Standing Under the Computer Fraud and Abuse Act

Michael J. O'Connor*

ABSTRACT

The Computer Fraud and Abuse Act ("CFAA") provides civil and criminal penalties for computer intrusion. Current scholarship seeks to determine when a putative defendant has accessed a system without authorization. But no academic articles address who can bring suit for the intrusion. The system owner seems the natural complainant; after all, the CFAA punishes cyber-trespass. But the few courts to address the issue thus far have come to a surprising and contrary conclusion: anyone with confidential information on the system may bring suit. This turns the CFAA from a cyber-trespass statute into a more expansive tool, guarding against trade secret theft and other offenses normally governed by very different case law. Resolving this question has profound implications in an era when confidential documents get routinely stored on Dropbox, Google Drive, Amazon Web Services, and similar platforms. This Article will examine whether courts are correct to accord such broad standing to complainants and whether this comports with the Supreme Court's views on constitutional standing. This Article will also consider whether this broad concept of CFAA standing makes sense in light of the statute's history and purpose, and what effect it has on ideas about digital ownership generally.

*J.D., University of Pennsylvania Law School; B.S., The Pennsylvania State University (Computer Science).

Table of Contents

I. INTRODUCTION

The Computer Fraud and Abuse Act ("CFAA") punishes computer misuse.[1] When a user accesses a system without authorization or exceeds their authorization, the user becomes criminally and civilly liable.[2] Despite dozens of CFAA lawsuits brought each year, courts have left curiously unexplored the question of who can bring suit under the CFAA. Most would assume that the system owner can bring suit; after all, the cyber-trespasser broke into their "home." But the few courts to address the issue have cast standing in a much broader fashion. They conclude that the statute's language granting a civil remedy to "[a]ny person who suffers damage or loss"[3] permits standing not only by system owners, but anyone with documents on those systems. Essentially, this transforms the CFAA into a law protecting trade secrets, personal privacy, or both.

This Article will consider whether the current consensus aligns with the history, text, structure, and purpose of the CFAA. Part II of this Article discusses the CFAA's history. Part III discusses the limited case law on CFAA standing and whether broad standing creates tension with more

[1] *See* Paul J. Larkin, Jr., *Reasonably Construing the Computer Fraud and Abuse Act to Avoid Overcriminalization*, HERITAGE FOUND. (June 19, 2013), https://herit.ag/3aQp2Lb ("The Computer Fraud and Abuse Act (CFAA) is the federal government's principal legal weapon in the battle to protect computer systems and electronically stored information from thieves and vandals.").

[2] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2018).

[3] *Id.* § 1030(g).

established case law on concepts like access and authorization. Part IV discusses whether broad CFAA standing satisfies the Supreme Court's constitutional standing jurisprudence. Part V discusses whether Congress should revise the current broad approach to CFAA standing to better align with either a trespass or digital ownership framework.

II. HISTORY OF THE COMPUTER FRAUD AND ABUSE ACT

The CFAA has evolved throughout its history, but it remains focused on punishing those that invade or damage computer systems. The statute first arose from popular pressure to combat computer hacking[4] and concern that existing laws did not cover common hacking crimes.[5] Congress initially limited the law to computers implicating national security and financial privacy. Congress later expanded the statute to reach all computers in interstate commerce. With cross-state computer delivery and the ubiquitous Internet, the CFAA now reaches essentially every computer and every computer user in the United States and many outside the country's borders.

When originally enacted in 1984, Congress limited the CFAA to three specific scenarios: "computer misuse to obtain national security secrets, computer misuse to obtain personal financial records, and hacking into U.S. government computers."[6] In 1986, Congress added interstate offenses committed over an interstate computer network.[7] The change meant little at the time; three decades ago, "when use of the Internet remained in its infancy, few crimes would be included in [the statute's] reach."[8] In 1994, the CFAA's civil provision first appeared.[9] It has been

[4] *See, e.g.*, H.R. REP. No. 98-894, at 10 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3696 ("For example, the motion picture 'War Games' showed a realistic representation of the automatic dialing and access capabilities of the personal computer."); Patrick S. Ryan, *War, Peace, or Stalemate: Wargames, Wardialing, Wardriving, and the Emerging Market for Hacker Ethics*, 9 VA. J. L. & TECH. 1, 27 (2004) ("Notably, the first version of the CFAA was passed shortly after the release of *WarGames*, almost as if the law were drafted to directly address the types of activities carried out by [Matthew Broderick's character] Lightman.").

[5] *See, e.g.*, H.R. REP. No. 98-894, at 6 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689, 3691 ("There is no specific federal legislation in the area of computer crime. Any enforcement action in response to computer-related crime must rely on statutory restrictions that were designed for other offenses, such as mail fraud (18 U.S.C. 1341) or wire fraud (18 U.S.C. 1343) statutes. Even if an approach is devised that apparently covers the alleged acts in computer-related crimes, it still must be treated as an untested basis for prosecution in the federal trial courts.").

[6] Orin S. Kerr, *Cyberspace & the Law: Privacy, Property, and Crime in the Virtual Frontier: Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1564 (2010) (citing 18 U.S.C. § 1030(a)(1)–(3) (Supp. II 1985)).

[7] *See id.* at 1565.

[8] *Id*.

[9] *See* Computer Abuse Amendments Act of 1994, Pub. L. No. 103-322, 108 Stat. 2097, 2098 (codified at 18 U.S.C. § 1030(g) (2018)).

used for a range of purposes, from employers punishing trade secret misappropriation[10] to plaintiffs bootstrapping into federal court fundamentally state-law claims like trade secret theft and breach of contract.[11]

In 1996, Congress dramatically expanded the CFAA. Of principal interest are two changes to Section 1030(a)(2), now the broadest and most commonly used provision for punishing hacking.[12] First, the "Federal interest" computer protected under the earlier statute was replaced by a new category called the "protected computer."[13] Although the prior definition covered crimes involving computers in two or more states, the "protected computer" included any machine "used in or affecting interstate or foreign commerce or communication."[14] With that change, the statute reached any computer connected to the Internet.[15] Second, Section 1030(a)(2) went from prohibiting unauthorized access that obtains certain sensitive information to prohibiting unauthorized access that obtains *any* information.[16] Obtaining information includes merely reading it.[17]

The statute has always maintained a strange tension. The law frames access and authorization in terms of the computer itself.[18] But the actual offense requires obtaining information, with the information's nature changing the crime's severity.[19] At one time, with everything from servers

[10] *See, e.g.*, WEC Carolina Energy Sols. LLC v. Miller, 687 F.3d 199 (4th Cir. 2012); Richard Warner, Symposium, *The Employer's New Weapon: Employee Liability Under the Computer Fraud and Abuse Act*, 12 EMP. RTS. & EMP. POL'Y J. 11 (2008).

[11] *See* Kelsey T. Patterson, *Narrowing It Down to One Narrow View: Clarifying and Limiting the Computer Fraud and Abuse Act*, 7 CHARLESTON L. REV. 489, 496 (2013) ("[A]sserting a claim under a federal statute, such as the CFAA, opens the door to federal court.").

[12] *See* Tim Wu, *Fixing the Worst Law in Technology*, NEW YORKER (Mar. 18, 2013), https://bit.ly/2ReLENS (referring to 18 U.S.C. § 1030(a)(2)(c) as "the broadest provision").

[13] *See* Economic Espionage Act of 1996, Pub. L. No. 104-294, tit. II, 110 Stat. 3488, 3491–92 (1996).

[14] 18 U.S.C. § 1030(e)(2) (2018).

