Hamline Law Review

Volume 36
Issue 1 *Comparative Papers From the Administrative Law Discussion Forum*

Article 5

1-30-2014

Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail

Samantha Jensen
Hamline University School of Law, sjensen06@hamline.edu

Recommended Citation
Jensen, Samantha (2013) "Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail," *Hamline Law Review*: Vol. 36: Iss. 1, Article 5.
Available at: http://digitalcommons.hamline.edu/hlr/vol36/iss1/5

ABUSING THE COMPUTER FRAUD AND ABUSE ACT: WHY BROAD INTERPRETATIONS OF THE CFAA FAIL

Samantha Jensen[*]

[*] Juris Doctor expected at Hamline University School of Law, May 2014. I would like to thank my editors, Patty Devoy and Jenna Grembowski, for their guidance and dedication in helping bring my article to fruition. I would also like to thank Liz Winchell for her encouragement and inspiration throughout the process, as well as my family for being a pillar of support.

I. INTRODUCTION

It is likely that many, if not most, employees in the United States are unfamiliar with the Computer Fraud and Abuse Act (CFAA), despite the ubiquitous use of computers in the workplace.[1] The CFAA is a federal criminal statute, implemented to prosecute computer hacking at a time far removed from today's technological landscape.[2] Currently one of the broadest criminal laws in the United States Code, the CFAA potentially affects anyone who uses a computer.[3] Despite the statute's criminal stature, employers are increasingly using its civil provision to haul disloyal employees into federal court.[4]

A typical employer CFAA cause of action alleges that an employee obtained information by accessing a computer either without authorization or in a manner that exceeded the employee's authorized access.[5] Whether the

[1] Sarah Boyer, *Computer Fraud and Abuse Act: Abusing Federal Jurisdiction*, 6 RUTGERS J.L. & PUB. POL'Y 661, 664 (2009) (describing how the nature of business has changed significantly over the past twenty-five years as a result of technological advances).

[2] *See infra* Part II.A (detailing the initial enactment of the CFAA).

[3] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1561 (2010) (describing how amendments to the CFAA potentially regulate use of every computer in the United States and millions abroad).

[4] Michael D. Scott, SCOTT ON INFORMATION TECHNOLOGY LAW, § 17.12 (3d ed. 2012) (describing how employers are increasingly pursuing claims under the CFAA against employees who use company computers for personal reasons); *see also* Lee v. PMSI, Inc., No. 8:10 CV 2904 T 23TBM, 2011 WL 1742028, at *1, *3 (M.D. Fla. May 6, 2011) (dismissing a counterclaim by employer who alleged CFAA violation for employee's use of Facebook on company computer); *see also* Clarity Servs., Inc. v. Barney, 698 F. Supp. 2d 1309, 1316 (M.D. Fla. 2010) (expressing skepticism that an employee violates the CFAA simply by checking personal e-mail at work).

[5] Molly Eichten, *The Computer Fraud and Abuse Act–A Survey of Recent Cases*, 66 BUS. LAW 231, 232 (2010). The typical employer CFAA claim involves an employee who

CFAA is limited to hacking or extends to employees who misuse company computers hinges entirely on how a court interprets the terms "without authorization" and "exceeds authorized access."[6] Applying the CFAA to this common situation has resulted in a split of authority as courts struggle with the definition of "authorization."[7]

Some courts construe the term "authorization" narrowly.[8] An employee's misuse or misappropriation of the employer's business information is not "without authorization" as long as the employer gave the employee permission to access the information.[9] Once an employee is granted authorization to access an employer's computers, the CFAA is not violated despite subsequent misuse of the information.[10] Other courts construe the term broadly, recognizing an employer's cause of action when an employee obtains business information with disloyal intent or in breach of an agreement.[11]

The CFAA's vast reach, along with commonplace use of computers in business, makes it critical to clearly define the statute's scope.[12] Unfortunately, the divisive split brings more questions than clarity and allows the CFAA to be used in unprecedented ways.[13] With the Supreme Court's recent dismissal of a *certiorari* petition on the issue and Congressional efforts focused elsewhere, courts are faced with the responsibility of clearly and accurately interpreting the CFAA.[14]

obtains confidential or proprietary information from the employer's computer system while still employed but subsequently leaves the company. *Id.* at 232–33. The employee then uses information to the employer's detriment, often in direct competition with the employer. When discovered, employers bring claims against the employee under the CFAA, often with state tort claims for breach of contract.

