WHEN CIRCUIT BREAKERS TRIP: RESETTING THE CFAA TO COMBAT ROGUE EMPLOYEE ACCESS

Obie Okuh[*]

TABLE OF CONTENTS

ABSTRACT

This article focuses on the narrow question of whether the

[*] Obiajulu Charles Okuh, JD, Case Western Reserve University School of Law, 2011. Professor Jacqueline Lipton provided helpful comments. Sarah E. Greenlee provided constructive criticism.

Computer Fraud & Abuse Act (18 U.S.C. § 1030 et. seq) should be available to a private-sector employer as a vehicle to litigate classic employee business information theft, sabotage, economic espionage or misappropriation cases when such employee's conduct does not result in damage to the employer's electronic system, a computer's circuitry or programming, or interruption of service. The current circuit split regarding the construction and application of the CFAA's access authorization provisions to employment cases has meant that an employer's likely recovery under the statute depends in most instances upon factors external to the employee's alleged conduct and more on whether and to what extent the court in a particular jurisdiction is willing to voyage into the subjective mindset of the employee during the alleged conduct.

After examining the legislative history of the CFAA, this article argues that the original intent of Congress was to target outside hackers, and employees of the company were not originally contemplated within the reach of the statute. However, as computer crimes became more sophisticated, Congress took steps to increase protection for owners of commercial information by factoring employee access into the CFAA provisions, albeit without crafting the amendments properly. Further, the article explains the theoretical underpinnings of the circuit split and argues that the split reflects divergent views on how to apply theories of contract, agency, and code-based approaches to the concept of "authorization" within the cyber security and computer information system context. While proffering a draft amendment to the statute, this article concludes by urging law makers or courts to 1) eliminate or exempt the "exceeding authorization" analysis when applying the statute to classic employee misappropriation cases; 2) end inquiries that focus on the employee's subjective intent at the time of the access or the employee's subsequent use of the information obtained; and 3) focus strictly on the unauthorized nature of the employee's intrusion upon the employer's protected computer information – Under this approach, the employer's inability to prove an employee's breach of explicit contractual prohibition or a trespass of system code would constitute an automatic bar to recovery under the statute.

I. INTRODUCTION

Tales of the recalcitrant, wild-eyed, often disgruntled or merely

curious employee who decides to peer into the employer's computer information are hardly uncommon scenarios.[1] Suppose, however, that a departing employee uses the same username and password combination issued to the employee by the employer to login and review or retrieve information stored on the company's network prior to retiring or joining a competitor and the employer sues claiming a violation of the federal Computer Fraud and Abuse Act ("CFAA").[2] Under such circumstances, *should* the employer be able to recover?[3]

Employer recovery under the CFAA currently depends on the specific jurisdiction where the parties are located or which the employer chooses and is able to bring suit. This is both unfortunate[4] and a direct consequence of the circuit split

[1] Brian H. Corcoran, *The Computer Fraud and Abuse Act: "Hacker Repellent" That Works Great on Ex-Employees, Too*, 7 No. 1 CYBERSPACE LAW. 2 (2002) (noting that this scenario is so common that it is frequently the subject of big screen thrillers).

[2] 18 U.S.C. § 1030 (2006). The CFAA is a federal criminal statute that prohibits the unauthorized *access into protected computers* or conduct that actually damaged a computer's circuitry or programming, and permits a party that suffers damage or loss by reason of a violation of the CFAA to maintain a civil action against the violator for damages and injunctive relief under subsection § 1030(g). *Id.* It did not originally reach harms caused by methods other than unauthorized access. *See generally,* Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (*18 U.S.C.A. § 1030), 174 A.L.R. FED. 101, § 2[a] (2001) (recalling, for example, that the statute provided only criminal penalties until the 1994 amendment when Congress added civil penalties in § 1030(g)).

[3] Note that the CFAA is merely one of several causes of action available to the employer. Employers can bring suit for violation of any of the following statutes: State Trade Secret Act (Massachusetts, New Jersey, New York, Pennsylvania, Tennessee, Texas and Wyoming are the only states to not adopt the Uniform Trade Secret Act and they follow their own state statutes or common law, *see generally, The Uniform Trade Secrets Act State (UTSA),* NDAS FOR FREE, http://www.ndasforfree.com/UTSA.html (last visited Feb. 4, 2011)); Digital Millennium Copyright Act, Pub. L. No. 105-304, 112 Stat. 2860 (codified as amended in scattered sections of 17 U.S.C.) (2006); Stored Wire and Electronic Communications and Transactional Records Access, 18 U.S.C. §§ 2701-2712 (2006); Wire and Electronic Communications Interception and Interception of Oral Communications, 18 U.S.C. § 2510-2522 (2006); etc. An employer may also bring suit for Unfair Competition, Breach of Fiduciary Duty Breach of Contract, Tortious Interference with Business Interest, traditional trespass claims, etc.

[4] *See, e.g.,* Roger J. Miner, *Federal Court Reform Should Start at the Top*, 77 JUDICATURE 104, 106–07 (1993) (noting that "circuit conflicts [generate] litigation, because the law remains unsettled, and attorneys take their cases to the forum most favorable . . . . Clients doing business nationally may have their conduct regulated one way in one place and another way in another and continue to challenge unfavorable precedent. Government agencies, charged

regarding the construction and application of the CFAA's access authorization provisions to employment cases.[5] Neither Congress[6] nor the Supreme Court has articulated yet the circumstance under which an employee's conduct could exceed prior authorized access.[7] Yet the gravamen of CFAA pleadings is a plaintiff's proof that a defendant's access was unauthorized or was in excess of authorization.[8]

Unauthorized access to computer information systems poses significant costs to owners and society at large.[9] Unauthorized

with the administration of national law in a uniform way, follow policies of non-acquiescence, refusing to accept the views of a circuit that rejects the agency position. Aside from the fact that fairness is lost and justice is not seen to be done, the lower courts become clogged with cases that would not be brought if the law was clearly stated.").

[5] Condux Int'l Inc. v. Haugum, No. 08-4824, 2008 WL 5244818, at *3 (D. Minn. Dec. 15, 2008) (collecting cases and acknowledging that the federal courts have yet to decide the issue of which violations of the subsections of the CFAA may support a civil action in the first place). For more on what parts of the CFAA may or may not support a civil cause of action, see Richard Warner, *The Employer's New Weapon: Employee Liability Under the Computer Fraud and Abuse Act*, 12 EMP. RTS. & EMP. POL'Y J. 11, 14 (2008) ("Questions arise because employers typically cannot successfully sue under §§ 1030(a)(2) & 1030(a)(4), which apply to both 'unauthorized access,' and 'exceeding authorized access.' The problem is that those sections require an intent to defraud, and employees who abscond with trade secrets arguably do not fulfill that intent requirement. Employers typically resort to § 1030(a)(5) which has no such requirement. § 1030(a)(5), however, applies only when the person accessing the computer does so 'without authorization.' The problem is that an employee typically has permission to access the employer's computers, so the employee is arguably 'authorized' to do so . . . .").

[6] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 (1st Cir. 2001) (noting in dicta that the term "without authorization" is not defined in the Act and one court found its meaning "to be elusive.") (internal citations omitted); George Roach & William J. Michiels, *Damages is the Gatekeeper Issue for Federal Computer Fraud*, 8 TUL. J. TECH & INTELL. PROP. 61, 62 (2006) (explaining that Congress had two conflicting priorities resulting in a compromise that continues to be problematic: discouraging significant damage to hardware or data files and wanting to avoid criminalizing or overreacting to some insignificant activity).

[7] *See* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. Rev. 1596, 1596 (2003) (discussing the mystery of unauthorized access and noting that despite popular aspirations for regulations to be clear, this is not so with statutes regulating computer crimes).

[8] Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 495 (D. Md. 2005) ("A prerequisite to liability under both the SECA and the CFAA is that the alleged violator has accessed the computer either without authorization, or in excess of authorization.").

[9] *See generally* John J. Falvey, Jr. & Amy McCallen, *Crimes Online:* § 26:6 *Intellectual Property Crimes, in* 2 INTERNET L. & PRAC. (West 2010) (noting that

access accounted for one of the top four most prevalent categories of threat incidences to computer systems reported in the decade-running annual *Computer Crime & Security Survey*.[10] Unauthorized access was the second-greatest source of financial loss to corporations behind virus attacks and ahead of losses related to laptop or related hardware theft and theft of proprietary information.[11] Besides financial losses, respondents to the *Global State of Information Security Survey* reported that unauthorized access to business information caused theft of intellectual property as well compromised brand or reputation.[12]

Fluctuations in federal courts' interpretation of the CFAA's access authorization jurisprudence[13] impede multistate employers' ability to formulate or implement firm-wide comprehensive CFAA policy. Meanwhile, various federal[14] and state[15] statutes require employers to promptly and publicly disclose any unauthorized access to certain types of commercial information to their clients and stakeholders.[16] As noted above,

the methods for stealing electronic trade secrets through unauthorized access of computers, hacking of computers, and destruction of data on computers are evolving at a rapid rate); Robert Mueller, Dir., FED. BUREAU OF INVESTIGATION, Address to the National Press Club Luncheon (June 20, 2003), *available at* http://www.fbi.gov/news/speeches/meeting-new-challenges (noting that U.S. businesses are losing more than $200 billion annually from theft of intellectual property).

[10] *See, e.g.,* Robert Richardson, *2008 CSI Computer Crime & SecuritySurvey*, COMPUTER SEC. INST., 14–15 (2008), http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf.

[11] Lawrence A. Gordon et al., 2006 *FBI/CSI Computer Crime and Security Survey*, COMPUTER SEC. INST., 10–14 (2006), http://i.cmpnet.com/gocsi/db_area/pdfs/fbi/FBI2006.pdf.

[12] PricewaterhouseCoopers et al., *The 2011 Global State of Information Security Survey*, PWC, 33 (2010), http://www.pwc.com/gx/en/information-security-survey/pdf/giss-2011-survey-report.pdf.

[13] *See generally* Miner, *supra* note 4, at 106–07 (showing the discrepancies between state and federal law and the "uncertainty of the law" established by the U.S. Supreme Court).

[14] *See* Christian S. Genetski, *Overview of Sources and Theories of Liability from Information Security Breaches*, 929 PLI/PAT 365, 369–80, 385–85 (2008) (discussing, among others, HIPAA, the Gramm-Leach-Bliley Act and Safeguards Rule, The Fair and Accurate Credit Transactions Act and Disposal Rule, The Federal Trade Commission Act, The Sarbanes-Oxley Act and theories of liability under contract, tort, and criminal law).

[15] *See e.g., 2006 Breach of Information Legislation*, NAT'L CONFERENCE OF STATE LEGISLATURES, http://www.ncsl.org/default.aspx?tabid=13488 (last updated Jan. 7, 2007) (listing and summarizing legislation from various states controlling information disclosure of business records and commercial information).

[16] *See* Warner, *supra* note 5, at 25–26 (noting that such notification can be

unauthorized access and the subsequent disclosure to the public expose owners to reputational, brand, and financial risks and liabilities.[17] Consequently, many organizations report that they sometimes do not disclose network intrusions and unauthorized access incidents to law enforcement because of the perception that the resulting negative publicity would hurt their organization's stock and/or image.[18] Nevertheless, employers want a private right of action for civil damages against computer

costly, and the cost of notification may not be recoverable under the CFAA because the contemplated costs recoverable under the CFAA appear to concern the analysis and restoration of the computer system, and not every jurisdiction considers lost business revenue or drops in stock price as covered loss under the statute).