[15] *See* Kerr, *supra* note 6, at 1568. Subsequent amendments expanded the "protected computer" definition yet again, so it now reaches any computer even "affecting" interstate commerce. *See id.* at 1569–71. Under current Commerce Clause jurisprudence, this would likely reach every computer, even those lacking any Internet connection. *See id.* But given the Internet's modern ubiquity, this may mean a legal distinction without practical difference.

[16] *See id.* at 1566–67.

[17] *See* S. REP. NO. 99-432, at 6 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 2479, 2484 (explaining that "obtaining information" in statute included "mere observation of the data"); *see also* Am. Online, Inc. v. Nat'l Health Care Discount, Inc., 121 F. Supp. 2d 1255, 1276 (N.D. Iowa 2000).

[18] *See* Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1976, 2190 (1984) ("Whoever—(1) knowingly accesses a computer without authorization"); Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a) (2018) ("Whoever—(1) having knowingly accessed a computer without authorization").

[19] *See, e.g.*, Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1976, 2190 (1984) ("Whoever . . . obtains information that has been determined by the

to laptops hosting principally the computer owner's data, this duality made little difference. But now, the server owner and the information owner could be totally unrelated, which leads to questions about who can enforce the CFAA.

III. CFAA INJURY

Without injury, a litigant cannot bring a lawsuit. To determine injury, the court looks first to statute or common law: Does the law recognize that you were wronged? Particularly when Congress uses vague language at odds with the statute's purpose, this seemingly straightforward analysis can require substantial thought about Congress' intended goals. But even when Congress makes clear its intent, the Constitution imposes limits on the legislature's ability to define injury, or at least the federal courts' ability to redress it.

The CFAA implicates both these tests. Congress chose to permit civil claims by "any person who suffers damage or loss" due to actions violating the CFAA.[20] This seems to open the door for claims not only by system owners, but anyone with data on the system. But Congress also intended to craft a cyber trespass statute, and premised liability on lack of authorization *as determined by the system owner*. This creates a disconnect between the standing inquiry and the liability inquiry. These seemingly untethered results raise legitimate questions about whether Congress intended such broad standing.

A. Current CFAA Standing Case Law

Every day, more people utilize cloud services like Dropbox, Google Docs, and Microsoft OneDrive to store their files.[21] The benefits are obvious: ubiquitous data access from every device you own.[22] The CFAA

United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations"); Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a) (2018) ("Whoever . . . having obtained information that has been determined by the United States Government pursuant to an Executive order or statute to require protection against unauthorized disclosure for reasons of national defense or foreign relations").

[20] Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g) (2018).

[21] *See, e.g.*, Kevin Curran, *Can Dropbox Keep Its Paid User Growth Momentum Going?*, REAL MONEY (Aug. 10, 2018, 4:37 PM), https://bit.ly/2vUv1iR ("Dropbox Inc.'s (DBX) paid users grew to 11.9 million in the second quarter, up 400,000 from the prior quarter and 1 million from the prior year quarter.").

[22] *See Easy File Syncing*, DROPBOX, https://bit.ly/3bxT8Di (last visited April 30, 2020) ("Save a file to the Dropbox folder on your computer, and it's synced automatically to your mobile device.").

case law is slowly moving to reflect this new reality, with more cases brought by account or document owners against trespassers.

In *Theofel v. Farey-Jones*, a civil litigant "used a 'patently unlawful' subpoena to gain access to e-mail stored by [the opposing parties'] Internet service provider."[23] When the opposing parties learned that the Internet service provider ("ISP") had turned over their e-mails without notice from either the litigant or the ISP, they sued under the Wiretap Act, the Stored Communications Act, and the CFAA.[24] The district court dismissed the CFAA claim "on the theory that the Act does not apply to unauthorized access of a third party's computer."[25] But the Ninth Circuit disagreed, holding that the CFAA extends to third-party computers:

> The district court erred by reading an ownership or control requirement into the Act. The civil remedy extends to "[*a*]*ny person* who suffers damage or loss by reason of a violation of this section." . . . Individuals other than the computer's owner may be proximately harmed by unauthorized access, particularly if they have rights to data stored on it.[26]

District courts across three other circuits have also addressed the point, and unanimously agree with *Theofel* that third-party computer ownership poses no obstacle to a CFAA claim.[27]

Congress manifests its intent through statutory text. The courts' role is to faithfully apply that text: "[W]hen the statute's language is plain, the sole function of the courts—at least where the disposition required by the text is not absurd—is to enforce it according to its terms."[28] But individual statutory provisions must not be isolated from the rest.[29] We should read a

[23] Theofel v. Farey-Jones, 341 F.3d 978, 981 (9th Cir. 2003).

[24] *See id.* at 981–82.

[25] *Id.* at 986.

[26] *Id.* (quoting 18 U.S.C. § 1030(g) (2018)).

[27] *See, e.g.*, Phillips Med. Sys. Puerto Rico, Inc. v. GIS Partners Corp., 203 F. Supp. 3d 221, 230 (D.P.R. 2016) ("Moreover, '[i]ndividuals other than the computer's owner' may bring an action under the CFAA because they 'may be proximately harmed by unauthorized access, *particularly if they have rights to data stored on [the computer]*.'" (citing *Theofel*, 359 F.3d 1066, 1078)); Océ N. Am., Inc. v. MCS Servs., Inc., 748 F. Supp. 2d 481, 487 (D. Md. 2010) ("Plaintiff correctly cites to *Theofel v. Farey-Jones* for the proposition that it does not need to own the 'protected computer' in order to claim damages for a violation of the CFAA[.]"); Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 472–78 (S.D.N.Y. 2004) (holding that confidential document owner could enforce CFAA when stolen documents stored on business partner's server, but finding loss insufficient to trigger CFAA private-action threshold), *aff'd*, 166 F. App'x 559 (2d Cir. 2006).

[28] Lamie v. U.S. Trustee, 540 U.S. 526, 534 (2004).

[29] *See* FDA v. Brown & Williamson Tobacco Corp., 529 U.S. 120, 132 (2000) ("In determining whether Congress has specifically addressed the question at issue, a reviewing court should not confine itself to examining a particular statutory provision in isolation. The meaning—or ambiguity—of certain words or phrases may only become evident when placed in context.").

statute to "fit, if possible, all parts into an harmonious whole."[30] And the broad view of standing creates tension with the concept of authorization under the CFAA.

B. Tensions With "Access" and "Authorization"

Congress cannot criminalize every interaction with a computer, so the CFAA contains a gating concept: it punishes "access[] . . . without authorization[.]"[31] The circuits have deeply split over how to define "authorization," but every circuit tethers the concept to permission from the system owner. If we link "authorization" to the system owner but give broad standing to anyone injured, that disconnect injects both substantive and practical uncertainty into CFAA litigation.

1. Current Approaches to Authorization

The CFAA punishes whoever "intentionally accesses a computer without authorization or exceeds authorized access."[32] In its wisdom, Congress defined neither "access" nor "authorization."[33] Surprisingly,

[30] FTC v. Mandel Bros., Inc., 359 U.S. 385, 389 (1959); *see also* Davis v. Mich. Dep't of Treasury, 489 U.S. 803, 809 (1989) ("It is a fundamental canon of statutory construction that the words of a statute must be read in their context and with a view to their place in the overall statutory scheme."); United Sav. Ass'n of Tex. v. Timbers of Inwood Forest Assocs., Ltd., 484 U.S. 365, 371 (1988). As the Supreme Court explains in *Mandel Brothers*, this "harmonious whole" rule does not apply for penal statutes, which "deserve[] strict construction." *Mandel Bros.*, 359 U.S. at 389. In addition, while the CFAA contains both civil and criminal provisions, it generally uses the same standards to determine when an offense occurred. Because the same words in the same section of the same statute cannot be read two different ways—one way when the government brings criminal charges and another when a plaintiff brings a civil complaint—due process requires strict construction. *See* Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004) ("Because we must interpret the statute consistently, whether we encounter its application in a criminal or noncriminal context, the rule of lenity applies."). The civil-action provision seems one of the few elements in the entire statute that will only be encountered outside the criminal context, and thus can be viewed through an alternative lens.