[6] *Id.* at 231.

[7] Ajuba Intl. LLC v. Saharia, 871 F. Supp. 2d 671, 685–87 (E.D. Mich. 2012) (detailing the current circuit split of authority regarding whether the CFAA applies in employer-employee situations).

[8] LVRC Holdings, LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009) (holding that an employee acts without authorization when he has no permission to access computers at all or such permission is rescinded).

[9] *Id.*

[10] *Ajuba,* 871 F. Supp. 2d at 687.

[11] *See* Int'l Airport Ctr., LLC v. Citrin, 440 F.3d 418 (7th Cir. 2006); EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001) (identifying agency-based interpretation in *Citrin* and a contract-based interpretation in *Explorica*).

[12] Paul J. Larkin, Jr., *United States v. Nosal: Rebooting the Computer Fraud and Abuse Act*, 8 SETON HALL CIRCUIT REV. 257, 261 (2012) (lamenting the need for more specificity in determining which actions create liability under the CFAA as the CFAA can be used in unprecedented ways not intended by Congress).

[13] *Id.*

[14] WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199 (4th Cir. 2012), *cert. dismissed*, 133 S. Ct. 831; *see also* Alan W. Nicgorski, *Employees Exceeding Authorized Access? Trends in Interpreting the Computer Fraud and Abuse Act*, 30 No. 18 WESTLAW J. COMPUTER & INTERNET 1 (2013) (describing how a recent spark in Congressional efforts to amend the CFAA has seemingly stalled); *see also* Sebastian E. Kaplan, *The Rise of the Computer Fraud and Abuse Case*, 17. No. 4 CYBERSPACE LAW 14, 14 (2012) (explaining

This Comment contends that broad interpretations of the CFAA implicate constitutional vagueness and overbreadth concerns, are inconsistent with the underlying policy of the statute, and result in inappropriate federal jurisdiction for traditional state law claims.[15] Only a narrow interpretation of the CFAA keeps the statute constitutional and fulfills Congress's original and primary intent to punish criminal computer hackers and people who abuse legitimate access privileges.[16]

Part II of this Comment examines the history and legislative intent behind the CFAA, focusing on the types of crime Congress targeted and the balance Congress intended to strike by not preempting the field of computer crimes.[17] Part II also traces the important amendments throughout the statute's relatively short history and details current actions under the CFAA.[18] Part III explores several relevant doctrines and canons of statutory construction that courts should consider when interpreting the CFAA.[19]

Part IV discusses the current circuit split, summarizing the development and rationale behind each theory.[20] It examines how each theory handles "authorization," and how employers fare when presenting misappropriation claims.[21] Part V contends that broad interpretations of the CFAA do not meet constitutional requirements under the void for vagueness doctrine or the doctrine of overbreadth.[22] Moreover, courts applying a broad interpretation of the CFAA shirk their duty to effectuate Congressional intent by avoiding established canons of statutory construction and demolish Congress's intended scope by trampling existing state laws.[23] In addition to enumerating the deficiencies of broad interpretations, Part V also outlines how a narrow interpretation's restrained reading of the statutory language complies with relevant doctrines, follows canons of construction, and

current Congressional proposals include Senator Leahy's revision to limit liability to exceeding authorized access to seven categories of sensitive information, and Senators Grassley and Franken's proposal to carve out an exception to the statute for violating terms of service agreements).

[15] *See infra* Part V (arguing why the CFAA requires a narrow interpretation).

[16] *See infra* Parts IV–V (concluding that a narrow interpretation comports with the intent of the CFAA and canons of construction).

[17] *See infra* Part II.A–D (outlining why the CFAA was enacted, discussing the exact type of crime and scope that Congress intended for the CFAA to cover).

[18] *See infra* Part II.E–F (describing amendments of the CFAA and current actions).

[19] *See infra* Part III (outlining various doctrines and canons of statutory construction).

[20] *See infra* Part IV (detailing the current circuit split).