[17] *See generally* Julia S. Cheney, *Heartland Payment Systems: Lessons Learned from a Data Breach*, Payment Cards Center Discussion Paper , FEDERAL RESERVE BANK PHILADELPHIA, 1–4, (Jan. 2010), http://www.philadelphiafed.org/payment-cards-center/publications/discussion-papers/2010/D-2010-January-Heartland-Payment-Systems.pdf (discussing solutions to the security problems involved with card payment systems). *See* also Robert McMillan, *After Google Hack, Warnings Surface in SEC Filings*, CSO (June 8, 2010), http://www.csoonline.com/article/596315/after-google-hack-warnings-surface-in-sec-filings (quoting Google's warning to its shareholders in its SEC filing that these types of unauthorized access breaches to its system may constitute material risk: "[o]utside parties may attempt to fraudulently induce employees, users, or customers to disclose sensitive information in order to gain access to our data or our users' or customers' data . . . . [Such unauthorized access poses serious risks] [b]ecause the techniques used to obtain unauthorized access, disable or degrade service, or sabotage systems change frequently and often are not recognized until launched against a target, we may be unable to anticipate these techniques or to implement adequate preventative measures . . . .). For example, in late 2008, Heartland Payment Systems was sued by shareholders for failing to disclose that the company's information systems had been accessed without authorization. *Id.* "[Shareholder-p]laintiffs argued that the company should have disclosed the incident in SEC filings and in calls with financial analysts." *Id.* The Heartland incident was eventually linked to the largest data breach in U.S. history. *Id.* Heartland's stock dropped nearly 80 percent when the company finally disclosed the full extent of the attack in January 2009 and the company ultimately lost 50 percent of its market capitalization and, as of August 2009, had spent more than $32 million on legal fees, forensic costs, reserves for potential card brand fines, and other related settlement costs. Cheney, *supra* at 18. Google, Intel, Symantec and Northrop Grumman have all started "adding new warnings to their U.S. Securities and Exchange Commission filings informing investors of the risks of computer attacks," including sabotage by insider employees. McMillan, *supra.*

[18] *See* Richardson, *supra* note 10, at 23 (noting the "interesting finding" that 22% of respondents "[d]id not believe that law enforcement could help in the matter."). *Cf.* PricewaterhouseCoopers et al., *supra* note 12, at 34 (finding a significant shift in organizational response to negative computer systems incident reporting channel away from the CIO in favor of the company's senior business decision-makers).

systems and network employee tortfeasors.[19] There is an urgent need, therefore, for a clearly defined regulatory and judicial CFAA framework.

As an initial matter, this article focuses on the narrow question of whether the CFAA should be available to a private-sector employer as a vehicle to litigate classic employee misappropriation cases when such employee's conduct does not result in damage to the employer's electronic system, computer's circuitry or programming or interruption of service—all of which are conduct expressly and appropriately outlawed by the CFAA.[20] This article begins in Part I with a background discussion of the legislative history of the CFAA, paying particular attention to amendments that apply to employment situations. The discussion shows that the original intent of Congress was to target legislation against outside hackers, and employees of the company were not originally contemplated within the reach of the statute. However, as computer crimes became more sophisticated, Congress took steps to increase protection for owners of commercial information by factoring employee access into the CFAA provisions, albeit without crafting the amendments properly.

Part II of this article outlines the circuit conflict and focuses on the seminal cases that define the split. While some courts—in the *Shurgard/Citrin*[21] line of cases—have applied an agency approach in finding a broad justification for applying the CFAA to employee misappropriation cases, other courts have rejected the suitability of agency doctrine as basis for extending the

[19] *See, e.g.*, Condux Int'l Inc. v. Haugum, No. 08-4824, 2008 WL 5244818, at *1 (D. Minn. Dec. 15, 2008) (dismissing a claim by a former employer against a former employee who allegedly wrongfully obtained and attempted to distribute confidential business information).

[20] § 1030(a)(5) criminalizes all computer damage done by outsiders, as well as intentional damage by insiders, albeit at different levels of severity. It is, however, the intentional act of trespass that makes the conduct criminal. To provide otherwise is to openly invite hackers to break into computer systems, safe in the knowledge that no matter how much damage they cause, they commit no crime unless that damage was either intentional or reckless. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, THE NATIONAL INFORMATION INFRASTRUCTURE PROTECTION ACT OF 1996: LEGISLATIVE ANALYSIS, § III(E), *available at* http://www.justice.gov/criminal/cybercrime/1030analysis.html.

[21] Shurgard Storage Ctrs. Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1122, 1125 (W.D. Wash. 2000); Int'l Airports Ctrs, L.L.C. v. Citrin, 440 F.3d 418, 419–21 (7th Cir. 2006).

statute, agreeing instead with the *Lockheed*[22] court that the subjective intent of the employee is an insufficient basis to defeat an authorization that preexisted the access in controversy. *Lockheed* cases evidence an emerging trend that narrowly construes the reach of the CFAA such that an employee's subsequent misuse of information acquired under authorization is not actionable under the statute.[23] Further, the article explains the theoretical motivations for the disagreement and argues that the split reflects divergent views on how to distinguish "authorization" within the cyber security and computer information system context.

In Part III, the article exposes a lack of plausible basis for continuing the division between radically different CFAA access authorization jurisprudence; hence, urging savvy lawmakers or the judiciary[24] to consider narrowing the scope of the statute when the situation typifies a misappropriation claim by an employee with prior authorization. Specifically, the article proposes 1) eliminating the "exceeding authorization" analysis for employee CFAA cases regardless of the provision's textual presence in the statute; 2) ending inquiries that focus on the employee's subjective intent at the time of the access or subsequent use of the information obtained; and 3) focusing strictly on the unauthorized nature of the employee's intrusion upon the employer's protected computer information and requiring the employer to prove a breach of explicit contractual prohibition or a trespass of system code by the employee. This latter reform is significant given as the CFAA currently "contains absolutely no requirement that data be secured and rendered inaccessible to unauthorized users to enjoy the protection of the statute."[25]

---

[22] Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *6–8 (M.D. Fla. Aug.1, 2006).

[23] *See e.g.* ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp 2d 605, 610, 616 (M.D. Tenn. 2010) (construing the statute narrowly).

[24] Courts have broad grant of discretion by Congress to interpret the CFAA. *See* Katherine M. Field, Note, *Agency, Code or Contract: Determining Employee's Authorization under the Computer Fraud and Abuse Act,* 107 MICH. L. REV. 819, 821–22 (2008).

[25] Beryl A. Howell, *Real World Problems of Virtual Crime*, 7 YALE J. L. & TECH. 103, 108, 122 (2005). In effect, this article argues that a showing of some objective restriction on employee's access be made by the employer in the form of codes such as usernames and passwords or contract specifically addressing the nature of authorized use. This kind of showing is obviously not necessary for outside hacker cases, since outsiders are not presumed to have authorization

II. EVOLUTION OF THE CFAA

Understanding how the CFAA has evolved is useful not only for identifying the specific harm that Congress sought to remedy when it enacted and amended the statute, but also the statute's history serves to highlight junctures where congressional action or judicial intervention may have forced the statute to evolve in the manner that have resulted in its current form. To safeguard civil liberties and privacy as well as make clear to people the boundary of legally permissible conduct, a statute's reach should be constrained to reach no more than the specific harm that the legislature intended to combat.[26] Unauthorized access, as a subset of various threats to computer network security, should be met with a different response than required for other forms of threats.[27]

A. Legislative History of the CFAA

Congress intended, with the CFAA, to combat then-emerging computer torts such as hacking,[28] denial of service attacks,[29] and distributing worms and viruses, which have the practical effect of

to access employer computer networks or information.

[26] *See id*. at 104–05 (noting that in the specific case of cyber security, policy makers should narrow and circumscribe law to address clearly defined problems in order to "minimize the risk of an overly expansive law that could chill innovation and technological development"); Jennifer A. Chandler, *Security in Cyberspace: Combating Distributed Denial of Service Attacks*, 1 U. OTTAWA L. & TECH. J. 231, 233 (2004) ("[L]egal policy analysis [in the group problems within cyber security] must begin by identifying the particular problem to be considered.").

[27] Chandler, *supra* note 26, at 233–35 (noting that owner's negligence or outsider denial of service attacks, for example, should be met with different sorts of legislation because the nature of the threats and the motivation of the perpetrators vary).

[28] *See also* Mary M. Calkins, Note, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 GEO. L.J. 171, 172 (2000). "Hacking" or "cracking" is the umbrella term for the act of "gaining unauthorized access to another network, computer system, or files." Keith J. Epstein & Bill Tancer, *Enforcement of Use Limitations by Internet Service Providers: "How to Stop that Hacker, Cracker, Spammer, Spoofer, Flamer, Bomber,"* 19 HASTINGS COMM. & ENT. L.J. 661, 669 (1997). Cracking refers specifically to the act of "breaking password protection on a network, computer system, or files." *Id.*

[29] "A [denial of service attack] is an attack that seeks to disable the target so that it no longer is able to offer the services it normally provides. In the usual internet scenario, a denial of service attack is an attack in which a server is deliberately sent a large volume of communications traffic that overwhelms it and causes it to crash." Chandler, *supra* note 26, at 236.

interrupting services and information flow in the stream of commerce.[30] Congress enacted the Counterfeit Access Device and Computer Fraud and Abuse Act of 1984,[31] the CFAA precursor, in part due to the notoriety given to hackers in the 1983 classic film *War Games*.[32] In *War Games*, an outsider teenage "computer whiz hack[ed] into a North American Aerospace Defense Command (NORAD) computer at Los Alamos and, thinking he was playing a computer game, nearly started a freighting global thermonuclear war."[33]

Hacking "includes, for instance, breaking passwords; creating 'logic bombs;' e-mail bombs; denial of service attacks; writing and releasing viruses and worms; viewing restricted, electronically-stored information owned by others; URL redirection; adulterating Web sites; *or any other behavior that involves accessing a computing system without appropriate authorization*."[34] The Act was not intended to combat traditional torts such as fraud schemes perpetrated by means of the internet, internet gambling, online distribution of prohibited paraphernalia, cyberstalking,[35] or harms caused by other methods other than unauthorized access.[36] The CFAA was originally intended to protect covered computers[37] from criminal hacking by outsiders and to prevent conduct that actually "'damaged' a computer's circuitry or programming."[38] Notwithstanding these intended exclusions, however, most employees who are sued by their former employers under the

[30] Field, *supra* note 24, at 835–36 (citing several sources and explaining that "the CFAA was originally conceived as a specific response to the growing concern of computer-misuse crimes rather than traditional crimes").

[31] 18 U.S.C. § 1030 (2006).

[32] Peter T. Leeson & Christopher J. Coyne, *The Economics of Computer Hacking*, 1 J.L. ECON. & POL'Y 511, 513 (2005). Calkins, *supra* note 28, at 175, 179.

[33] Calkins, *supra* note 28, at 175, 179 ("In the wake of *War Games*, Congress criminalized unauthorized computer use by passing the Counterfeit Access Device and Computer Fraud and Abuse Law.").

[34] Leeson & Coyne, *supra* note 32, at 514 (emphasis added).