[31] Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) (2018).

[32] *Id.* Similar language appears throughout the statute, but subsection (a)(2) is the broadest and most frequently charged provision.

[33] *See id.* § 1030(e) (defining neither "access" nor "without authorization"); *see also* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001) ("Congress did not define the phrase 'without authorization,' perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive."). Congress may have left the statute intentionally ambiguous; by sacrificing precision for flexibility, a single statute can apply to the many ways that individuals abuse computers. *See* Greg Pollaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, 2010 DUKE L. & TECH. REV. 012, ¶ 10 (2010) ("Congress decided early in the CFAA's history that it wanted a single statute to cover the field of computer crime 'rather than identifying and amending every potentially applicable statute affected by advances in computer technology.' The price for this legislative expediency is that one relatively brief statute is applied to a range of disparate activities such as fraud, trespass, spam, phishing, worms, viruses and denial of service attacks. This has inevitably forced square pegs into round holes.").

Congress *did* define "exceeds authorized access," explaining that it means to access a computer with authorization and then transgress that authorization's boundaries.[34]

Left with little statutory guidance, courts and scholars have spun numerous tests and theories for access and authorization. This Article organizes those approaches into four groups: (1) *International Airport Centers, LLC v. Citrin*'s agency approach; (2) the use contract approach; (3) the access contract approach; and (4) the code-based approach.

Citrin's agency approach premises liability on loyalty.[35] Defendant Jacob Citrin decided to breach his non-compete agreement with his current employer and wiped his work laptop to impede his employer's investigation.[36] Citrin's employer, International Airport Centers ("IAC"), sued under the CFAA for this "damage."[37] IAC had issued this laptop to Citrin. But while IAC permitted Citrin to use it for the company's benefit, the Seventh Circuit concluded that IAC's authorization lapsed when Citrin decided to use (or abuse) it for his *own* benefit.[38] Setting aside intentional misconduct, employees are neither automatons nor indentured servants. Minds wander. People find new jobs. They should not incur criminal liability every time they read the news on their work computer or find themselves mildly less productive in their last few weeks on the job.

Seemingly uncomfortable with cabining criminal liability only by the loose concept of agency, no other circuits have adopted *Citrin*'s unalloyed reliance on that doctrine. Every other circuit, except the Ninth, bases CFAA liability on violating contracts and terms of service. But the contracts do not merely specify the times, circumstances, and methods by which a user can access the system; they often specify what a user can do after they access it. This turns an anti-hacking statute into a general license to combat bad behavior.

For example, in *EF Cultural Travel BV v. Explorica, Inc.*, the First Circuit concluded that using proprietary data to inform the method by which a party accessed a public website would likely "exceed[] authorized

[34] 18 U.S.C. § 1030(e)(6) (2018) ("[T]he 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 accesser is not entitled so to obtain or alter.").

[35] *See* Int'l Airport Ctrs. LLC, v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006).

[36] *See id.*

[37] *See id.* at 420 (citing Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A)(ii) (2018)).

[38] *See id.* ("[Citrin's] authorization to access the laptop terminated when, having already engaged in misconduct and decided to quit IAC in violation of his employment contract, he resolved to destroy files that incriminated himself and other files that were the property of his employer, in violation of the duty of loyalty that agency law imposes on an employee." (citing United States v. Galindo, 871 F.2d 99, 101 (9th Cir.1989); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124–25 (W.D. Wash. 2000); Restatement (Second) of Agency §§ 112, 387 (1958))).

access."[39] There, all the pages accessed were publicly available,[40] but the First Circuit explained that using the data while navigating the website "reeks of use—and, indeed, abuse—of proprietary information that goes beyond any authorized use of EF's website."[41] Similarly, based on a Citigroup policy restricting how employees use customer information, the Fifth Circuit upheld Dimetriace Eva-Lavon John's CFAA conviction for passing confidential customer account information to her confederates in a fraud ring.[42] Additionally, in *United States v. Drew*, the U.S. Government advocated criminal CFAA prosecution for violating website terms of service.[43] The district judge concluded that the website terms were too vague to inform the defendant that violating them would strip her authorization to use the site,[44] but the position remains a logically consistent application of the use contract approach.

Courts have criticized the use contract approach as misapplying the CFAA's text[45] and creating an endlessly malleable criminal law[46] similar to the agency approach. Any employee that violates an employer's trust or its computer-use policy could end up behind bars. Calling a family member from their work phone, checking scores on ESPN.com, or playing Sudoku online all result in potential tickets to jail.[47] Responsive to these textual and practical concerns, some courts hold that while the CFAA does not criminalize improper *use*, improper *access* falls within its reach.

The Eleventh Circuit's opinion in *United States v. Rodriguez* arguably originated the access contract theory.[48] In that case, Rodriguez

[39] *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–84 (1st Cir. 2001).

[40] The First Circuit conceded this point in a later companion opinion. *See* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 61–62 (1st Cir. 2003) ("[I]t appears that the codes could be extracted more slowly by examining EF's webpages manually, so it is far from clear that Zefer would have had to know that they were confidential. The only information that Zefer received that was described as confidential (passwords for tour-leader access) apparently had no role in the scraper project.").

[41] *Explorica*, 274 F.3d at 583.

[42] *See* United States v. John, 597 F.3d 263, 269–71 (5th Cir. 2010).

[43] *See* United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009).

[44] *See id.* at 464–66.

[45] *See* United States v. Nosal, 676 F.3d 854, 858–64 (9th Cir. 2012).

[46] *See id.* at 862 ("Not only are the terms of service vague and generally unknown–unless you look real hard at the bottom of a webpage–but website owners retain the right to change the terms at any time and without notice. . . . Accordingly, behavior that wasn't criminal yesterday can become criminal today without an act of Congress, and without any notice whatsoever.").

[47] *See id.* at 860 ("Employees who call family members from their work phones will become criminals if they send an email instead. Employees can sneak in the sports section of the *New York Times* to read at work, but they'd better not visit ESPN.com. And sudoku enthusiasts should stick to the printed puzzles, because visiting www.dailysudoku.com from their work computers might give them more than enough time to hone their sudoku skills behind bars.").

[48] *See* United States v. Rodriguez, 628 F.3d 1258, 1260–63 (11th Cir. 2010).

received repeated, explicit warnings to access Social Security records only when necessary for his job.[49] He ignored those warnings and delved into files for romantic partners, friends, acquaintances, and strangers.[50] Rejecting the use contract approach,[51] the Eleventh Circuit held that because Rodriguez had *accessed* files beyond his purview, his use was irrelevant.[52] While the access contract approach seems more defensible than the use contract approach, the result often turns on labeling, not substance, rendering the line between the two approaches "illusory."[53] Indeed, the court in *United States v. Drew* considered the MySpace Terms of Service as a constraint on access and would have permitted them on that basis, even though ultimately finding them void for vagueness.[54] Some conclude that such malleability provides insufficient notice. They argue that accessors only lack authorization when they bypass authentication gates using a stolen password, software exploit, or similar method.[55]

[49] *See id.* at 1260–62.

[50] *See id.*

[51] Courts and scholars often group *Rodriguez* with *John* (the use contract case). *See, e.g.*, *Nosal*, 676 F.3d at 862 (classifying *Rodriguez* with *Citrin* and *John*); Patricia L. Bellia, *A Code-Based Approach to Unauthorized Access Under the Computer Fraud and Abuse Act*, 84 GEO. WASH. L. REV. 1442, 1452 n.51 (2016) (classifying *Rodriguez* with *John*, but not *Citrin*). But *Rodriguez* explicitly differentiated itself from *John*. *See Rodriguez*, 628 F.3d at 1263.