[21] *See infra* Part IV (describing the effect of each theory).

[22] *See infra* Part V.A–B (contending that agency and contract-based interpretations of the CFAA do not provide the required notice to meet due process concerns, and leave the CFAA vulnerable to arbitrary enforcement and overbreadth concerns).

[23] *See infra* Part V.C–E (describing the deficiencies of broad interpretations through their noncompliance with doctrines, canons of statutory construction, and avoidance of Congressional intent).

effectuates Congressional intent.[24] This Comment concludes that the only way to keep the CFAA constitutional is for courts to interpret it narrowly; any other interpretation undermines the purpose and scope of the statute while raising constitutional concerns.[25]

II. BACKGROUND

Although computer crime statutes exist in all fifty states and on the federal level today, they remain a relatively new concept.[26] The Counterfeit Access Device and Computer Fraud and Abuse Act, more commonly referred to as the CFAA, was enacted in 1984 and is the primary federal statute used to combat computer crime.[27] The CFAA criminalizes accessing a computer without authorization or accessing a computer by exceeding the authorization given.[28] Originally narrow in scope and aimed at criminal hackers, rapidly advancing technology and expansive amendments exploded the CFAA's use, transforming it into one of the most far-reaching criminal statutes in the United States Code.[29] A surge in the number of CFAA claims brought by employers against disloyal employees followed a 1996 update to the definition of "protected computers."[30] Consequently, a majority of the law addressing the meaning and scope of the CFAA developed within the context of employment disputes.[31] Despite numerous amendments and

[24] *See infra* Part V (demonstrating the benefits of narrowly interpreting the CFAA).

[25] *See infra* Parts V–VI (explaining how a narrow interpretation is the only way to keep the CFAA constitutional and to effectuate the legislative intent).

[26] Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statute*, 78 N.Y.U. L. REV. 1596, 1615 (2003) (noting that Florida was the first state to pass a computer crime statute in 1978, and Vermont was the last state to pass its version of a computer crime statute in 1999. Congress passed the first federal statute in 1984).

[27] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, PUB. L. NO. 98-473, § 2102(a); § 98 Stat. 2190, 2190–92. Initially enacted in 1984, § 1030 became known as the CFAA with the 1986 amendments; *see also* S. REP. NO. 104-357, at 5 (1996) ("[a]s intended when the law was originally enacted, the Computer Fraud and Abuse statute facilitates addressing in a single statute the problem of computer crime, rather than identifying and amending every potentially applicable statute affected by advances in computer technology.").

[28] 18 U.S.C. § 1030(a)(2)(c); *Ajuba*, 871 F. Supp. 2d at 684.

[29] *See* U.S. DEPT. OF JUSTICE PROSECUTING COMPUTER CRIMES, at 2 (2007) available at http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf. The CFAA has been amended multiple times as Congress attempts to keep pace with changes in technology. Initially enacted in 1984, subsequent amendments followed in 1986, 1988, 1989, 1990, 1994, 1996, 2001, 2002, and 2008. *Id. See also* Kaplan, *supra* note 14, at 14 (tallying a 600% increase in complaints alleging a cause of action under the CFAA since 2002).

[30] Peter A. Winn, *The Guilty Eye: Unauthorized Access, Trespass, and Privacy*, 62 BUS. LAW 1395, 1408 (2007). After the CFAA's 1996 amendments, the number of civil cases quickly eclipsed the number of criminal cases prosecuted. *Id.*

[31] United States v. Drew, 259 F.R.D. 449, 456–57 (C.D. Cal 2009) (explaining that a majority of CFAA case law has been developed in the context of civil cases).

repeated use of the term throughout the statute, "without authorization" remains undefined.[32] A predicate for liability under the CFAA, this undefined term has led to a three-way split of authority concerning the proper interpretation of the terms "without authorization" and "exceeds authorized access."[33]

A. The Need for a Computer Crime Statute Becomes Obvious

Understanding the problem Congress faced and identifying the type of behavior Congress intended to target through the CFAA is critical to defining the statute's proper scope.[34] Subdividing computer crimes into two categories—traditional crimes committed using computers, and crimes of computer misuse—helps demonstrate the specific type of crime the CFAA was enacted to target.[35] Congress's aim in enacting the CFAA was specifically to deter and combat only crimes of computer misuse.[36]