[35] Kerr, *supra* note 7, at 1602–03.

[36] Buckman, *supra* note 2, § 2(a) ("There was, therefore, a loophole where either: authorized persons caused harm to protected computer systems; or unauthorized persons gave codes or software to authorized persons who loaded them into their computers.").

[37] *I.e.* computers belonging to Government and financial businesses. *Id.*

[38] Corcoran, *supra* note 1, at 2. *See* COMPUTER CRIME & INTELLECTUAL PROP. SECTION, U.S. DEP'T OF JUSTICE, PROSECUTING COMPUTER CRIMES MANUAL 34 (2007), *available at* http://www.justice.gov/criminal/cybercrime/ccmanual/01ccma.html.

CFAA are generally hauled into court under claims akin to traditional torts such as purporting to steal the employer's information in anticipation to leaving employment.[39]

Prior to 1984, Congress and the courts had relied on mail-and-wire fraud statutes to combat computer crimes, but this proved to be an inadequate mechanism because emerging computer crimes did not fit elements of existing mail-and-wire statutes.[40] Although Congress has cautiously broadened the scope and coverage of the CFAA since its original enactment in 1984,[41] Congress continued to express its disfavor for applying the statute in the context of insider liability.[42] For example, even after the 1986 and 1996 amendments,[43] Congress, while acknowledging that insiders may sometimes come under the purview of the CFAA, resisted the call to equate insider liability with outsider hacking by carefully restricting the circumstances under which an insider – i.e., a user with authorized access – could be held liable for violating the statute:

[I]nsiders, who are authorized to access a computer, face criminal liability *only if they intend to cause damage to the computer*, not for recklessly or negligently causing damage. By contrast, outside hackers who break into a computer could be punished for any intentional, reckless, or other damage they cause by their trespass.[44]

The plain language of the 1996 Committee Report supports the

[39] Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003) ("[T]he majority of CFAA cases still involve 'classic' hacking activities. Employers, however, are increasingly taking advantage of the CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system."). Obviously the tenuous connection these traditional tortfeasors have to the CFAA appear to be that the information they purportedly steal is stored in computer systems.

[40] Buckman, *supra* note 2, § 2(a).

[41] *Id.* For example, the CFAA was originally a criminal statute designed to protect classified information belonging to government or financial institutions. Civil right of action and remedies came much later in the 1994 amendments. *Id.*

[42] Field, *supra* note 24, at 831.

[43] S. Rep. No. 104-357, at 4–5 (1996).

[44] *Id.* at 4–5, 10 (emphasis added). *See* S. Rep. No. 99-432, at 7–8 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479. From this language it is reasonable to conclude that congress intended to exempt employee subsequent misuse of information acquired under existing authorization from the purview of the CFAA regardless of the subjective intent. Congress intended to reach the employee only in classic cases where the employee's actions were directed at harming the infrastructure or system itself.

inference that Congress did not intend for the access of an authorized user to be actionable under the CFAA because the employee merely possessed adverse intentions to those of the employer. As one jurist has surmised, "the legislative history supports the conclusion that Congress intended the CFAA to do 'for computers what trespass . . . laws did for real property'"[45] such that the necessary inquiry is whether the property owner invited the entrant and not the subsequent conduct of the invitee while on the property. Courts should therefore decline to extend the CFAA to employment where the gravamen of the complaint is the employee's intended or actual misuse of employer's information, because such construction extends the Act beyond the contours of legislative intent.

Commentators who support applying the CFAA to traditional crimes such as trade secret misappropriation and theft of employer information do so for a number of reasons. First, the CFAA has provided employers with purely traditional tort claims a previously unavailable easy access to federal courts.[46] Second, under the CFAA federal question jurisdiction, employers do not need to show the parties' diversity of citizenship in order for federal courts to have subject matter jurisdiction.[47] Third, the federal courts provides for a nationwide service of process, which is valuable for the plaintiff employer.[48] Moreover, the pleading standards under the CFAA are much easier to meet than those of state trade secrets claims.[49]

---

[45] Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 935 (W.D. Tenn. 2008) (citations omitted).

[46] *See. e.g.,* Linda K. Stevens & Jesi J. Carlson, *The CFAA: New Remedies for Employee Computer Abuse*, 96 ILL. B. J. 144, 161 (2008) (celebrating that the CFAA will continue to offer many victims of *computer misuse* a pathway to federal court); Graham M. Liccardi, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court*, 8 J. MARSHALL REV. INTELL. PROP. L. 155, 156–57, 187 (2008) (promoting the CFAA as a means to secure access to the federal courts in order to meet the needs of trade secret litigation until congress enacts legislation authorizing federal question jurisdiction specifically for trade secrets misappropriation).

[47] Liccardi, *supra* note 46, at 156.

[48] *Id.* at 187 ("Litigating this type of case in state court might require filing motions and proceedings in multiple jurisdictions throughout the country in order to depose key witnesses and obtain necessary evidence. Nationwide service of process avoids this entire situation and saves substantial amounts of time [and resources].").

[49] *Id.* at 188 ("[T]he CFAA does not require the plaintiff to prove that a trade secret exists or that the plaintiff took reasonable efforts to prevent disclosure, both of which are required in all state-based causes of action relying on the UTSA.").

These reasons—skewed largely in favor of employer convenience—are not, however, compelling enough to warrant a radical extension of the statute beyond the intent of Congress. Besides, there is already a federal statute, the Economic Espionage Act (EEA),[50] and various state statutes which expressly target the misappropriation of employer trade secrets.[51] The EEA *would* provide identical procedural benefits as the CFAA.[52] Arguably, the EEA provides better procedural benefits for corporate victims of information torts given the statute's extra-territorial applicability to conduct outside the United States.[53] Moreover, the category of trade secrets under the EEA is broader than the definition of trade secrets under state civil law standards.[54] But the EEA is limited by its lack of a private right of action for civil damages.[55] Corporate victims of information torts can refer an EEA case to the FBI, cooperate with the FBI investigations, and ask the Attorney General to seek an injunction against a rogue employee or another party that has stolen its trade secrets.[56] Reforming the EEA to grant employers a private right of action is beyond the scope of this article; however, many commentators have made a quite compelling case for the idea of expanding the statute to include a private right of action.[57] Thus, unauthorized access should be

[50] 18 U.S.C. §§ 1831-1839 (2006).

[51] *See* Thomas J. Gray & Peter O'Rourke, *Preventing Employee Trade Secret Misuse From Derailing Your Company*, LAW. BRIEF, April 25, 2008, at 1 ("[E]very state has enacted some form of protection for a company's trade secrets.").

[52] 18 U.S.C. § 1836(b) (2006) (granting federal district courts exclusive original jurisdiction of civil actions under the EEA).

[53] 18 U.S.C. § 1837 (2006) (applying only when "(1) the offender is a citizen or permanent resident alien of the United States; or an organization organized under the laws of the United States or a State or political subdivision thereof; or (2) an act in furtherance of the offense was committed in the United States.").

[54] United States v. Hsu, 155 F.3d 189, 196 (3rd Cir. 1998) ("There are, though, several critical differences [between the EEA and state trade secrets laws] which serve to broaden the EEA's scope. First, and most importantly, the EEA protects a wider variety of technological and intangible information than current civil laws.").

[55] *See* 18 U.S.C. § 1836(a) ("The Attorney General may, in a civil action, obtain appropriate injunctive relief against any violation of this chapter.").

[56] Jerome P. Coleman et al., *Electronic Communications and Privacy in the Workplace*, 762 PLI/LIT 597, 613 (2007).

[57] *See generally* Mark Halligan, *Protection of U.S. Trade Secret Assets: Crucial Amendments to the Economic Espionage Act of 1996*, 7 J. MARSHALL REV. INTELL PROP. L. 656, 675 (2008) (proffering an amendment to the EEA, which creates a civil cause of action allowing companies to protect trade secret

narrowly construed under the CFAA because unauthorized use is covered under other appropriate federal and state laws.

Despite available civil and criminal law alternatives, proponents of extending CFAA provisions to employee classical information theft cases can point to statements in the 1986 Senate Report in which the Judiciary Committee noted that:

Any enforcement action in response to criminal conduct indirectly or directly related to computers must rely upon a statutory restriction dealing with some other offense. This requires the law enforcement officer, initially the agent, and then the prosecutor, to attempt to create a "theory of prosecution" that *somehow fits what may be the square peg of computer fraud into the round hole of theft, embezzlement or even the illegal conversion of trade secrets*.[58]

At best, this comment provides but a weak signal of legislative intent regarding the need for *a statute* targeting traditional *crimes* perpetrated using the computer. It is noteworthy that the comment addresses criminal prosecution and makes no mention of authorized insider liability in a civil context. In fact, the same Judiciary Committee cautioned that it wished "to avoid the danger that every time an employee exceeds his authorized access to his department's computers . . . he could be prosecuted under [§ 1030(a)(5)]."[59] Thus, courts should refran from extending the statute's civil liability provisions to insider *use*-cases where the employee was authorized to access information in the employer's computer system.

assets and ensuring the continued growth and protection of trade secret assets in the international marketplace); Michael L. Rustad, *The Negligent Enablement of Trade Secret Misappropriation*, 22 SANTA CLARA COMPUTER & HIGH TECH. L.J. 455, 458 (2006) (arguing for amending the EEA to give corporate victims standing to file a statutory tort action against the tortfeasor of business information and information products). *Cf.* Geraldine Szott Moohr, *The Problematic Role of Criminal Law in Regulating Use of Information: The Case of the Economic Espionage Act*, 80 N.C. L. REV. 853, 860–61 (2002) (arguing that the criminalizing theft of information through the EEA restrains employ mobility, reduces the creation of innovative products and ideas, and constrains economic growth, and a more judicious course is to address the takings of information and information products though civil law); David S. Almeling, *Four Reasons to Enact a Federal Trade Secrets Act*, 19 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 769, 770 (2009) (treating the EEA as a precursor to a much needed federal statute to enforce trade secrets violations).

[58] *See* S. Rep. No. 99-432, at 14 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479 (emphasis added).

[59] *Id.* at 7.

B. Judicial Statutory Flux

The CFAA is problematic when applied to employee situations for various reasons. First, as "insiders," employees do not exactly conform to the typical idea of the "hacker" who is commonly understood as a third-party outsider, and against whom the statute was originally targeted.[60] Second, the CFAA is not easily applicable in the disloyal employee context given that most employees would normally be given permission to access some minimum amount of the employer's information. It should come as little surprise, then, that current judicial attempts to stretch the contours of the statute to encompass disloyal employee access have their critics.

1. Civil Action under the CFAA

Although the CFAA is primarily a criminal statute aimed at punishing fraudulent damaging activities related to the wrongful access of computers,[61] a victim may bring civil action for damages arising from violation of certain sections of the CFAA.[62] However, exactly which sections of the CFAA give rise to civil action remains the subject of much debate and disagreement by the courts.[63] Some courts have held that civil actions under the CFAA may not be brought for violations other than those based on provisions of § 1030(a)(5).[64] This subsection prohibits knowingly transmitting a program, information, code, or command that causes damage to a computer or intentionally accessing a computer without authorization and as a result of the unauthorized access causing damage and loss or recklessly causing damage.[65] In other words, these courts require a

[60] *See* Field, *supra* note 24, at 820.