[52] *See Rodriguez*, 628 F.3d at 1263 ("[Rodriguez's] use of information is irrelevant if he obtained the information without authorization or as a result of exceeding authorized access.").

[53] Bellia, *supra* note 51, at 1454–55 ("Some courts have enforced restrictions on access that attempt to incorporate restrictions on use. For example, an employer may state that its employees have access to a confidential database for a specific purpose and that access to the database for any other purpose is not permitted. . . . Under such an approach, liability under the CFAA turns on whether an employer that seeks to restrict its employees' use of confidential information happens to incorporate the use restriction into its policy on access. The line between 'broad' and 'narrow' views becomes illusory."); *see also* Jonathan Mayer, *The Narrow Interpretation of the Computer Fraud and Abuse Act: A User Guide Applying United States v. Nosal*, 84 GEO. WASH. L. REV. 1644, 1659 (2016) ("That is not to say that the access-use dichotomy is a paragon of doctrinal clarity.").

[54] *See* United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009) ("Clearly, the MSTOS was capable of defining the scope of authorized access of visitors, members and/or users to the website.").

[55] *See, e.g.*, Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2173 (2004) ("I . . . demonstrate that courts should apply the federal Computer Fraud and Abuse Act only when a system owner uses strong technical measures to control access, and argue that courts have too broadly interpreted that statute by allowing system owners to invoke it to enforce terms of use and other weak forms of notice."); Bellia, *supra* note 51, at 1475 ("[A] code-based approach to the CFAA offers a number of advantages."); Orin S. Kerr, *Norms of Computer Trespass*, 116 COLUM. L. REV. 1143, 1164 (2016) ("In my view, an authentication requirement draws the proper line."); Patterson, *supra* note 11, at 528 ("[C]ourts should expressly adopt a code-based approach to [the CFAA's] interpretation."). *But see* Mayer, *supra* note 53, at 1670 ("There is much to commend the code-based standard of liability, for example, and the Author's own preference is that Congress implement a version of that approach. . . . Much as the code-based test holds appeal, it simply cannot be squared with the statute.").

Until very recently, no court had accepted this code-based approach for the CFAA.[56] The Ninth Circuit changed that in *HiQ Labs, Inc. v. LinkedIn Corp.*, adopting the position that liability attaches only when one bypasses an authentication gate.[57] *HiQ Labs* concluded that when a system owner revokes a user's access, the system owner does not (and seemingly cannot) prohibit access to portions of the website located *outside* an authentication gate.[58] Rather, the system owner's cease-and-desist prohibits the user from creating new accounts or using an existing account to reach *through* an authentication gate.[59]

2. Textual Tensions

Both the access contract approach and the code-based approach recognize that the statute tethers authorization to access.[60] The question is not whether some aspect of the user's interaction with the system was unwanted by the owner, but whether their *access* was unwanted.[61] And *all*

[56] *See The Computer Fraud and Abuse Act: Circuit Split and Efforts to Amend*, U. CAL. BERKELEY SCH. L.: BTLJ BLOG (Mar. 31, 2014), https://bit.ly/2WEA6H6 ("No court has adopted the code-based interpretation of the CFAA.").

[57] *See* HiQ Labs, Inc. v. LinkedIn Corp., No. 17-16783, slip op. at 29 (9th Cir. Sept. 9, 2019) (suggesting that "authorization is only required for password-protected sites or sites that otherwise prevent the general public from viewing the information").

[58] *See id.* at 30–31.

[59] *See id.*

[60] *See, e.g.*, Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) (2018) (imposing criminal liability on one who "intentionally accesses a computer without authorization or exceeds authorized access"); Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 619 (E.D. Pa. 2013) (quoting Clinton Plumbing & Heating v. Ciaccio, No. 09-2751, 2010 WL 4224473, at *5 (E.D. Pa. Oct. 22, 2010)) ("These [use contract] rulings wrap the intent of the employees and use of the information into the CFAA despite the fact that the statute narrowly governs access, not use. . . . Subjective intent departs from the original view that the CFAA concerns what is 'tantamount to trespass in a computer.'"); H.R. REP. No. 98-894, at 20 (1984), *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3706 ("Section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer. Thus, the conduct prohibited is analogous to that of 'breaking and entering' rather than using a computer (similar to the use of a gun) in committing the offense."); David J. Schmitt, *The Computer Fraud and Abuse Act Should Not Apply to the Misuse of Information Accessed With Permission*, 47 CREIGHTON L. REV. 423, 432 (2014) ("The CFAA was aimed at 'outside hackers' who improperly access protected computers, and 'inside hackers' who have permission to use protected computers but obtain information beyond the permission that had been granted.").

[61] An earlier version of the statute considered use. *See* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473 § 2102, 98 Stat. 2190, 2190-91 (1984) ("Whoever . . . knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend . . . ."). But Congress abandoned that approach, strongly suggesting that it did not intend to criminalize improper use. *See* ANTONIN SCALIA & BRYAN A. GARNER, READING LAW: THE INTERPRETATION OF LEGAL TEXTS § 40 (2012) ("Reenactment Canon. If the legislature amends or reenacts a provision other than by way of a consolidating statute or restyling project, a significant change in language is presumed to entail a change in meaning."); Samantha Jensen, Comment, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*,

the approaches consider authorization at the system level, rather than the document or data level. The CFAA itself strongly suggests these linkages among access, authorization, and the computer itself: "Whoever—(1) having knowingly accessed a computer without authorization . . . ."[62]

Admittedly, in many situations, the system owner cannot be easily identified.[63] With dedicated servers, "you lease an entire server from your hosting company."[64] With virtual servers, you get the appearance of an entire computer to yourself, but in reality you are working within a software-created sandbox on a computer that may host many similar sandboxes.[65] With normal Internet accounts like an e-mail account, you abandon even the pretense of having your own computer; you have only limited access to a single application. But system ownership and data ownership are completely different concepts, and the CFAA ties access and authorization to system ownership.

This creates tension with the broad standing articulated in *Theofel*.[66] Both the plain statutory language and every circuit's approach hold that the system owner can authorize or withhold access. For that reason, the system owner is arguably the only person harmed when a hacker breaks in without authorization or a user transgresses their granted authorization's boundaries. But *Theofel* grants standing to sue even where a person had no authority to permit—or, more importantly, to withhold—access.

This generates a notable discontinuity between the statute's gatekeepers and its enforcers, which raises both practical and substantive concerns. From a practical aspect, the system owner would be a stranger to the litigation. They would be forced to produce documents and testify only under the deferential standard applied to third parties. In civil cases, this requires that the litigants "avoid imposing undue burden or expense" on the system owner.[67] Litigants will find it more difficult to prove how the system owner communicated authorization or prohibition. Documenting access may require records that are unavailable to the parties themselves. On the substantive side, broad standing suggests that the

36 HAMLINE L. REV. 81, 125 (2013) ("Agency and contract-based interpretations are incorrect because persistent incorporation of 'use' flagrantly returns the CFAA to a version Congress has expressly revoked.").

[62] Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a) (2018).

[63] *Cf.* Mayer, *supra* note 53, at 1651–53 (suggesting the problems with drawing boundaries around systems).

[64] *See Colocation Pricing (The 2020 Definitive Guide)*, DIG. SERV. CONSULTANTS (Nov. 15, 2019), https://bit.ly/39l0xV1.

[65] *See Server Virtualization*, PCMAG, https://bit.ly/2UxIdCC (last visited May 4, 2020) ("Running applications in separate, isolated partitions (separate 'virtual machines') within a single server. Widely used in enterprise and cloud computing datacenters, each virtual machine (VM) runs its own OS and applications and can be moved or copied from one server to another for load balancing or to expand processing capability.").