Traditional crimes using computers involve the online commission or facilitation of traditional criminal offenses that ordinarily do not include a computer.[37] The elements of such crimes are not affected by the use of a computer and remain susceptible to federal prosecution under existing criminal statutes.[38] For example, a death threat is still a death threat whether sent through email or postal mail; the involvement of a computer does not affect the ability to prosecute the crime.[39] These traditional crimes using

[32] *See* 18 U.S.C. § 1030 (2006); *see also* S. REP. NO. 99-432, at 13 (1986) ("without authorization" contained in § 1030(a)(1), (2), (3), (4), (5)(A), (5)(B), (5)(C), (6), and (7)(B) was not defined because Congress thought it was "self-explanatory").

[33] *Ajuba*, 871 F. Supp. 2d at 686 (describing the current split of authority concerning the proper interpretation of "without authorization" and "exceeds authorized access" before ultimately deciding that the narrow interpretation is the better approach).

[34] Kerr, *supra* note 26, at 1602. Computer crime statutes were a response to perceived failures of preexisting laws to respond to crimes of computer misuse. Amendments to the CFAA were enacted to address changes in computer technology, "particularly new computer abuse techniques such as computer viruses and worms, which make prosecutions difficult in some types of cases." *Id*. *See also* S. REP. NO. 101-544 (1990).

[35] *See* Kerr, *supra* note 26, at 1602–05. Scholar Orin Kerr's categorical approach to computer crimes helps clearly delineate Congress's targeted crimes.

[36] S. REP. NO. 101-544 (1990).

> Overall, existing criminal statutes provide an adequate framework for the prosecution of most types of computer-related criminal conduct. Existing fraud, embezzlement, theft, and destruction of property statutes can be used to punish those who commit these types of offenses with the assistance of a computer. However, as computer criminals become more sophisticated, using viruses, worms and other types of computer software and hardware to commit heretofore unanticipated offenses, the criminal code must be readjusted to keep up with these developments.

Id.

[37] Kerr, *supra* note 26, at 1602–03.

[38] *Id.* Examples of traditional crimes committed using computers include internet fraud schemes, online distribution of child pornography, and cyberstalking.

[39] *Id.*

computers did not require new laws to protect against abuse at the state level either, since a hallmark of federalism placed these issues squarely within state police powers.[40]

Computer misuse crimes, on the other hand, represented a new type of crime.[41] Computer misuse crimes consist of conduct that intentionally, knowingly, recklessly, or negligently causes interference with the proper functioning of computers and computer networks.[42] Common computer misuse crimes include hacking or distributing viruses.[43] The government had difficulty prosecuting computer misuse crimes under traditional criminal statutes like trespass, burglary, and theft because the elements of traditional crimes tie closely to the physical world, while the elements of computer misuse crimes do not.[44] For example, a computer hacker can illicitly steal a computer program without physically trespassing or depriving the owner of possession.[45] Even though the hacker has committed a wrongful act, prosecution under traditional trespass, burglary or theft statutes would be difficult because elements such as the defendant's physical intrusion onto the owner's property, or the defendant physically depriving the owner of his property, are not met.[46] The CFAA was created to protect people and property against only these new computer misuse crimes by filling in gaps where existing crime statutes could not account for the unique problem posed by computer data.[47]

[40] *Id.; see also* Gonzales v. Raich, 545 U.S. 1, 66 (2005) (referencing the state's "traditional police powers to define the criminal law and to protect the health, safety, and welfare of their citizens"); *see also* Advanced Aerofoil Techs., AG v. Todaro, No. 11 Civ 9505, 2013 WL 410873 at *8 (S.D.N.Y. Jan. 30, 2013) (dismissing an employer's CFAA claim alleging misuse of company information, but noting that employer may still have remedies available to it under state and common law).

[41] H.R. REP. NO. 98-894, at 20 (1984) *as reprinted in* 1984 U.S.C.C.A.N. 3689, 3695 ("[i]t is obvious that traditional theft/larceny statutes are not the proper vehicle to control the spate of computer abuse and computer assisted crimes.").