[61] Hewlett-Packard Co. v. Byd:Sign, Inc., No. 6:05-CV-456, 2007 WL 275476, at *12 (E.D. Tex Jan. 25, 2007).

[62] 18 U.S.C. § 1030(g) (2006) ("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. A civil action for a violation of this section may be brought only if the conduct involves 1 of the factors set forth in subclauses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i). Damages for a violation involving only conduct described in subsection (c)(4)(A)(i)(I) are limited to economic damages.").

[63] *See infra* notes 64-69 and accompanying text.

[64] Cenevo Corp. v. Celumsolutions Software GMBH & Co., 504 F. Supp. 2d 574, 580 (D. Minn. 2007) ("A party cannot bring a civil action based on provisions other than § 1030(a)(5). Accordingly, any claim based on violations of § 1030(a)(4) and § 1030(a)(6) fails as a matter of law.") (citations omitted).

[65] 18 U.S.C. § 1030(a)(5).

showing of some damage to the computer system as a precondition to insider liability. Some courts, however, have rejected the argument that § 1030(g) authorizes civil actions only for violation of subsection 1030(a)(5), and one such court noted that this reasoning is at "odds with the language of the statute."[66] These latter courts have opted for a broader reach of the CFAA and held that civil actions under the CFAA can be based on a violation of any of the subsections of § 1030(a) as long as one of the five factors in subsection 1030(a)(5) is implicated.[67] These courts that support a broader right of action under the CFAA would apply the statute to cases where no damage was made to the computer system as long as the employee obtains anything of value by means of access exercised without authorization or in excess of authorization.[68] Another group of courts have deferred or evaded ruling on the issue altogether with some preferring instead to concentrate on whether the access was authorized or

[66] Fiber Sys. Int'l, Inc. v. Roehrs, 470 F.3d 1150, 1157 (5th Cir. 2006) (holding that civil actions under the CFAA can be based on a violation of any of the subsections of § 1030(a) as long as one of the five factors in subsection (a)(5) is involved); *See* P.C. Yonkers, Inc. v. Celebrations The Party & Seasonal Superstore, L.L.C., 428 F.3d 504, 511–12 (3d Cir. 2005) ("We do not read section 1030(g)[ ] . . . as limiting relief to claims that are *entirely based only on* subsection (a)(5), but, rather, as requiring that claims brought under other [sub]sections must meet, in addition, one of the five numbered (a)(5)(B) 'tests.'"); Theofel v. Farey-Jones, 359 F.3d 1066, 1078 & n.5 (9th Cir. 2003) (stating that § 1030(g) "applies to any violation of [1030(a)] and, while the offense must involve one of the five factors in (a)(5)(B), it need not be one of the three offenses in (a)(5)(A).").

[67] *See infra note* 66. § 1030 sets forth various causes of action. *See, e.g.*, 18 U.S.C. § 1030(a)(2)(A) ("[I]ntentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution . . . ."); § 1030(a)(2)(C) ("[I]ntentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information from any protected computer."); § 1030(a)(4) ("[K]nowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of 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 and the value of such use is not more than $5,000 in any 1-year period.").

[68] *Compare* McLean v. Mortg. One & Fin. Corp., No. Civ.04-1158(PAM/JSM), 2004 WL 898440, at *2 (D. Minn. Apr. 9, 2004) ("[CFAA] limits civil enforcement to actions claiming a violation of § 1030(a)(5)(B), not § 1030(a)(4)."), *with P.C. Yonkers, Inc.*, 428 F.3d at 511–13 (holding that a claim based on § 1030(a)(4) is actionable in a civil suit in direct disagreement with contrary authorities, even noting that at least "one court seems to have read section 1030(g)'s reference to subsection (a)(5)(B) as limiting relief under § 1030(g) to only subsection (a)(5) claims, but we disagree.").

not.[69] Thus, employers across jurisdictions have brought suits under the various subsections of the statute with mixed results. However, this article seeks a common understanding of the statute's *access authorization* provisions irrespective of by which subsection the employee's conduct is scrutinized.

2. The Indeterminacy of Authorization

When an employee leaves his workplace, voluntarily or otherwise, the employee customarily returns items belonging to the employer. If the employee later tries to access his former employer's computer system, it is generally understood that he is accessing the system after his previous authorization has expired (i.e., the employee is without authorization) and in a manner analogous to that of the outside hacker.[70] However, the analysis becomes complicated when the employee is *still* employed and exercises his existing authorization to view commercial information available to him or her. Such access may be motivated by purposes adverse to the employer's interest or by simple curiosity. The difference between *access* "without authorization" and *access that* "exceeds authorization" can be no more than exegesis in semantics.[71] Yet this paper-thin margin continues to be a source of a great deal of division for courts trying to apply the CFAA "to the delicate and complex relationship that exists between employees and employers."[72]

As noted above, neither Congress nor the Supreme Court has

[69] Condux Int'l, Inc. v. Haugum, No. 08-4824 ADM/JSM, 2008 WL 5244818, at *3–5 (D. Minn. Dec. 15, 2008) ("[T]he apparent conflict in case law need not be resolved here. Even assuming that the CFAA authorizes civil actions for violations of any of the subsections in § 1030(a), [plaintiff] has failed to allege sufficient facts to support its CFAA claim for violations . . . .").

[70] However, at least one court has required that an employer take explicit steps to revoke employee systems authorization post employment before the employee's subsequent access could be deemed unauthorized. *See* Clarity Servs., Inc. v. Barney, 698 F. Supp. 2d 1309, 1314–16 (M.D. Fla. 2010) (holding that employee's reading of email from former employer's customer after employee had tendered his resignation was not unauthorized, and thus did not violate Computer Fraud and Abuse Act (CFAA), where employer had not suspended employee's email account, and employee did not attempt to access his email account after it eventually was suspended).

[71] Lasco Foods, Inc. v. Hall & Shaw Sales, Mktg., & Consulting, LLC, No. 4:08CV01683 JCH, 2009 WL 3523986 at *3 (E.D. Mo. Oct. 26, 2009) ("[T]he difference between 'without authorization' and 'exceeding authorized access' is 'paper thin.'" (citing Int'l Airport Ctrs., L.L.C., v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006))).

[72] Field, *supra* note 24, at 821.

articulated clearly the circumstances under which an employee's conduct exceeds authorized access.[73] Commentators who have attempted to define *access in excess of authorization* invariably amalgamate independent notions of authorization and access from multidisciplinary sources.[74] A more plausible starting point should construe authorization as *something*[75] the owner has the primary right to bestow and control.[76] However, once bestowed, a fact-finder should presume that the employee's authorization to access the specified information contained in the employer's system is valid and effective. This presumption should only be rebutted when the employer can show by clear evidence that the employer, by contract, code or policy 1) constrained the employee's access to specific boundaries (e.g. specific files on a network) and the employee transgressed beyond those boundaries; 2) the employer withdrew its consent with notice to the employee; or 3) the employment relationship terminated prior to the access in question.[77] However, the question remains: what constitutes a revocation of the employer's consent? Specifically, *should* an employee, by a disloyal intent, unilaterally invalidate an existing authorization even without the owner's knowledge of such employee's subjective intent?

Although there are other issues associated with the construction of the CFAA, the disagreement over the CFAA's vague access authorization provisions has contributed much to the split among the federal courts. The seminal cases that iterate this disagreement are discussed in the following section.

---

[73] *See supra* text accompanying notes 6-8.

[74] *See generally* Kerr, *supra* note 7, at 1640–41 (discussing why courts have struggled to interpret unauthorized access and arguing, with regards to access, that while the concept may have made sense in the 1970's computer era, the contemporary user may be unaware of the point when a particular conduct completes an entry sufficient to be deemed access).

[75] Perhaps a form of consent. For example, usernames and passwords are types of manifestations of the owner's consent as are oral or written contracts. *See id.* at 1625–26.

[76] *See id.*at 1641.

[77] *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133–35 (9th Cir. 2009) ("If the employer has not rescinded the defendant's right to use the computer, the defendant would have no reason to know that making personal use of the company computer in breach of a state law fiduciary duty to an employer would constitute a criminal violation of the CFAA. It would be improper to interpret a criminal statute in such an unexpected manner.").

III. INTERCIRCUIT CONFLICT

A recent district court decision, *ReMedPar, Inc. v. AllParts Med., LLC,* iterates the long running federal circuits' split over employee CFAA access authorization.[78] In *ReMedPar,* plaintiff-employer brought CFAA claims and a concurrent trade secret claim against a departing employee who shared the information he obtained from the employer's computer system with a competitor.[79] The relevant thrust of the employer's allegation was that the employee, whilst still employed, "unlawfully breach[ed] his duty of loyalty and agreement[80] to maintain the confidentiality of [the employer's] trade secrets" and that by this breach the employee "exceeded his authority, regardless of the fact that he had the authorization to access the information in the first place."[81] The employer ReMedPar's argument is typical of the formerly dominant construction of CFAA authorized access jurisprudence – one where the concept of authorized access is broadly enmeshed in agency theory, and conferred authority evaporates once the employee acquires an interest adverse to the employer's business.[82] In rejecting the employer's argument, the *ReMedPar* court, citing a sister court's holding in *Black & Decker Inc. v. Smith,*[83] concluded that legislative history supports the conclusion that "Congress did not intend the CFAA to extend to situations where the access was *technically* authorized but the [subsequent] use of the information was not."[84]

---

[78] ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 610–13 (M.D. Tenn. 2010) ("There is in fact, a split in legal authority as to whether the CFAA applies in a situation where an employee who has been granted access to his employer's computers, but uses that access for an improper purpose.").

[79] *Id.* at 606–08.

[80] *Id.*at 610. The agreement in *ReMedPar* does not concern an agreement as to navigable zones of access but rather traditional confidentiality agreement against disclosure – i.e. *use of* – trade secrets. *Id.* at 607, 610–11. This distinction is necessary for purposes of this article's support for the use of contract law in defining zones of authorized access.

[81] *Id.* at 610.

[82] *See* Field*, supra* note 24, at 823 (explaining that under agency-based interpretation of the CFAA the "employee's authorization is implicitly revoked when he accesses a computer for purposes that do not further his employer's interests").

[83] 568 F. Supp. 2d 929 (W.D. Tenn. 2008).

[84] *ReMedPar,* 683 F. Supp. 2d at 613 (emphasis added) (citing *Black & Decker, Inc.* 568 F. Supp. 2d at 935–36). The choice of word "technically" is instructive here as it suggests that the court would consider code-based authorization akin to express invitations sufficient to bar plaintiff employer from arguing that the access, irrespective of the subjective intent of the

Courts are increasingly split on whether to continue applying the broad construction of CFAA access authorization jurisprudence or adopt a much narrower interpretation to the text of the statute. The table in *Schedule 1* shows the pattern of split among the circuits. It is, however, noteworthy that only one Court of Appeals decision to date has *expressly*[85] adopted the narrow view of the CFAA,[86] whereas the Seventh[87] and First Circuits[88] have adopted the agency-based approach. However, the majority of the posturing continues to occur at the district court level.

A. The Broad Constructionists

"*Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*[89] is the [leading] case championing the broad[est] interpretation of the term 'without authorization.'"[90] In *Shurgard*, a competitor of the employer approached the employee, who was authorized and had full access to the employer's confidential business plans, expansion plans, and other trade secrets stored in the employee's computers.[91] Prior to quitting his job and accepting employment with the competitor, the employee sent e-mails to the competitor containing various trade secrets and proprietary information belonging to the employer.[92]

employee at the time or subsequent to the access, constituted a trespass.