[66] *See* Theofel v. Farey-Jones, 341 F.3d 978, 981 (9th Cir. 2003).

[67] FED. R. CIV. P. 45(d)(1).

statute was intended to protect digital property generally. But the legislative history, case law, and scholarship all suggest that the CFAA is fundamentally a cyber-trespass statute, which raises the question whether *Theofel* and the other courts adopting its approach have given sufficient thought to the zone of interests that Congress intended to protect.

C. Statutory Standing

Just as rules of construction determine who must obey a statute, similar rules determine who can bring suit. Among these rules are the "zone of interests" test and proximate causation.[68]

1. Zone of Interests

Statutory causes of action extend to plaintiffs whose complaints "fall within the zone of interests protected by the law invoked."[69] We must, therefore, ask what interests Congress intended the CFAA to protect. The text, structure, and history of the CFAA all suggest that Congress was enacting a cyber-trespass law.

The statutory text suggests trespass by using the terms "access" and "authorization,"[70] both drawn from physical trespass.[71] Meanwhile, the legislative history indicates that Congress was concerned with computer break-ins. As explained above, the CFAA was a direct reaction to popular media depicting hackers trespassing into sensitive government systems.[72] Indeed, the Senate Report explains that Congress was concerned that hacking was being shoehorned into inappropriate causes of action like "theft, embezzlement or even the illegal conversion of trade secrets."[73] In light of this evidence, both courts and scholars have recognized that Congress was enacting a cyber-trespass law.[74] Indeed, in the earliest

[68] *See* Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118, 128–33 (2014). While these tests were often referred to as determining "prudential standing," in *Lexmark*, the Supreme Court clarified that they are tools aiding statutory interpretation. *See id.* at 127.

[69] *Id.* at 129 (quoting Allen v. Wright, 468 U.S. 737, 751 (1984)).

[70] *See, e.g.*, Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) (2018).

[71] *See, e.g.*, Josh Goldfoot & Aditya Bamzai, *A Trespass Framework for the Crime of Hacking*, 84 GEO. WASH. L. REV. 1477, 1478 ("The text, structure, and history of the CFAA all indicate that its 'without authorization' term incorporates preexisting physical trespass rules."); Kerr, *supra* note 55, at 1146 ("[C]oncepts of authorization rest on trespass norms.").

[72] *See supra* Part II.

[73] S. REP. No. 99–432, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479, 2491.

[74] *See, e.g.*, Facebook, Inc. v. Power Ventures, Inc., 844 F.3d 1058, 1065 (9th Cir. 2016) ("The CFAA prohibits acts of computer trespass by those who are not authorized users or who exceed authorized use."); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 495 (D. Md. 2005) ("Federal courts interpreting [SECA and the CFAA] have noted that their general purpose . . . was to create a cause of action against computer hackers (e.g., electronic trespassers)." (internal quotation marks omitted)); Goldfoot & Bamzai, *supra* note 71, at 1478; Kerr, *supra* note 55, at 1146.

significant CFAA case, the Second Circuit referred repeatedly to the CFAA as punishing "trespass."[75]

Thus, it seems prudent to determine the CFAA's zone of interests by reference to trespass law.[76] Trespass law does not permit those storing property in a place to bring suit for trespass; only the "possessor" of the land may bring suit.[77] This makes sense because trespass violates the possessor's right to quiet enjoyment in their land. By the same token, cyber-trespass violates the computer owner's right to quiet enjoyment, requiring that they expend money, time, and stress expelling the invaders and barricading against their repeated entry. Therefore, it seems questionable to extend the CFAA's zone of interests to those that do not own the server, do not lease it, do not grant or restrict access to it, and are not responsible for preventing or remediating attacks.

2. Proximate Cause

For determining statutory standing, proximate cause operates similarly to its operation in tort. There it has been called "a well established principle of [the common] law, that in all cases of loss we are to attribute it to the proximate cause, and not to any remote cause."[78] Proximate cause "excludes only those 'link[s] that [are] too remote, purely contingent, or indirect.'"[79] Remoteness and directness require a particular examination here.

Considering remoteness, the proximate cause inquiry turns principally on foreseeability: Could a reasonable tortfeasor have expected the damage and resultant liability that occurred from their conduct?[80] Here, the CFAA neatly demonstrates the difference between the "zone of interests" test and the proximate cause analysis. As a cyber-trespass statute, the CFAA deters breaching and damaging computer systems. But although the zone of interests extends to the servers themselves, certainly accessing and damaging documents on those servers was foreseeable.

[75] *See* United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991).

[76] *See, e.g.*, Michael J. O'Connor, *The Common Law of Cyber-Trespass*, 85 BROOK. L. REV. 421 (2020) (applying trespass law to resolve open questions in CFAA interpretation); Goldfoot & Bamzai, *supra* note 71, at 1478 (advocating incorporating trespass standards into CFAA interpretation).

[77] *See, e.g.*, Beach St. Corp. v. A.P. Constr. Co., 658 A.2d 379, 380 (Pa. Super. Ct. 1995) ("It is well-settled that any right to sue for the trespass belongs solely to the possessor at the time of the trespass[.]"); Smith v. Cap Concrete, Inc., 184 Cal. Rptr. 308, 310 (Cal. Ct. App. 1982) ("The proper plaintiff in an action for trespass to real property is the person in actual possession; no averment or showing of title is necessary.").

[78] Waters v. Merchants' Louisville Ins. Co., 36 U.S. (11 Pet.) 213, 223 (1837).

[79] Staub v. Proctor Hosp., 562 U.S. 411, 419 (2011) (quoting Hemi Grp., LLC v. City of New York, 559 U.S. 1, 9 (2010)).

[80] *See, e.g.*, Webb v. Jarvis, 575 N.E.2d 992, 997 (Ind. 1991) ("[Proximate cause] seek[s] to find what consequences of the [alleged] conduct should have been foreseen by the actor who engaged in it.").

But when we consider derivative protection, the picture gets murkier. Recall that the plaintiff's injury in the *Theofel* context stems from documents read or damaged by third parties. But the plaintiff brings a cause of action not for trade secret theft or any other cause that vindicates the plaintiff's rights in those documents themselves. Rather, the documents are merely the damage that permits the plaintiff to protect the server owner's property rights. Proximate cause suggests that this might be "purely derivative of 'misfortunes visited upon a third person by the defendant's acts.'"[81]

Our conclusion is thus somewhat muddled. The CFAA's plain language is deceptively expansive, promising recompense to anyone damaged by violations. But the zone-of-interests test suggests that Congress intended to protect system owners from cyber-trespass, not data owners from trade secret theft (which was already universally protected at the state level). Meanwhile, proximate causation suggests that the document owner's harm was foreseeable to the wrongdoer, but that the plaintiff's claim may derive from the system owner's.

There is another factor to consider. Recent case law questions whether digital privacy invasions cause harm at all. If merely "obtain[ing] . . . information"[82] causes no harm, then the Constitution interposes an obstacle. The federal courts cannot remedy injuries that do not exist.

IV. CONSTITUTIONAL STANDING

The federal judiciary does not offer advice.[83] Instead, the Constitution empowers it to decide "[c]ases" and "[c]ontroversies."[84] By including that constitutional requirement, the Framers made a practical and moral judgment about the "proper—and properly limited—role of the courts in a democratic society."[85] On the practical axis, directly impacted litigants can present a more complete factual picture to illuminate the legal issues.[86] On the moral axis, when courts can only resolve disputes between litigants with a direct stake in the outcome, this limitation blunts the courts' ability

[81] Lexmark Int'l, Inc. v. Static Control Components, Inc., 572 U.S. 118, 133 (quoting Holmes v. Sec. Inv'r Prot. Corp., 503 U.S. 258, 268–69 (1992)).