[42] Kerr, *supra* note 26, at 1603–04. This type of conduct misuses and violates the rights and privileges that the computer or account owner expects to have over their computer or account. *Id.*

[43] *Id.*

[44] Kerr, *supra* note 26, at 1605–11. For example, traditional trespass and burglary require the defendant to physically trespass on someone else's property, and deprive the rightful owner of physical possession. The limited scope is difficult to apply to computer misuse because the user doesn't physically enter another's property, or physically misappropriate a tangible thing. Even when courts identified a computer as a property interest, it became difficult to explain how computer misuse actually deprived the owner of that property.

[45] *Id.*

[46] *Id.*; *see also* H.R. REP. NO. 98-894, at 10 (1984) (explaining why computer misuse crimes did not fit well into categories of property subject to abuse or theft).

[47] Garrett D. Urban, *Causing Damage Without Authorization: The Limitations of Current Judicial Interpretations of Employee Authorization Under the Computer Fraud and Abuse Act*, 52 WM. & MARY L. REV. 1369, 1388–89 (2011). Congress's intent was for the CFAA to target new forms of computer crimes not currently addressed by federal or state criminal statutes. Despite technological advances, using computers to carry out traditional

B. The Initial Enactment of the CFAA in 1984

Computer crime statutes did not exist when computer misuse became a cognizable problem in the 1970s.[48] The federal government responded to these new crimes by enacting the first computer-crime statute as part of the Comprehensive Crime Control Act of 1984.[49] Consciously narrow in scope and aimed at hackers, the statute was limited to protecting classified information, financial records, and credit information stored on computers owned by the government and financial institutions.[50]

Unfortunately, the concentrated scope of the 1984 statute drew immediate criticism from legislatures, industry leaders, and law enforcement officials.[51] The limiting language in the original version was so narrowly drawn that the statute could not be effectively used.[52] The statute's ineffectiveness coupled with the increasing use of computers in public and private sectors led to significant changes in 1986.[53]

crimes did not require new laws, and had always been implemented and enforced by states as part of their police powers.

[48] Katherine Mesenbring Field, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 835 (2009) (detailing the legislative history and concluding that the CFAA seeks to capture crimes of computer misuse rather than traditional offenses using a computer).

[49] H.R. REP. NO. 98-894, at 20 (1984). "It is noteworthy that section 1030 deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer." The conduct prohibited in the CFAA is analogous to breaking and entering rather than using a computer (similar to the use of a gun) in committing a crime. Specifically, the CFAA targets crimes where the computer is the victim and not crimes that simply use a computer to commit another traditional crime. *See also* Charles Doyle, *Cybercrime: An Overview of the Federal Computer Fraud and Abuse Statute and Related Federal Criminal Laws, Congressional Research Service*, 7-5700 Dec. 27, 2010 at 1 (describing the CFAA as, "not a comprehensive provision, but instead it fills cracks and gaps in the protection afforded by other federal criminal laws.").

[50] *Id.* Legislators considered and rejected a broader scope, concentrating instead only on the most vital federal interests. *See* Dodd S. Griffith, *The Computer Fraud and Abuse Act of 1986: A Measured Response to A Growing Problem*, 43 VAND. L. REV. 453, 455–56 (1990).

[51] Frank P. Andreano, *The Evolution of Federal Computer Crime Policy: The Ad Hoc Approach to An Ever-Changing Problem*, 27 AM. J. CRIM. L. 81, 86 (1999); *see also* 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 at 1 (2001); *see* Griffith, *supra* note 50, at 485 (noting the widespread dissatisfaction with the original statute. Described as both "overly vague and too narrow in scope," prosecution proved difficult under the statute which decreased its deterrent value).

[52] S. REP. No. 99-432, at 6 (1986). The original statute limited the information protected by referencing the Right to Financial Privacy Act. Recognizing that important financial information existed outside the scope of this narrow Act, Congress extended the protection to financial records of all customers of financial institutions.

[53] *See* S. REP. NO. 99-432, at 3-4 (1986); *see also* Griffith, *supra* note 50, at 483. The 1986 amendments were necessary to broaden protection to cover private sector computers and facilitate federal prosecution of computer-related crimes.