[85] The Second Circuit has however denied CFAA claimants a remedy for competitive harm suffered as a result of misuse or misappropriation. Nexans Wires S.A. v. Sark-USA, Inc., No. 05-3820-CV, 2006 WL 328292, at *1–2 (2d Cir. Feb. 13, 2006); *See also* Nexans Wires S.A. v. Sark-USA, Inc., 319 F. Supp. 2d 468, 477–78 (S.D.N.Y. 2004), *aff'd*, 166 F.App'x 559 (2d Cir. 2006), (stating that the plaintiff could not recover revenue lost "as a result of defendants' . . . [ability] to unfairly compete for business," where the defendants misappropriated the plaintiff's proprietary information).

[86] LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1132–33 (9th Cir. 2009).

[87] *See* Int'l Airports Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 418–21 (7th Cir. 2006) (explaining that defendant's decision to quit in addition to his misconduct towards the company violated his agency relationship making all future transmissions unauthorized).

[88] *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582–86 (1st Cir. 2001) (stating that plaintiff was likely to succeed on CFAA claim and therefore preliminary injunction was properly ordered when employee transmitted confidential information to third party in violation of confidentiality agreement).

[89] 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

[90] Liccardi, *supra* note 46, at 163.

[91] *Shurgard,* 119 F. Supp. 2d at 1123.

[92] *Id.*

Similar to the fact pattern in *ReMedPar* discussed above, the *Shurgard* employer filed a claim under the CFAA alleging, among other claims, that the authorization for its former employee ended when the employee began acting as an agent for the competitor.[93] However, in *Shurgard*, the employee's motion to dismiss was rejected by the court, which instead agreed with the employer and relied on the agency theory in holding that "the authority of an agent terminates if, without knowledge of the principal, he acquires adverse interests or if he is otherwise guilty of a serious breach of loyalty to the principal."[94] The thrust of the agency-based approach is that the employee's subjective intent is critical in analyzing whether the employee's otherwise contemporaneous authority remains valid and effective for purposes of accessing employer's information.[95] But, as shall be shown below, this approach raises two potentially thorny questions: 1) when and how often should the courts be involved in determining when some kinds of access or use will be authorized for the employee in a given circumstance while being unauthorized in another circumstance; and 2) how should the courts distinguish the access point from a permitted versus impermissible use of the information subsequent to the original access. In order words, for how long between the time of employee's access to the wrongful use of information allegedly gained should the court hold that the employee's subsequent misuse of that information is within the prohibited actions of the CFAA? Undoubtedly, there could be cases where an employee may access and view his employer's information in the course of performing his duties on Monday and then develop an anti-competitive intent to use that information on Tuesday. Should such cases be within the purview of the CFAA?

The Seventh Circuit officially adopted the *Shurgard* holding and reasoning in *International Airports Centers, L.L.C. v. Citrin*, where Judge Posner used the occasion to entrench agency law into the judicial interpretation of the CFAA.[96] Since the *Citrin* court's express affirmation of the *Shurgard* precedence,

[93] *Id.* at 1122, 1124.

[94] *Id.* at 1125 (quoting RESTATEMENT (SECOND) OF AGENCY § 112 (1958)) (internal citations omitted).

[95] *See* Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 934 (W.D. Tenn. 2008) (an employee oversteps whatever authority he is otherwise granted "the minute his intentions are adverse to those of his principal").

[96] Int'l Airports Centers, L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006).

several courts have endorsed *Shurgard's* broad interpretation of the CFAA's authorized access language, and this approach has become, by and large, the dominant view among federal circuit courts until recently.[97]

B. The Narrow View

About five years after *Shurgard*, a district court in Florida rejected the broad agency-based interpretation of CFAA authorized access jurisprudence in *Lockheed Martin Corp. v. Speed*.[98] The plaintiff-employer invited, but the *Lockheed* court declined the invitation to peruse the employee's subjective intentions for evidence of malevolent or disloyal purpose.[99] Instead, the court focused strictly on the preexisting authorization, noting instead that:

[I]t is plain from the outset that Congress singled out two groups of accessers, those "without authorization" (or those *below* authorization, meaning those having no permission to access whatsoever-typically outsiders, as well as insiders that are not permitted *any* computer access) and those exceeding authorization (or those *above* authorization, meaning those that go beyond the permitted access granted to them-typically insiders exceeding whatever access is permitted to them).[100]

Lockheed and its progeny represent alternative approaches to the CFAA access authorization jurisprudence that rejects a consideration of the employee's mindset. The fact patterns in *Lockheed* and *Shurgard* are similar. In *Lockheed*, the employee, who had complete access to his employer's confidential and proprietary and trade secret protected information, resigned from Lockheed and thereafter became employed with its competitor.[101] "Shortly before resigning, [the employee] allegedly copied 200 documents . . . from his [work] computer by burning them onto a compact disc."[102] Even though the *Lockheed* court determined that the employer had alleged injury sufficient for some form of

[97] The Seventh Circuit endorsed the broad view in 2006, whereas the Ninth Circuit first endorsed the narrower view in 2009. *See infra* Schedule 1.

[98] No. 6:05-CV-1580-ORL-31, 2006 WL 2683058, at *7 (M.D. Fla. Aug 1, 2006).

[99] *Id.* at *4.

[100] *Id.* at *5.

[101] *Id.* at *1.

[102] *Id.*

civil relief,[103] the court, however, dismissed the complaint on the grounds that the employer had not sufficiently pled a CFAA violation because Lockheed allowed its employees "to access the company computer, [therefore] they were not without authorization."[104] "Further, because Lockheed permitted the Employees to access the precise information at issue, the Employees did not exceed authorized access . . . . [since they] fit within the very group that Congress chose not to reach, *i.e.*, those with access authorization."[105]

The *Lockheed* case also cites the rule of lenity as a basis for a narrower construction of the statute.[106] The rule of lenity is "a manifestation of the fair warning requirement" and a bedrock of public policy, holding that, absent fair warning to the defendant, the courts should resolve statutory ambiguity in the defendant's favor.[107] Although lenity is a canon of interpretation mostly utilized in criminal statutes, courts have employed the rule in interpreting qualifying civil statutes.[108] For example, the Supreme Court in *Leocal v. Ashcroft* held that where a statute has both criminal and noncriminal applications, courts should interpret the statute consistently in both criminal and noncriminal contexts.[109] The CFAA contemplates both civil and criminal applications, and given the two diametrically different interpretations of the statute's access authorization scope, the

103 *Id.* at *2–3 ("Lockheed Adequately Alleges Injury Under § 1030(g).").

104 *Id.* at *5.

105 *Id.*

106 *Id.* at *7 ("To the extent [a term] can be considered ambiguous . . . the rule of lenity, a rule of statutory construction for criminal statutes, requires a restrained, narrow interpretation."). *See also* Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 386 (S.D.N.Y. 2010) ("[T]he rule of lenity guides the Court's interpretation of the CFAA, which is primarily a criminal statute.").

107 *Orbit One*, 692 F. Supp. 2d at 386. Time-framing should be important here – the relevant *warning requirement* should be tolled at the time the employer notifies the employee that authorization has been withdrawn.

108 *See, e.g.*, LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1134–35 (9th Cir. 2009) (collecting Supreme Court cases and concluding that the rule of lenity applies to the interpretation of the CFAA because "our interpretation of §§ 1030(a)(2) and (4) is equally applicable in the criminal context.").

109 543 U.S. 1, 11 & n.8 (2004) (explaining that, "if a statute has criminal applications, 'the rule of lenity applies' to the Court's interpretation of the statute even in immigration cases") (citation omitted). *See also* Clark v. Martinez, 543 U.S. 371, 380 (2005) (explaining that the rule of lenity applies to civil statutes that have criminal applications because courts are required to interpret such statutes consistently, regardless of whether the court encounters the statute in a criminal or a noncriminal context).

rule of lenity compels courts to favor the narrower interpretation.[110]

C. Approaches to Authorized Access

Courts disagree on whether to approach CFAA authorization interpretation using agency, contract or code-based theories. These approaches in turn hinge on whether and to what extent a court should consider the mindset of the employee at the time the access in controversy was made. This section reviews the strengths and weaknesses of each of the approaches. Because contract and code-based approaches focus on objectively ascertainable standards and thus are less prone to abuse, they provide sounder bases for determining whether an employee was unauthorized within the meaning of CFAA. On the other hand, agency-based approaches threaten to impose liability on a range of potentially access-inoffensive conduct[111] and are inconsistent when adapted to the employment relationship.

1. The Agency-Based Approach

The agency argument undergirds a broader interpretation of the CFAA authorization language. Agency approach posits that an employee with authorization to access an employer's protected computer loses such authorization merely by developing a disloyal intent towards the employer.[112] This approach has its strengths. First, it is arguably "another weapon [for employers] against rogue employees who are pilfering confidential information."[113] Second, "agency rules can function as a control mechanism, discouraging behavior that may or may not violate

[110] *Lockheed*, 2006 WL 2683058, at *7 ("[A broad] reading is especially disconcerting given that the CFAA is a *criminal* statute with a civil cause of action. To the extent 'without authorization' or 'exceeds authorized access' can be considered ambiguous terms, the rule of lenity, a rule of statutory construction for criminal statutes, requires a restrained, narrow interpretation.").

[111] An employee may indeed have authorization to access the employer's computer for work-related internet searches. Assume, however, that the employee begins to search for pornography during work time, this conduct may violate his employer's policy but, nonetheless, this conduct arguably does not disturb the status of his authorization under the CFAA.

[112] Liccardi, *supra* note 46, at 163 & n.74 ("Violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship." (quoting Int'l Airport Ctrs., L.L.C., v. Citrin, 440 F.3d 418, 42021 (7th Cir. 2006))).

[113] Field, *supra* note 24, at 843.

fiduciary obligations . . . since liability may attach any time the employee acts in a manner capable of being characterized as against his employer's interests."[114]

Commentators have argued that the presumed weaknesses of the agency approach invariably override its strengths. For example, one commentator has argued that the deterrent effect of using agency principles in access authorization analysis is at best doubtful, because for agency-based approach to affect an employee's decisions, "the employee would have to . . . know about the existence of liability under the CFAA for unauthorized computer access;" however, most employees do not fully understand their relationship with the employer as based on agency, and moreover, agency relationships may be formed even absent an agent's knowledge.[115] Other commentators have argued that merely breaching a duty of loyalty or confidentiality to the employer should not be actionable under the CFAA because there are other suitable remedies for the employer.[116] A "domino effect" phenomenon inherent in agency-based interpretation renders the approach more problematic. It is unclear whether a determination that an employee terminated his agency relationship for CFAA purposes also binds the employer for non-CFAA purposes.[117] Courts are likely to become bogged down in a determination of exactly how much, if not all,

[114] *Id.* at 846.

[115] *Id.*

[116] *See* Richard Warner, *The Employer's New Weapon: Employee Liability Under the Computer Fraud and Abuse Act*, 12 EMP. RTS. & EMP. POL'Y J. 11, 27 (2008) (questioning an employer's need for protection under the CFAA as "employers already have statutory and common law protection through trade secret law, non-competition and confidentiality agreements, and breach of loyalty claims").