[82] Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(2) (2018).

[83] *See* Massachusetts v. EPA, 549 U.S. 497, 516 (2007) ("[N]o justiciable controversy exists when parties . . . ask for an advisory opinion[.]"); Clinton v. Jones, 520 U.S. 681, 700 (1997) ("[T]he judicial power to decide cases and controversies does not include the provision of purely advisory opinions to the Executive, or permit the federal courts to resolve nonjusticiable questions.").

[84] U.S. CONST. art III, § 2, cl. 1.

[85] Warth v. Seldin, 422 U.S. 490, 498 (1975).

[86] *See* Schlesinger v. Reservists Comm. to Stop the War, 418 U.S. 208, 220–21 (1974) ("Concrete injury . . . enables a complainant authoritatively to present to the court a complete perspective upon the adverse consequences flowing from the specific set of facts undergirding his grievance.").

to legislate by injunction.[87] Citizens with broad, abstract, or vague objections about the government's goals and operation can address their concerns to the representative branches. If those branches prove recalcitrant, citizens replace them every two, four, or six years.[88] If we change this essential allocation of power between the representative and the judicial branches, we risk diminishing both.[89]

A court therefore decides a dispute between parties. The court issues a judgment. Someone wins and someone loses. The court may award damages. It may issue an injunction. Regardless, the court resolves the parties' dispute and clarifies their rights and obligations going forward. The court's *opinion* is an extraneous adjunct to this process.[90] While useful for helping appellate courts determine whether the judgment was correct and for clarifying the law going forward, the opinion does not *do* anything. It explains why the *judgment* did the correct thing.

Constitutional standing emerges from these ideas. It says that a case or controversy cannot exist in a vacuum. Rather, it emerges from interactions between parties. Indeed, cases and controversies only exist in relation to those parties. For example, assume that John Smith believes Adam Brown stole his patented idea. John Smith has a dispute with Adam Brown, and Adam Brown has a dispute with John Smith. Assuming several other requirements get satisfied, a court could issue a judgment favoring one or the other. The court could resolve their case. But other than being annoyed by their dull, overused names, Hixby Higginbotham has no dispute with John Smith or Adam Brown. A case exists, but he plays no part in it.

[87] *See id.* ("To permit a complainant who has no concrete injury to require a court to rule on important constitutional issues in the abstract would . . . open the Judiciary to an arguable charge of providing 'government by injunction.'").

[88] *See* United States v. Richardson, 418 U.S. 166, 179 (1974) ("In a very real sense, the absence of any particular individual or class to litigate these claims gives support to the argument that the subject matter is committed to the surveillance of Congress, and ultimately to the political process. . . . The Constitution created a *representative* government with the representatives directly responsible to their constituents at stated periods of two, four, and six years; that the Constitution does not afford a judicial remedy does not, of course, completely disable the citizen[.]").

[89] *See id.* at 188–89 (1974) (Powell, J., concurring) ("Relaxation of standing requirements is directly related to the expansion of judicial power. . . . [R]epeated and essentially head-on confrontations between the life-tenured branch and the representative branches will not, in the long run, be beneficial to either. The public confidence essential to the former and the vitality critical to the latter may well erode if we do not exercise self-restraint in the utilization of our power to negative the actions of the other branches. We should be ever mindful of the contradictions that would arise if a democracy were to permit general oversight of the elected branches of government by a nonrepresentative, and in large measure insulated, judicial branch.").

[90] *See Warth*, 422 U.S. at 499 ("The Art. III judicial power exists only to redress or otherwise to protect against injury to the complaining party, even though the court's judgment may benefit others collaterally.").

For that reason, constitutional standing demands three elements: (1) an injury to the party demanding redress; (2) a causal connection between the injury and the defendant's conduct; and (3) a likelihood that a favorable decision will redress the injury.[91] By no coincidence, even the simplest lawsuit has three actors: the injured plaintiff, the injuring defendant, and the court addressing the injury. Standing's three elements ensure that these three players have a sufficient connection to the dispute such that a case or controversy exists, not merely in the abstract, but regarding these specific actors.

A. Injury-in-Fact

The injury requirement ensures that the plaintiff bringing the claim has been wronged in such a way to give rise to a case or controversy.[92] The injury requirement itself has three sub-requirements. The injury must be "particularized."[93] It must be "concrete."[94] And it must be "actual or imminent, not 'conjectural' or 'hypothetical.'"[95] Particularization ensures that the harm "affect[s] the plaintiff in a personal and individual way."[96] It presents no serious obstacle to the CFAA fact patterns here, with plaintiffs alleging that breachers accessed their personal confidential information. But several courts have suggested that current data breach harms are not concrete and future data breach harms are solely hypothetical.

1. Present Injury

Injuries can be either tangible—like a rock dropping on one's head—or intangible—like a metaphorical rock dropping on one's head.[97] But standing permits only "concrete" harms.[98] Though all tangible harms are concrete, only some intangible harms will qualify. The concreteness analysis thus determines which metaphorical rocks still cause injury. This test has two strands: history and legislative choice.

The historical analysis looks to similar claims that have been traditionally accepted in English and American common law.[99] Where an injury has been long recognized, the courts will continue to offer standing

[91] *See* Lewis v. Alexander, 685 F.3d 325, 338 (3d Cir. 2012) (citing Lujan v. Defenders of Wildlife, 504 U.S. 555, 560 (1992)).

[92] *See Warth*, 422 U.S. at 502 ("Petitioners must allege and show that they personally have been injured.").

[93] *Lujan*, 504 U.S. at 560.

[94] *Id.*

[95] *Id.*

[96] *Id.* at 560 n.1.

[97] *See, e.g.*, Stanley Ingber, *Rethinking Intangible Injuries: A Focus on Remedy*, 73 CAL. L. REV. 772, 774 (1985) ("[T]he term 'intangible injuries' most often is used to refer to nonphysical injuries[.]").

[98] *Lujan*, 504 U.S. at 560.

[99] Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1549 (2016).

for that injury. The legislature may still remove legal redress for the injury, but the injury exists nonetheless. For example, consider adultery, which has largely ceased to support a civil claim,[100] but creates unquestionable harm. If a plaintiff brought a claim for adultery, the court could not dismiss it for lack of standing, but could dismiss it for failure to state a claim.

Legislative enactments granting rights are "instructive and important," but they do not mean "that a plaintiff automatically satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right."[101]

To apply these tests, it is helpful to divide the field into three partitions: definite injury, possible injury, and no injury. If common law has traditionally recognized a cause of action, then it is a definite injury. If neither the common law nor common sense recognize a cause of action, then it is definitely *not* an injury, even if the legislature says it is. If the common law has not traditionally recognized a cause, but recognizes similar causes of action, then it is a possible injury. When common law causes of action harmonize with statutory causes of action, even if they do not align precisely, courts seem particularly likely to find an injury-in-fact.[102] The common law history demonstrates that a type of harm exists, though congressional action recognizes or respects a new aspect of it.

Applying these considerations to intrusions on confidential information, we find ample support in both history and statute for protecting privacy rights.

On the historical front, privacy invasions have been broadly accepted as a basis for civil suit for more than a hundred years. Though privacy protections have ancient roots in property and tort law, recognition of their importance in and of themselves has usually been traced to Samuel Warren and Louis Brandeis's seminal article *The Right to Privacy*.[103] In that article, Warren and Brandeis articulated the fundamental idea that privacy was worth protecting.[104] From that central idea, privacy torts developed,

[100] *See* Joanna L. Grossman & Lawrence M. Friedman, *Elizabeth Edwards v. Andrew Young: Can He Be Held Liable for Contributing to the Failure of the Edwardses' Marriage?*, (Feb. 19, 2010), https://bit.ly/3bwiYY2 ("[O]ver the course of the Twentieth Century, heart-balm laws were abolished virtually everywhere in America.").

