges currently determine what computer use should be criminalized without much guidance).

[265] *See supra* notes 9–11 and accompanying text.

[266] *See supra* notes 122–123 and accompanying text (explaining Sachs' Default and Alternative Fair Warning Rules); *see also supra* Section II.C.2 (noting that it is impossible to follow perfectly the Lenity Model and the Default Fair Warning Rule).

[267] *See supra* notes 113–124 and accompanying text.

officials, are appointed by the president.[268] Usually, U.S. Attorneys do not need approval from the DOJ before beginning an investigation or prosecution.[269] However, there are exceptions, including for RICO prosecutions: the DOJ's U.S. Attorneys' Manual instructs that "[n]o RICO criminal indictment . . . shall be filed . . . without the prior approval of the Criminal Division [of the DOJ]."[270] If prosecutors do not comply with the DOJ's requirements, the DOJ can reduce funding to those prosecutors' offices, resolve procedural disputes against them, and even discipline or remove them.[271]

Accordingly, the DOJ could add to its U.S. Attorneys' Manual a mandate that no CFAA prosecution can commence until it is approved by the DOJ. This procedural hurdle would cause prosecutors to think twice before bringing CFAA charges, and it would add the discretion of a second gatekeeper with a more national perspective and immediate access to the expertise of CCIPS.[272] Furthermore, the DOJ could require U.S. Attorneys seeking approval to justify their intended prosecution based on the factors set out in the 2014 Intake and Charging Policy.[273] Although the policy's balancing test does not produce definitive results, ordering prosecutors to work through it would at least uncover political motives, and force prosecutors to confront the factors that discourage charging minor, non-hacking violations. A description of these factors could also provide a record of how and why prosecutors decide to bring charges under the CFAA.

[268] *See* Daniel Richman, *Federal Criminal Law, Congressional Delegation, and Enforcement Discretion*, 46 UCLA L. REV. 757, 781 (1998).

[269] RICHMAN, STITH, & STUNTZ, *supra* note 141, at 12–13. Congress can also require that prosecutions receive approval from the Attorney General of the United States, but it does so only rarely. Richman, *supra* note 268, at 802–05. Because Congress imposes this requirement only rarely, and because the other solutions presented in this Note already address Congress, this Note focuses instead on requiring the DOJ's approval.

[270] *See* RICHMAN, STITH, & STUNTZ, *supra* note 141, at 510–12.

[271] Richman, *supra* note 268, at 781.

[272] *Id.* at 802–05.

[273] *See* CCIPS Memorandum, *supra* note 153.

However, this proposed requirement has limitations and drawbacks. It would not stop every overzealous prosecution: after all, Swartz's charges had approval from the DOJ.[274] It would also strip some much-valued independence from U.S. Attorneys.[275] It would centralize authority, despite a national ideal of fragmented, local law enforcement.[276] And it would modify the application of a statute that Congress enacted without Congressional approval.[277] Still, these downsides do not outweigh the benefits of protecting the public from arbitrary, politically-motivated, or disproportionate prosecutions, and the chilling of beneficial activity and trust in government that comes from them.[278]

CONCLUSION

The CFAA's rapid expansion demonstrates how new technologies can transmute old laws and legal procedures. Left unchecked, this process will often further consolidate power with society's most powerful government and corporate groups. To avoid that result, and to promote the democratizing potential of new technologies, legislatures, judges, and advocates should consider how laws are structured, in addition to what laws explicitly prohibit. Adding structural safeguards to statutes that address evolving technologies can guide their development and prevent their misuse.

[274] *See* Steven Hsieh, *Why Did the Justice System Target Aaron Swartz?*, ROLLING STONE (Jan. 23, 2013), https://www.rollingstone.com/politics/politics-news/why-did-the-justice-system-target-aaron-swartz-106848/.

[275] Richman, *supra* note 268, at 806–08.

[276] *Id.*

[277] *Id.* at 813–14.

[278] *See supra* notes 226–227 and accompanying text.