[117] Assuming, *arguendo*, that an employee develops a disloyal intent by 10 a.m. on Friday morning, under agency-based approach, his subsequent access of the employer's information by 10:01 a.m. would be unauthorized. Assuming the employee sends an email that secures a lucrative deal for the employer by 10:15 a.m. the same day, could the third-party business rescind the deal on the theory that the employee was in fact unauthorized? *See, e.g.,* Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 385 & n.65 (S.D.N.Y. 2010) ("[The employee's] breach of his duty of loyalty terminated his agency relationship (more precisely, terminated any rights he might have claimed as [his employer's] agent-he could not by unilaterally terminating any duties he owed his principal gain an advantage!) and with it his authority to access the laptop, because the only basis of his authority had been that relationship." (alteration in original) (quoting Int'l Airport Ctrs., LLC. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006))).

subsequent access should be deemed unauthorized,[118] especially when one considers that an employee who is downloading his emails with the intent to abscond with them may also at the same time be sending emails to his employer's creditors about an invoice that is due to the employer. In this scenario, would all actions taken in furtherance of the master's business be null and void because the agent previously lost his authorization?

The agency-based approach also disturbs policy preferences underlying laws designed to protect business and trade secrets.[119] Because employers are more likely to bring suit under the CFAA in cases where the facts are analogous to trade secret misappropriation,[120] an agency-based interpretation of authorized access heralds a watershed moment in trade secret jurisprudence because employers have recourse to essentially similar relief under a much lower pleading standard.[121] A fact-finder should require employers to objectively demonstrate preexisting restrictions on the employee, which the employee would have circumvented or breached.

2. The Contract-Based Approach

The contract-based approach to CFAA access authorization jurisprudence requires the employer to prove that there was a binding contract with the employee delineating the zones of access granted to and precluded from the employee, and that the employee breached the contractual terms regarding access to his employer's network. The seminal case employing a contractual

[118] *See* Field, *supra* note 24, at 843–44.

[119] These laws require a showing that the information allegedly misappropriated or stolen derives independent economic value from being secret and is the subject of reasonable effort to maintain its secrecy before the lawsuit. *See* 18 U.S.C. § 1839(3) (2010); UNIFORM TRADE SECRETS ACT § 1(4) (1985) (which has been adopted in forty-six states and the District of Columbia and the U.S. Virgin Islands). *See* MELVIN F. JAGER, 1 TRADE SECRETS LAW § 3:29: STATES COVERED BY THE ACT, (2010) (collecting states that have adopted the UTSA); RESTATEMENT (FIRST) OF TORTS, § 757, Comment (b) (1939).

[120] *See, e.g.,* Liccardi, *supra* note 46, at 188 ("[Benefits of the CFAA:] the CFAA does not require the plaintiff to prove that a trade secret exists or that the plaintiff took reasonable efforts to prevent disclosure, both of which are required in all state-based causes of action relying on the UTSA. Many trade secrets lawsuits fail because the plaintiff cannot prove that the information meets the UTSA definition of a trade secret."). This is also a benefit because "[t]here is no federal trade secrets statute . . . [and] the CFAA can act as a gap-filler until Congress explicitly provides for federal protection of trade secrets. *Id.* at 187.

[121] *See*, *supra,* notes 118–19.

interpretation to the CFAA authorization definition is *Hewlett-Packard Co. v. Byd:Sign, Inc.*,[122] where a district court denied an employee's motion to dismiss because the employer pointed to certain sections of a confidentiality agreement, which prohibited "disclosing HP's proprietary information," and HP's Standards of Business Conduct signed by the employees, in which each employee agreed to refrain from, among other things, use of HP computers for personal gain.[123]

The contract-based approach promotes clarity, albeit to a lesser extent than a code approach, because it depends on the existence of an implicit or explicit contract that defines the scope of authorization for a particular employee.[124] The First Circuit has championed the use of contracts to clearly define employee limits for purposes of determining when authorized access has been exceeded.[125] Although a relatively new approach, some courts are beginning to recognize the weight of contractual restrictions on authorized access inquiries.[126]

A potential pitfall with the contract-based approach is the likelihood that courts may ultimately be called upon to devise the intentions of the parties. For example, contracts themselves may be ambiguous, and the employer's intent may not be clear in the wording of an express contract. The employer's intent may even

[122] No. 6:05-CV-456, 2007 WL 275476 (E.D. Tex. Jan. 25, 2007).

[123] *Id.* at *11, *13. *See* Victoria A. Cundiff, *Digital Defense: Protecting Trade Secrets Against New Threats*, *in* 14th ANNUAL INST. ON INTELLECTUAL PROP. LAW, at 724–25 (PLI Patents, Copyrights, Trademarks, & Literary Prop., Course Handbook Series No. 947, 2008) (noting the *Hewlett-Packard* decision provides guidance to employers who may draft contracts in order to protect trade secrets from employees misusing information in the future).

[124] Field, *supra* note 24, at 827–28.

[125] *See* EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 63–64 (1st Cir. 2003) ("It is also of some use for future litigation among other litigants in this circuit to indicate that, with rare exceptions, public website providers ought to say just what non-password protected access they purport to forbid."); United States v. Czubinski, 106 F.3d 1069, 1071 (1st Cir. 1997).

[126] *See, e.g.*, Ticketmaster Corp. v. Tickets.com, Inc., No. CV997654HLHVBKX, 2003 WL 21406289, at *1–3 (C.D. Cal. Mar. 7, 2003) (deciding that the contractual exclusion from site was enforceable, but trespass claim could not be maintained where defendant merely gathered public information on plaintiff's web site and nothing more); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 248, 252 (S.D.N.Y. 2000), *aff'd as modified*, 356 F.3d 393 (2d Cir. 2004) (finding the defendant assented to plaintiff's online contract terms by submitting inquiries to plaintiff's website even though defendant was not asked to click on an icon to accept the terms, whereby, the court issued an injunction against defendant from further use of plaintiff's database on various grounds, including a violation of the CFAA).

be far less clear if the contract were merely implied or generically posted on a wall in the break room or clipped inside the middle page of a thick volume employee handbook. It is possible, under the *Hewlett-Packard* reasoning, that a court would find that an employee was using a computer for his personal gain in violation of the CFAA.[127] But a court may not always make this determination unless it peruses the subjective intent of the employee, and this line of inquiry places contract-based approach in close proximity with the agency-based approach.

There may be concern about the potential misuse of the CFAA to bypass or overreach traditional breach of contract claims or breach of confidentiality agreements,[128] leading a commentator to expressly call on the courts to reject contract-based notions of authorization.[129] However, these critics agree that some contractual agreements can adequately define zones of authorized access the violation of which should result in some form of at least civil liability,[130] nor does he oppose the view that owners should be allowed to contractually define the zone of access they do not wish to grant their employees.[131]

Other commentators have criticized the contract-based approach for granting too much power to owners against users.[132] However, this criticism fails to consider the practical burden that the contract-approach places on employers to ensure that a valid

---

[127] *Hewlett-Packard*, 2007 WL 275476, at *13.

[128] *See, e.g.,* Kerr, *supra* note 7, at 1600–02 (calling on the courts to reject contract-based notions of authorization reasoning due to the usual rule that civil precedents apply to criminal cases as there is genuine potential that liability derived from a contract-based approach could lead to potentially unconstitutional expansion of criminal liability). "A breach of Terms of Use or Terms of Service is a breach of trust with the computer owner or operator, but it is a breach of trust that traditional rules and remedies of contract law are well equipped to regulate and deter." *Id.* at 1657.

[129] *Id.* at 1600 ("The fact that computer use violates a contractual restriction should not turn that use into an unauthorized access.").

[130] *Id.* at 1637 ("[T]wo parties are bound by a contract that implicitly or explicitly regulates access to a computer, and one side uses the computer in a way that arguably breaches the contract. The question: Does the breach of contract make the access unauthorized? The remarkable answer, at least in civil cases: Yes.").

[131] *Id.* at 1641–42, 1651 (noting "[i]t is one thing to say that a defendant must pay a plaintiff for the harm his action caused; it is quite another to say that a defendant must go to jail for it").

[132] Field, *supra* note 24, at 847–48 (noting that the relationship between the computer-network owner and the computer-network user was the type of relationship that commentators focused on when saying that the contract-based approach gave too much power to owners without protection for the user).

contract is drafted and that agreements are in compliance with the law.[133] Because employers have the burden to define zones of authorization in advance, a contract-based approach promotes crucial notice between the parties and promotes awareness of the importance of network security by making owners take proactive steps continuously to define and monitor zones of access. Standing alone, a contract-based approach would prove a difficult and costly method of enforcement, particularly in the context of large corporations. This is why this article takes the position that a composite model, involving a mix of contract and code-methodologies, is most preferable. In the contract-code approach, the contract serves a crucial notice element about limits agreed with the employee while the code can provide evidence of employee circumvention of agreed restrictions.

3. The Code-Based Approach

The code-based approach provides a stronger and more clearly delineated alternative to the agency-approach to authorization in the CFAA.[134] This understanding of authorization, limits liability to instances where a user explicitly manipulates a computer system into giving the user greater access and use privileges than she would otherwise have.[135] "When an owner regulates privileges by code, the owner . . . codes the computer's software so that the [employee] has a limited set of privileges on the computer."[136] This can be achieved by "requir[ing] every [employee] to have an account with a unique password, and . . . assign[ing] privileges based on the particular account, [while] limiting where the [employee] can go and what [the employee] can do on that basis."[137] For an employee thus restricted, "to exceed privileges imposed by code, the [employee] must somehow

[133] In most employment settings, the employer drafts the contract and courts construe ambiguous language against the drafter. *See* RESTATEMENT (SECOND) OF CONTRACTS § 206 (1981) (explaining that when interpreting a contract, a court should construe ambiguous language against the interests of the party that drafted it).

[134] Kerr, *supra* note 7, at 1646 ("Regulation by contract offers a significantly weaker form of regulation than regulation by code.").

[135] *Id.* at 1599–1600 ("[A] user can circumvent a code-based restriction on the user's privileges . . . . [and therefore,] the use is unauthorized in the sense that it bypasses a code-based effort to limit the scope of the user's privileges. An example might be use of a stolen password to bypass the password gate designed to block access to a victim's account.").

[136] *Id.* at 1644.

[137] *Id.*

'trick' the computer into giving the user greater privileges."[138]

A code-based approach is most congruent to the instrumental goals of most computer hacking laws. Computer hacking laws have been correctly identified as variations of trespass laws.[139] A code-based approach is more akin to an invitation, the lack of which should expose the access of the employee to liability under variants of trespass[140] and burglary laws.[141] Legislative history also lends support to the proposition that "unauthorized access" is best judged by code restriction since Congress, at the time of enacting the statute, understood the term to be "analogous to that of 'breaking and entering.'"[142] Although Congress contemplated the concept of *exceeding authorization* at the time of enacting the statute, it concluded that information obtained "pursuant to an express or implied authorization," or in accordance with "normal and customary business procedures and information usage" is not actionable under the statute.[143]

The Second Circuit has taken the lead in promoting a code-based approach to CFAA access authorization jurisprudence.[144] In *United States v. Morris,* the court articulated an "intended-function" test for determining when defendant has acted outside the scope of authorized access.[145] In *Morris,* a graduate student

---

[138] *Id.*

[139] *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1072-73 (9th Cir. 2003) (analogizing trespass law with an individual's privacy and propriety interests in the confidentiality of communications, and noting that individuals have a "legitimate interest" in protecting themselves in both instances).