[101] *Spokeo*, 136 S. Ct. at 1549; *see also* Warth v. Seldin, 422 U.S. 490, 500 (1975).

[102] *See* Robins v. Spokeo, Inc., 867 F.3d 1108, 1115 (9th Cir. 2017) ("Even if there are differences between FCRA's cause of action and those recognized at common law, the relevant point is that Congress has chosen to protect against a harm that is at least closely similar *in kind* to others that have traditionally served as the basis for lawsuit.").

[103] *See* Louis D. Brandeis & Samuel D. Warren, *The Right to Privacy*, 4 HARV. L. REV. 193, 220 (1890).

[104] *See id.* at 196 ("[T]he question whether our law will recognize and protect the right to privacy in this and in other respects must soon come before our courts for consideration. Of the desirability—indeed of the necessity—of some such protection, there can, it is believed, be no doubt.").

courts and legislatures accepted them, and eventually, Professor William Prosser recognized them as a distinct group. Prosser identified actions for intrusion upon seclusion, public disclosure of private facts, publicity which places the plaintiff in a false light, and appropriation of name or likeness.[105] In addition to Prosser's recognized torts, other confidentiality protections have long received protection, like trade secret law.[106]

The common law does not recognize a tort for reading a person's private documents held by another, but it does recognize adjacent torts for privacy violations. With the general category having several accepted injuries, legislative judgment plays a particularly important role in recognizing new injuries with the same basic character. On the legislative front, Congress determined in the CFAA to extend both criminal and civil liability merely for reading data that was accessed without authorization.[107] Additionally, both Congress and state legislatures have extended trade secret protection and liability for Prosser's privacy torts.

And yet the courts addressing the issue have frequently determined that a data breach standing alone does not create a present harm. They point to various reasons for this conclusion. Some courts note that the states generally eschew a personal right of action for data breaches, instead permitting enforcement only by the state attorney general.[108] Others point to a requirement to demonstrate actual damages, as opposed to a bare statutory violation.[109] (Of course, if a plaintiff can demonstrate actual damages independent of the claimed statutory violation, then they have an injury-in-fact.) Courts have likewise rejected secondary effects like emotional upset and fear of identity theft and fraud.[110]

Thus, it seems that injury-in-fact for the person storing data on a system should turn on the data's nature. If a third party surreptitiously reads my high school book report, it might cause me to cringe, but it would

[105] *See* William L. Prosser, *Privacy*, 48 CALIF. L. REV. 383, 389 (1960).

[106] *See* Board of Trade of Chicago v. Christie Grain & Stock Co., 198 U.S. 236, 250 (1905) ("[P]laintiff's collection of quotations is entitled to the protection of the law. It stands like a trade secret. Plaintiff is entitled to keep the work which it has done, or paid for doing, to itself.").

[107] *See* S. REP. NO. 99-432, at 6, as *reprinted in* 1986 U.S.C.C.A.N. 2479, 2484 (explaining that "obtaining information" in statute included "mere observation of the data"); Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 121 F. Supp. 2d 1255, 1276 (N.D. Iowa 2000).

[108] *See, e.g.*, Pisciotta v. Old Nat'l Bancorp, 499 F.3d 629, 637 (7th Cir. 2007) (pointing to the Attorney General enforcement provision from Indiana's data breach law as evidence that no compensable injury occurred).

[109] *See* Remijas v. Neiman Marcus Grp., LLC, 794 F.3d 688, 695 (7th Cir. 2015).

[110] *See* Beck v. McDonald, 848 F.3d 262, 272 (4th Cir. 2017) ("We also reject the Plaintiffs' claim that 'emotional upset' and 'fear [of] identity theft and financial fraud' resulting from the data breaches are 'adverse effects' sufficient to confer Article III standing."). *But see* Krottner v. Starbucks Corp., 628 F.3d 1139, 1143 (9th Cir. 2010) (concluding that a plaintiff who alleged "generalized anxiety and stress" after a data breach had claimed sufficient injury to confer standing).

cause insufficient harm to enable me to sue. On the other hand, if a third party read and threatened to disseminate my confidential business plan, it would cause me less embarrassment than having my adolescent writing exposed to the world, but it would cause the right type of harm to enable me to sue. But that presents a relatively immediate harm, a direct threat that would damage me economically. What if the perpetrator downloaded significant quantities of data, with my business plan being only one small piece, and he has made no threats? Then we have a potential future injury.

2. Future Injury

In future harm cases, the plaintiff alleges that the defendant's actions make it likely that something terrible will befall the plaintiff in the future. The Supreme Court has explained that either a "substantial risk"[111] of injury or a "certainly impending" injury has sufficient concreteness to support federal standing.[112]

In data breach cases, plaintiffs frequently claim that the impending future harm of identity theft confers standing. But the courts are split. Some say that the data breach itself provides sufficient risk for future identity theft to confer standing.[113] As the Seventh Circuit put it: "Why else would hackers break into a store's database and steal consumers' private information?"[114] Other courts believe that finding impending harm here requires assuming that the thief targeted personal data, selected the specific plaintiff's personal data, and can use that data successfully for identity theft.[115] These courts conclude that *Clapper v. Amnesty International USA* forecloses this "attenuated chain."[116] When the plaintiff brings CFAA claims rooted in future rather than present harm, it seems likely that courts will split along the same lines.

[111] Susan B. Anthony List v. Driehaus, 134 S. Ct. 2334, 2341 (2014) ("An allegation of future injury may suffice if the threatened injury is 'certainly impending,' or if there is a 'substantial risk' that the harm will occur."); Clapper v. Amnesty Int'l USA, 133 S. Ct. 1138, 1150 n.5 (2013) ("Our cases do not uniformly require that it is literally certain that the harms they identify will come about. In some instances, we have found standing based on a 'substantial risk' that the harm will occur, which may prompt plaintiffs to reasonably incur costs to mitigate or avoid that harm."); *see also* Attias v. Carefirst, 865 F.3d 620, 627 (D.C. Cir. 2017) ("In *Susan B. Anthony List v. Driehaus*, the Court clarified that a plaintiff can establish standing by satisfying *either* the 'certainly impending' test or the 'substantial risk' test. *See* 134 S. Ct. at 2341.").

[112] *Clapper*, 133 S. Ct. at 1143. The Court also held that unless the future harm was "certainly impending," plaintiffs could not manufacture standing by spending on goods and services to avoid the hypothetical future harm. *Id.*

[113] *See, e.g.*, *Attias*, 865 F.3d at 629; *Remijas*, 794 F.3d at 693.

[114] *Remijas*, 794 F.3d at 693.

[115] *See* Beck v. McDonald, 848 F.3d 262, 275 (4th Cir. 2017); Reilly v. Ceridian Corp., 664 F.3d 38, 42 (3d Cir. 2011).

[116] *Beck*, 848 F.3d at 275.

B. Causation

The causation requirement ensures that the defendant accused of causing the injury has wronged the plaintiff in such a way to give rise to a case or controversy *between the plaintiff and the defendant*.[117] Causation problems arise when too many speculative steps intervene between the defendant's actions and the plaintiff's harm. For example, in *Simon v. Eastern Kentucky Welfare Rights Organization*, the plaintiffs claimed that changing IRS rulings allowed hospitals to refuse indigent patients.[118] On that basis, indigent patient plaintiffs and their community organizations sued the IRS.[119] The Court concluded that the plaintiffs' injury was not fairly traceable to the IRS, offering two reasons. First, changing the tax rules may or may not have induced hospitals to stop taking indigent patients.[120] Second, changing the rules back may or may not cause hospitals to start taking indigent patients.[121]

Causation concerns should not normally impede a CFAA claim. To the extent an injury exists, it arises from the violator accessing confidential documents. No speculative causal chain or intervening decisionmaker arises from the facts.