C. The 1986 Amendments: The CFAA is Born

The extensive 1986 amendments gave the statute its current name: the Computer Fraud and Abuse Act (CFAA).[54] Congress expanded the statute's scope by modifying existing crimes, adding new offenses, changing intent requirements, and adding definitions.[55] Despite the statute's increased scope, its premise remained the same and Congress kept the CFAA's jurisdiction limited to crimes involving a compelling federal interest.[56]

Congress made several changes to remove accidental access and the use of legitimately obtained information from the CFAA's scope.[57] Additionally, Congress added a subsection to define key terms and expand the definition of "federal interest computer."[58] The CFAA initially applied to a person who either (1) knowingly accessed without authorization, or (2) "having accessed a computer with authorization, use[d] the opportunity such access provide[d] for purposes to which such authorization [did] not extend."[59] Congress replaced the latter phrase with the defined term "exceeds authorized access."[60] The term "exceeds authorized access" is defined as "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."[61] Further, "exceeds authorized access" remains an element in multiple

[54] *See supra* note 27.

[55] S. REP. NO. 99-432, at 3–4 (1986).

[56] Buckman, *supra* note 51, at 1 (limiting the CFAA's jurisdictions to cases involving a compelling federal interest). *See also* S. REP. NO. 99-432, at 3–4 (1986) ("The premise . . . will remain the protection, for privacy reasons, of computerized credit records and computerized information relating to customers' relationships with financial institutions. This protection is imperative in light of the sensitive and personal financial information contained in such computer files.").

[57] Griffith, *supra* note 50, at 463 (changing the language to ensure that the provision would not be construed to prohibit computer access for legitimate business purposes, the Senate report stated the sole purpose of subsection (a)(2) was to "deter hackers and other criminals from accessing computerized financial files without authorization.").

[58] Andreano, *supra* note 51, at 86–87; 18 U.S.C. § 1030(e)(2)(B) (Supp. IV 1987) (expanding the definition of a "federal interest" computer to cover crimes committed using computers in more than one state).

[59] PUB. L. NO. 98-473 § 2102, 98 Stat. 2190, 2190–91 (1984).

[60] *See* S. REP. NO. 99-432, at 21 (1986) (stating the reason for the amendment was to eliminate coverage for authorized access used for improper purpose).

> This removes from the sweep of the statute one of the murkier grounds of liability, under which a Federal employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed his authorization. As the committee report points out, administrative sanctions should ordinarily be adequate to deal with real abuses of authorized access.

Id.

[61] *See* 18 U.S.C. § 1030(e)(6); *see also* Walsh Bishop Assocs., Inc. v. O'Brien, No. 11-2673, 2012 WL 669069 at *3 (D. Minn. Feb. 28, 2012) (concluding that the reason for the amendment was to remove use as a basis for exceeding authorization).

CFAA provisions.[62] Even though Congress included definitions for several key terms, "without authorization" remains undefined.[63]

Primarily designed to punish and deter the theft of information from outside hackers, legislative history affirms that Congress always intended for the CFAA to apply to insiders who intentionally damaged protected computers.[64] This distinction is expressed in the statutory language: outsiders would be "without authorization" while insiders would "exceed authorized access."[65] Outside intruders accessing a protected computer "without authorization" faced criminal liability for any intentional, reckless, or even negligent, damage caused by their trespass.[66] Congress raised the intent standard from "knowingly" to "intentionally" in several subsections to emphasize that "intentional acts of unauthorized access—rather than mistaken, inadvertent, or careless ones—are precisely what the Committee intends to proscribe."[67]

[62] Andreano, *supra* note 51, at 87.

[63] *See supra* note 32.

[64] *See* H.R. REP. NO. 98-894, at 20 (1984). The original House Report supporting passage of the first CFAA cited to two cases to illustrate the need for a computer crime statute; both involved unauthorized access by former employees. This indicates Congress was not solely focused on deterring hackers when passing the original CFAA statute; *See also* S. REP. NO. 104-357, at 9 (1996) ("[t]he law currently protects computers or computer systems from damage caused by either outside hackers or malicious insiders. . .'").