[140] H.R. REP. NO. 98-894, at 10, 12 (1984), *reprinted in* 1984 U.S.C.A.A.N. 3689, 3695–98 (noting that the legislation was motivated by the "capability [of computer networking] which has also enabled the recent flurry of electronic trespassing incidents").

[141] H.R. REP. NO. 98-894, at 20 ("[T]he conduct prohibited [by the CFAA] is analogous to that of 'breaking and entering' rather than using a computer . . . in committing the offense.").

[142] H.R. REP. NO. 98-894, at 20

[143] H.R. REP. NO. 98-894, at 21–22 (noting that the issue of exceeding authorization should be dealt with administratively).

[144] *See* United States v. Morris, 928 F.2d 504, 505–06 (2d Cir. 1991) (holding there was sufficient evidence to conclude that defendant acted "without authorization," within meaning of statute, when he used "a program of password guessing, whereby various combinations of letters are tried out in rapid sequence in the hope that one will be an authorized user's password, which is entered to permit whatever level of activity that user is authorized to perform").

[145] *Id.* at 509–10 (finding that the defendant did not have authorized access when using features of the computer networks in a manner unrelated to their intended function).

used a program to circumvent university restrictions on the computer network, thereby tricking the computer into giving him a "special and unauthorized access route into other computers."[146] The appeal of the code-based approach exists partly due to the fact that it is "usually easy to determine whether a person had properly acquired a password [through his employer] . . . versus when they had improperly acquired access either by stealing a password or hacking into the system by bypassing security measures."[147] Therefore, courts are spared the extra inquiry into the subjective intent of the employee.[148]

4. A Composite Model

Because most employees are given a password or other forms of physical or technical access to an employer's systems as part of their job, a code-based approach to authorization may require additional contractual limits establishing zones and methods of access as well as proof of notice that the employee has been restricted. Courts have often combined a contract and code-based analysis as two-prongs of the same test while deciding the meaning of CFAA authorization.[149] Some commentators have noted a trend in laws on commercial information protection that combines the features of both contract and code-based approaches.[150] A composite model recognizes the parallel

[146] *Id.* at 505, 510–11 (holding Morris lacked authorized access, by the meaning of the statute, even though he indeed had access to some, but not all, of the networked computers).

[147] Field, *supra* note 24, at 849.

[148] *See id.* at 842 ("Considerations of judicial administrability may also militate in favor of a code-based approach . . . . [as such an approach] provide[s] for greater predictability and require[s] less judicial fact-finding . . . .").

[149] *See, e.g.*, Bridal Expo, Inc. v. van Florestein, No. 4:08-cv-03777, 2009 WL 255862, at *10–11 (S.D. Tex. Feb. 03, 2009) ("[T]he Court declines to read the CFAA to equate 'authorization' with a duty of loyalty to an employer such that the CFAA is applicable to this case . . . . [The employees] had signed no confidentiality agreement with Bridal Expo or any other agreement restricting their access to the files they had been working with at their jobs at Bridal Expo. It was within the nature of their relationship with [the supervisor] that [the employees] could use their computers and access the files at issue.").

[150] *See* RAYMOND T. NIMMER, 1 INFORMATION LAW § 3:38: ACCESS CONTROL AS AN ALTERNATIVE RIGHT—PROTECTED LOCATION (2010) ("A concept of unauthorized access has become a common feature of modern U.S. law. In general, it is implemented in situations where, either through technology, contract, mere notice, or general circumstances, the other party has reason to know that access, or at least access in the manner and for the purpose it attempts, is not authorized.").

features of the contract and code-based theories of authorization—they both require objective showing of predetermined zones of authorized access.[151]

In *United States v. Phillips*, the court considered the fact that a university student had clear notice about his restricted zones of authorization as well as the fact that his access to the university's network was against the "expected norms of intended use."[152] In *Phillips*, the defendant was admitted to the computer science program at the University of Texas at Austin, and "[he] signed [the university's] 'acceptable use' computer policy, in which he agreed not to perform port scans using his university computer account."[153] Phillips began using various programs, including a "brute-force attack" designed to scan computer networks and steal encrypted data and passwords, eventually amassing "a veritable informational goldmine by stealing and cataloguing a wide variety of personal and proprietary data, such as credit card numbers, bank account information, student financial aid statements, birth records, passwords, and Social Security numbers."[154] The university brought charges under the CFAA; Phillips was convicted, and he appealed his conviction arguing that the government failed to prove 1) he gained access to the university's computers and website without authorization and 2) he did so intentionally.[155] In analyzing whether Phillips was unauthorized within the meaning of the CFAA, the court relied on the "intended-use analysis" developed by the Second Circuit as well as contract, which provided clear and evident notice that Phillips had about his restricted authorization.[156]

---

[151] *See* Kerr, *supra* note 7, at 1646 ("The difference between regulation by code and regulation by contract resembles the difference between keeping a stranger out by closing and locking the door and keeping a stranger out by putting up a sign in front of an open front door saying 'strangers may not enter.' Importantly, the distinction between regulation by code and regulation by contract is less an on-off switch than a continuum with two extremes. Examples exist that blend the two concepts.").

[152] 477 F.3d 215, 217, 219–20 (5th Cir. 2007).

[153] *Id.* at 217.

[154] *Id.* at 217–18.

[155] *Id.* at 218–19.

[156] *Id.* at 219–21 ("[C]ourts have recognized that authorized access typically arises only out of a contractual or agency relationship."). *See* United States v. Morris, 928 F.2d 504, 510 (2d Cir. 1991) (holding that conduct, like "password guessing" or finding "holes in . . . programs," that uses computer systems not "in any way related to their intended function" amounts to obtaining unauthorized access).

IV. REFORMING THE CFAA

The CFAA, in its current form, does not allow for a predictable determination of access authorization in the context of employment cases.[157] The proposed reforms include 1) Congress amending the statute to remove "exceeding authorization" liability for employment cases; or 2) using judicial policy to eliminate the distinction between authorized and exceeding authorized access for purposes of employer civil action under the CFAA despite its textual presence; and, therefore, 3) the courts limiting judicial inquiry to the unauthorized nature of employee's access without regards to the subjective intention and require the employer to prove a breach of explicit contractual prohibition or a trespass of system code by the employee.

A. Legislative Amendment

Legislative reform can come in the form of striking certain provisions from the statute, or Congress may use statutory exceptions as a mechanism to exempt certain class of cases from the reach of statute's provisions.[158] Exception has the effect of obviating the need for enacting a new statute while preserving the existing statute from constitutional infirmity. Congress should carve out an exception for employment cases in order to similarly improve uniform application of the statute and rescue the CFAA from the gamut of judicial interpretations, which risk imposing liability in relation to a surprising range of innocuous conduct involving employee use of employer computers. An amendment should focus on the primacy of the authorization, or lack thereof, accompanying the access over the subsequent misappropriation of information and information products. A more sensible approach should emphasize that once the access is unauthorized under the CFAA, it should not matter what the defendant subsequently does with the information. A suggested

---

157 *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1583–84 (2010) ("[S]ome courts have taken the view that an employee's authorization is implicitly bounded by whether he is acting as the employee's agent . . . . [O]ther courts have rejected the agency theory of the CFAA.").

158 For example, Congress enacted the Employment Contract Exception to the Federal Arbitration Act providing that nothing contained in the FAA shall apply to contracts of employment of "seamen, railroad employees, or any other class of workers engaged in foreign or interstate commerce." Act of July 30, 1947, ch. 392, 61 Stat. 669 (1947) (codified as amended at 9 U.S.C. § 1 (2010)).

exception could be:

18 U.S.C. § 1030(k):
Application of Statute to Employment Cases

Employee Liability for Unauthorized Access: Except as otherwise provided in sub-clauses (II), (III), (IV) and (V) of subsection (c)(4)(A)(i), an employee is liable for damages or loss resulting from the unauthorized access to employer's protected computer information only when such access is made in violation of or circumvention of the employer's code-based[159] or contractual restriction for which the employee knows or should reasonably know was in force at the time of such access. In controversies between an employer and an employee, the provision of this subsection modifies and limits the provisions of subsection (c)(4)(A)(i)(I) to the extent the two provisions conflict.

Exception to Employee Liability: Subject to §1030(k)(1), an employee is not liable for damages or loss in a civil action for access "in excess of authorization" under this section in connection with his access to the employer's protected computer information in the following situations:

Notwithstanding his subjective intent, an employee is not liable under this subsection for unauthorized access or access in excess of authorization if the employee gains access to employer's computer information using the physical or technical code issued to the employee by the employer;

Notwithstanding his subjective intent, an employee is not liable under this subsection for unauthorized access or access in excess of authorization if the employee's access is otherwise within the terms of a contractual agreement in force with his employer respecting the duration, method of access, and use of such access.

Contributory Negligence: In a civil action for damages under this section, if the employer is negligent for failing to adopt a reasonable code-based restriction or failing to use a valid contract to define the zones of authorized access and the failure is determined to be a contributory factor in the suit, then the employer's relief shall be reduced to the extent the trier of facts determines that such negligence by the employer contributed to controversy.

Application to other Statutes: Nothing in this subsection shall

[159] Code-based restriction may probably need to be defined under a new 18 U.S.C. § 1030(e)(13) (definition section of the statute). The term "code-based restriction" means an arrangement of symbols, signs or letters, whether physical, electronic, biometric, magnetic or verbal, that an owner of a protected computer under this title has issued to an accessor for the purposes of verifying the assessor's authority to access the owner's computer information system.

operate to limit the employer's exercise of his rights under other applicable federal or state laws.[160]

B. Judicial Exemption

Commentators have identified "a congressional intent to give courts greater discretion in determining the meaning of 'authorized access' in employment cases."[161] Moreover, courts historically have not hesitated to set policy, including the use of judicially-created exemptions to fill the gap between congressional statutory inaction and the amendment process. Sometimes, judicially-created exemptions to statutory rules become entrenched as part of the federal common law.[162] Courts certainly have the discretion and should set policy in respect to the reach of the CFAA to employee access cases.[163] Accordingly, and for reasons already discussed above, courts should reject the application of agency law and the corollary employee-mindset exploration to the CFAA access authorization jurisprudence.

A narrower approach to the CFAA authorization analysis that focuses on both code and contract-based approaches has the benefits of promoting predictability in case outcomes as well as maximizing judicial economy. This approach asks the employer to invest resources upfront, establishing and clarifying zones through which employees may navigate in the normal course of their employment, and to use contractual mechanisms to provide

---

[160] Including, but not limited to, those rights and remedies afforded under 17 U.S.C. § 501 *et seq*. (infringement of copyright), as well as those afforded under state statutes regarding the misappropriation of trade secrets. *See* 17 U.S.C. §§ 501–06 (2010).

[161] Field*, supra* note 24, at 838–39 (equating Congress's failure to define authorization under the CFAA, as well as its silence in addressing employee computer crimes despite repeatedly amending the statute to cover new and other specific types of computer crimes, to a determination to leave the authorization question to the courts).