C. Redressability

Redressability ensures that the court examining the case or controversy can materially resolve the plaintiff's injury.[122] Redressability concerns usually arise in two circumstances.

First, where an independent cause will continue inflicting a plaintiff's injury even after the case resolves, the court cannot redress the plaintiff's injury. For example, in *Harp Advertising Ill. Inc. v. Village of Chicago Ridge*, the plaintiff wanted to erect a sign that violated multiple local ordinances.[123] The plaintiff unwisely challenged the constitutionality of

[117] *See, e.g.*, Spokeo, Inc. v. Robins, 136 S. Ct. 1540, 1547 (2016) (the injury must be "fairly traceable to the challenged conduct of the defendant").

[118] *See* Simon v. E. Ky. Welfare Rights Org., 426 U.S. 26, 28–33 (1976).

[119] *See id.* at 28.

[120] *See id.* at 42–43 ("It is purely speculative whether the denials of service specified in the complaint fairly can be traced to petitioners' 'encouragement' or instead result from decisions made by the hospitals without regard to the tax implications.").

[121] *See id.* at 43 ("It is equally speculative whether the desired exercise of the court's remedial powers in this suit would result in the availability to respondents of such services. So far as the complaint sheds light, it is just as plausible that the hospitals to which respondents may apply for service would elect to forgo favorable tax treatment to avoid the undetermined financial drain of an increase in the level of uncompensated services."). While similar to the causation analysis, this actually seems to sound in redressability.

[122] *See* Steel Co. v. Citizens for a Better Env't, 523 U.S. 83, 103 (1998) ("And third, there must be redressability—a likelihood that the requested relief will redress the alleged injury.").

[123] *See* Harp Advert. Ill. Inc. v. Vill. of Chi. Ridge, 9 F.3d 1290, 1291 (7th Cir. 1993).

some, but not all, these ordinances. The Seventh Circuit explained that this prevented the federal courts from offering the plaintiff, Harp Advertising, any redress for its injury: "Harp suffers an injury (it can't erect the proposed billboard), but winning the case will not alter that situation."[124]

Second, where satisfaction will not flow to the plaintiff, the court cannot redress the plaintiff's injuries. For example, in *Steel Co. v. Citizens for a Better Environment*, the Supreme Court held that a citizens' group could not obtain redress for an environmental reporting violation.[125] The defendant had fixed its reporting violations before the suit was filed and seemed unlikely to re-offend.[126] The Court held that injunctive relief could not resolve a non-existent problem.[127] Meanwhile, damages under the relevant statute were payable only to the U.S. Treasury, and therefore would not remediate the plaintiff's injury.[128]

The CFAA raises neither redressability concern. It provides for civil damages to the complainant.[129] While a plaintiff cannot force the defendant to un-read its confidential documents, the plaintiff can punish the defendant's transgression.

V. CLARIFYING THE AMBIGUITY

The CFAA has a tension at its core. It is fundamentally a cyber-trespass law, but liability often triggers not when an attacker breaks in, but when that attacker obtains information from the breached system.[130] This creates substantial confusion. System owners grant or withhold authorization to access systems. System owners are the gatekeepers. And often system owners are the victims. Whenever a bad actor targets company secrets on company servers, the CFAA's concepts of access, authorization, and harm align.

But when bad actors target a server to steal a third party's confidential documents, these concepts clash. *Theofel v. Farey-Jones*[131] and other current case law grant standing to the third party. But these cases never acknowledge that the third party has no authority under the CFAA to withhold authorization to access the documents. Nor, surprisingly, does the third party have the authority to *grant* authorization, even to access its own documents. Only the system owner has that power. At a minimum,

[124] *Id.* at 1292.

[125] *See Steel Co.*, 523 U.S. at 87–88, 109–10.

[126] *See id.* at 87–88, 108.

[127] *See id.* at 108–09.

[128] *See id.* at 106.

[129] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g) (2018) ("Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief.").

[130] *See supra* notes 16–19.

[131] Theofel v. Farey-Jones, 341 F.3d 978, 981 (9th Cir. 2003).

this creates strange tensions within the statute. When recast into a standing inquiry, these tensions raise real questions about the scope of victims Congress intended to benefit with the CFAA. Congress could prudently clarify the ambiguity, either removing third-party standing or more fully embracing digital ownership.

The simplest route would have Congress definitively foreclose third-party standing. The CFAA would revert to its intended role as a cyber-trespass law. To accomplish this, Congress need only alter a few words in the statute. The civil action provision currently says: "Any person who suffers damage or loss by reason of a violation . . . ."[132] Congress could instead say: "Any person who controls authorization and suffers damage or loss by reason of a violation . . . ." This modification would prevent third parties from bringing CFAA claims. Third parties would remain free to invoke federal trade secret law or state causes of action *if* they qualify for them.[133] But third parties would no longer have an easy claim when a hacker breaks into a system the third party does not even own.

Alternatively, Congress could move fully toward protecting digital ownership. Both Congress and the states have been inching in this direction. In 2016 Congress nationalized trade secret protection for the first time.[134] The states have also moved to stronger privacy protections.[135]

But embracing broad federal privacy protections would require massively overhauling existing law. Congress would need to consider which documents were sufficiently confidential to require protection. For example, it would need to evaluate the traditional privacy torts and determine how this new legislation interfaced with existing trade secret protections. But each step carries risks. To effect its purpose, Congress may need to define property rights. This role traditionally belongs to the States, with Congress legislating on top of those existing definitions.[136] By imposing a blanket federal standard on a quickly evolving field, Congress could hamstring innovation and inhibit individuals and companies from voting with their feet. If Congress embraces the same access and authorization structure from the current CFAA, it would need to clarify what is being accessed and who can authorize it. The fact that Congress did none of this in the current CFAA raises further questions about the broad third-party standing that courts have thus far granted.

[132] Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g) (2018).

[133] Litigants are not shy about bringing such claims alongside CFAA violations. *See* Jonathan Mayer, *Cybercrime Litigation*, 164 U. PA. L. REV. 1453, 1489 (2016) (detailing frequency of co-claims in CFAA litigation).

[134] *See* Defend Trade Secrets Act of 2016, Pub. L. No. 114-153, 130 Stat. 376 (2016).

[135] *See, e.g.*, California Consumer Privacy Act, Cal. Civ. Code 1798.100 (2019).

[136] *Cf.* Lewis v. Alexander, 685 F.3d 325, 347 (3d Cir. 2012) ("Congress did not pass a federal body of trust law, estate law, or property law when enacting Medicaid. It relied and continues to rely on state laws governing such issues.").

VI. CONCLUSION

Third-party standing under the CFAA creates a bizarre situation. System owners authorize (or decline to authorize) users. Current case law says that if a hacker intrudes on the system, anyone storing a document there—any employee, any vendor, any customer, any user—may have a cause of action. But a party's interest in protecting confidential documents falls well outside the zone of interests that the CFAA protects. Taken to the extreme, with non-confidential documents, or confidential documents that a hacker may only discover after wading through a deep haystack, even the Constitution may not recognize an injury. Due to the disconnect between the system (which suffered the intrusion) and the actual claimed damage (viewing confidential files), CFAA cases with third-party standing may further contort the law on access and authorization. Regardless of whether Congress decides to broadly protect digital ownership—though that seems unlikely and perhaps unwise—Congress should clarify that the CFAA does not grant third-party standing.