[162] *See, e.g.*, Gonzales v. O Centro Espírita Beneficente União do Vegetal, 546 U.S. 418, 432–34 (2006) (interpreting the Religious Freedom Restoration Act (RFRA), the court said "*judicially crafted* exceptions" are relevant when applying the RFRA's compelling interest test and "*courts* would recognize [judicially crafted] exceptions-that is how the law works"); Petruska v. Gannon Univ., No. 1:04-cv-80, 2008 WL 2789260, at *5 (W.D. Pa. Mar. 31, 2008) ("'[T]he ministerial exception is not a doctrine borne of any express statutory exemption,' but is rather 'a judicially created doctrine . . . .'" (quoting Petruska v. Gannon Univ., 350 F. Supp. 2d 666, 681 (W.D. Pa. 2004))).

[163] *See* Elmendorf v. Taylor, 23 U.S. 152, 159 (1825) ("[T]he judicial department of every government . . . is the appropriate organ for construing the legislative acts of that government.").

notice to employees about unacceptable computer behavior.

Employers who make these minimum investments upfront are likely to benefit from judgment as a matter of law in a litigation context because code and contract-based approaches are fairly easy to decide objectively.[164] Abrogating the "exceeding authorization" analysis from CFAA employment cases reduces procedural redundancies. Consider the classical definition of "exceeds authorization" as used by Congress: "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."[165] When someone is not *entitled* to obtain or alter particular information, the plain meaning of that prohibition is that they are not authorized to *access* the information in the first place and has also appeared to confuse "access" with "use." In other words, Congress has defined access that "exceeds authorization" as a variant of "unauthorized access." Reconciling these two definitions in the employment context should require the courts to subsume the definition of the one into the other; thus, employers should have the burden of persuading the trier of fact that the employee was acting without authorization for the particular access under review—a burden which should be met when employer can demonstrate an objective restriction on employee's authority for which the employee knew or should know was in operation at the time of the alleged access.

V. CONCLUSION

There is a need to reform the existing CFAA. Reform can come in the form of a legislative amendment or a judicially created exemption that achieves the same end. Continued discordance amongst the circuits only serves to diminish predictability in CFAA litigation, whereas uniformity around the most effective option can be best achieved if courts take a narrow view regarding the meaning of unauthorized access within the CFAA. The narrow view is congruent with the common law of trespass

[164] *See generally* Field, *supra* note 24, at 849–51 (discussing how varying contract terms may affect judicial interpretation, inferring that specifically worded contracts can lead to easy interpretation by the court, and discussing how code-based approaches may lead to clearer court decisions under the CFAA).

[165] 18 U.S.C. § 1030(e)(6) (2010).

claims, which is the bedrock of most computer security laws.[166] This view obviates the need for a burdensome judicial exploration into the employee mindset and instead seeks to determine whether the employee has breached objectively determinable contractual terms or physical and technical codes limiting employee's access to employer's commercial and business information. Unauthorized access should be narrowly construed under the CFAA because unauthorized use is covered under other existing and appropriate federal and state laws.

In the meantime, employers can be well served by a few due diligence strategies. Employers should ensure that the methods for generating codes are not easily "hackable" and do not conform to a consistent pattern for all employees. While this may not prevent a truly determined rogue employee from trying to gain unauthorized access, employers can gain useful evidence of circumvention that may bolster its claims under the CFAA. Employers can also incorporate the use of forensic analysis to routinely detect misuse or patterns of access by employees.[167] These steps are necessary for at least three reasons. First, awareness of routine inspection can deter wrongful access of employer systems by employees. Secondly, awareness of the patterns of employees' computer access has instructive value for planning an effective secure information system. And finally, some of the due diligence steps discussed above have the added value of facilitating the gathering and preserving of evidence that may be crucial for civil litigation.

[166] *See supra* text accompanying note 45.

[167] Cundiff, *supra* note 123, at 727–28 ("Where [forensic] imaging seems prohibitively expensive, a second-best alternative may be to have a Company employee carefully review and inventory the contents of the computer.").

Schedule 1—Table Showing How the Circuits Split

Court	Case Name	Year	Accepted Agency	Rejected Agency	Additional Grounds for Determination
1st Cir.	*EF Cultural Travel BV v. Explorica, Inc.*	2001	X[168]		violation of contract/ policies/ norm
(D. Mass)	*Guest-Tek Interactive Entm't Inc. v. Pullen*	2009	X[169]		
2nd Cir.	*Nexans Wires S.A. v. Sark-USA, Inc.*	2006			employer could not prove loss[170]
(N.D.N.Y.)	*Penrose Computer Marketgroup, Inc. v. Camin*[171]	2010			
3rd Cir.[172]					
(W.D. Pa.)	*Consulting Prof'l Res., Inc. v. Concise*	2010		X[173]	

[168] 274 F.3d 577, 580–84 (1st Cir. 2001) (finding that employee's use of data was against employer's interest and also that breach of a broadly written confidentiality agreement amounted to "unauthorized access").

[169] 665 F. Supp. 2d 42, 45–46 (D. Mass. 2009) (holding in favor of the broader agency theory by noting that while the First Circuit has not expressly addressed the meaning of "unauthorized access" or "exceeded authorization" in the agency context, its ruling nonetheless supports a broader interpretation of the statutory language).

[170] 166 F. App'x 559, 562-63 (2d Cir. 2006) (affirming district court's summary judgment dismissing the case, as the employer could not demonstrate a recoverable loss under, thus never interpreting the language of the CFAA). The Second Circuit still has not had the opportunity to rule on the definitions contained in the CFAA. *See* Penrose Computer Marketgroup Inc. v. Camin, 682 F. Supp. 2d 202, 210 (N.D.N.Y. 2010) ("[T]he Second Circuit Court of Appeals has not addressed this issue.").

[171] 682 F. Supp. 2d at 210–12 (finding for the defendant-employee). However, the court was not explicit as to whether plaintiff's argument failed due to failure of the agency argument, or because the defendant's use was authorized under an agency agreement. *Id.*

[172] The Court of Appeals for the Third Circuit has not taken a position on the "unauthorized access" debate, but it has recognized the trend among employers to employ the "'CFAA's civil remedies to sue former employees and their new companies who seek a competitive edge through wrongful use of information from the former employer's computer system.'" *See* P.C. Yonkers, Inc. v. Celebrations the Party and Seasonal Superstore LLC, 428 F.3d 504, 510 (3d Cir. 2005) (quoting Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196 (E.D. Wash. 2003)).

[173] No. 09-1201, 2010 WL 1337723, at *6 (W.D. Pa. Mar. 9, 2010) ("This court likewise declines to construe the CFAA by reliance upon agency principles where the defendant's intent governs whether the access was without authorization or exceeded authorized access.").

	Techs. LLC				
4th Cir.					
(E.D. Va.)	*State Analysis, Inc. v. Am. Fin. Servs. Assoc.*	2009		X[174]	
5th Cir.	*United States v. Phillips*	2007			Violation of contract/ policies/ norm[175]
	United States v. John	2010	X[176]		Violation of contract/ policies/ norm
6th Cir.[177]					
(M.D. Tenn)	*ReMedPar, Inc. v. AllParts Med., LLC*	2010		X[178]	
7th Cir.	*Int'l Airport Ctrs., L.L.C. v. Citrin*	2006	X[179]		
8th Cir.[180]					‘
(C. Div. Iowa)	*NCMIC Fin. Corp. v. Artino*	2009	X[181]		

[174] 621 F. Supp. 2d 309, 316–17 (E.D. Va. 2009) (explaining that Plaintiff did not allege that the defendant "obtained or altered any information it was not entitled to," and the allegation of "us[ing] the information in an inappropriate way . . . do[es] not state a claim [under the CFAA]" thus, the defendant's motion to dismiss this claim will be granted).

[175] 477 F.3d 215, 221 (5th Cir. 2007) ("[C]ourts have recognized that authorized access typically arises only out of a contractual or agency relationship.").

[176] 597 F.3d 263, 273 (5th Cir. 2010) ("[W]hen an employee knows that the purpose for which she is accessing information in a computer is both in violation of an employer's policies and is part of an illegal scheme, it would be 'proper' to conclude that such conduct 'exceeds authorized access' within the meaning of § 1030(a)(2).").

[177] The Sixth Circuit has not had reason to interpret this provision. *See* ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 610 (M.D. Tenn. 2010) ("The Sixth Circuit has not addressed the issue . . . .").

[178] 683 F. Supp. 2d 605, 611–13, 616 (M. D. Tenn. 2010) **(**explaining how this court was persuaded in its decision by the reasoning adopted in the 9th circuit, which "specifically reject[s] the agency theory of authorization.").

[179] 440 F.3d 418, 420–21 (7th Cir. 2006). The first of all the circuit courts to explicitly endorse using the CFAA against employees who steal their employers' data based on the RESTATEMENT (SECOND) OF AGENCY § 112 (1958). *See id.*; Greg Pollaro, Article, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope,* 2010 DUKE L. & TECH. REV. 12, ¶¶12–13, 16 (2010)**.**

[180] NCMIC Fin. Corp. v. Artino, 638 F. Supp. 2d 1042, 1056–57 (C. Div. Iowa 2009) ("The Eighth Circuit has not yet ruled on the issue . . . .").

[181] 638 F. Supp. 2d 1042, 1056–59 (C.Div. Iowa 2009) **(**adopting the broad view that when an employee accesses information to the detriment of his employer, thus violating his duty of loyalty to his employer, he will be liable under the CFAA**).**

9th Cir.	*LVRC Holdings LLC v. Brekka*	2009		X[182]	
10th Cir.	*Triad Consultants, Inc. v. Wiggins*	2007			Employee obtained nothing of value, even if allegations were true.[183]
(D. Kan.)	*US Bioservices Corp. v. Lugo*	2009		X[184]	
11th Cir.					
(M.D. Fla.)	*Clarity Servs., Inc. v. Barney*	2010		X[185]	Employer placed no restrictions and employee obtained nothing of value
D.C. Cir.[186]					
D. D.C	*Lewis-Burke Assocs. v. Widder*	2010		X[187]	

[182] 581 F.3d 1127, 1133–35 (9th Cir. 2009) ("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.").

[183] 249 F. App'x 38, 40–41 (10th Cir. 2007). The Tenth Circuit had the occasion to, but avoided addressing the question in *Triad Consultants, Inc.*. *Id.* at 40 ("We need not decide whether [Employee] 'accesse[d] a protected computer without authorization, or exceed[ed] authorized access,' or furthered a fraudulent intent by doing so." (alteration in original) (quoting 18 U.S.C. § 1030(a)(4))).

[184] 595 F. Supp. 2d 1189, 1194 (D. Kan. 2009) ("[T]he court follows the line of cases that have rejected a reading of the CFAA by which the defendant's intent may determine whether he has acted without authorization or has exceeded his authorized access.").

[185] 698 F. Supp. 2d 1309, 1315–17 (M.D. Fla. 2010) (rejecting as overly broad the argument that an employee's authorization terminates at the point his or her interest becomes adverse to an employer).

[186] Lewis-Burke Assocs. v. Widder, 725 F. Supp. 2d 187, 192 (D. D.C. 2010) ("[T]he United States Court of Appeals for the District of Columbia Circuit has not yet considered the issue.").

[187] 725 F. Supp. 2d 187, 193–94 (D.D.C. 2010) (reasoning that whether the defendant exceeded his authorization depends on the actions taken by his employer).