[65] S. REP. NO. 99-432 (1986) (Congress distinguishes between the terms "without authorization" and "exceeds authorized access," using the first to apply to outside hackers, and the second applicable only to insiders, i.e. people within a company). A clear example is the amended § 1030(a)(3) which contains the term "unauthorized access" but *not* "exceeds authorized access." Congress removed "exceeds authorized access" to "preclude liability in purely 'insider' cases." *See also* Reid Skibell, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 BERKELEY TECH. L.J. 909, 913 n.16 (2003) (describing an outsider as anyone who intrudes on a computer from outside the organization, as opposed to an insider who exceeds their authorized access by viewing sensitive data or entering into a restricted computer); *see also* S. REP. NO. 104-357, at 8–11 (1996) (detailing the sentencing scheme for the CFAA and the rationale for why insiders and outsiders are treated differently).

[66] S. REP. NO. 99-432, at 5–6 (1986) (explaining that unsure of evolving technology, Congress changed the intent standard to "intentionally" in order to exclude individuals who "inadvertently 'stumble[d] into' someone else's computer file or computer data," especially where such individual was authorized to use a particular computer"); S. REP. NO. 104-357, at 11 (1996) ("[i]nsiders . . . 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.").

[67] S. REP. NO. 99-432, at 7 (1986). Further focusing the scope, the Senate Report clarified that the statute was not meant to cover employees' authorized to access computers that acted in a way that, although wrong, did not rise to the level of criminal conduct.

> It is not difficult to envision an employee . . . who, while authorized to use a particular computer in one department, briefly exceeds his authorized access and peruses data belonging to the department that he is not supposed to look at. This is especially true where the department in question lacks a clear method of delineating which individuals are authorized to access certain of its data. The Committee believes that

D. Congress's Careful Balance Between State and Federal Statutes

Senate reports contain clear evidence that despite widening the scope of the CFAA in 1986, Congress did not intend for the amendments to preempt the entire field of computer crime or to make every offense involving a computer a crime under the Act.[68] Although states had not uniformly addressed the still-emerging issue of computer crimes, forty-seven states had enacted specific computer crime statutes by 1986.[69] Congress rejected proposals to make the statute so sweeping that "no computer crime is potentially uncovered," and decided a more appropriate balance would be to limit the CFAA to crimes concerning a compelling federal interest or crimes interstate in nature.[70] Congress intentionally left room for states to be undisturbed by the moderate reach of the CFAA and able to develop their own solutions to the burgeoning issue.[71]

E. The Civil Provision and Expanded Definitions Continue to Broaden the CFAA's Scope

Congress added the private cause of action to the felony provisions of the CFAA in 1994 to allow victims to recover damages for economic loss

> administrative sanctions are more appropriate than criminal punishment in such a case. The Committee wishes to avoid the danger that every time an employee exceeds his authorized access to his department's computers—no matter how slightly—he could be prosecuted.

Id.

[68] S. REP. NO. 99-432, at 4 (1986). "Throughout its consideration of computer crime, the Committee has been especially concerned about the appropriate scope of Federal jurisdiction in this area." *Id*.

[69] *Id.;* see Griffith, *supra* note 50, at 485 (describing why Congress chose not to preempt a significant body of law by limiting the scope of the CFAA to compelling federal interest).

[70] S. REP. NO. 99-432, at 4; *see* Griffith, *supra* note 50, at 484 (acknowledging "the Judiciary Committee's long-standing policy of limiting federal crimes to matters of compelling federal interest or to criminal acts that state or local governments were incapable of handling.").

[71] Griffith, *supra* note 50, at 484; *see also* S. REP. NO. 99-432, at 4 (1986).

> It has been suggested that, because some States lack comprehensive computer crime statutes of their own, the Congress should enact as sweeping a Federal statute as possible so that no computer crime is potentially uncovered. The Committee rejects this approach and prefers instead to limit Federal jurisdiction over computer crime to those cases in which there is a compelling federal interest, i.e., where computers of the Federal Government or certain financial institutions are involved, or where the crime itself is interstate in nature. The Committee is convinced that this approach strikes the appropriate balance between the Federal Government's interest in computer crime and the interests and abilities of the States to proscribe and punish such offenses.

Id.

against wrongdoers as a civil remedy.[72] Congressional records indicate that the civil provision was a reaction to a dramatic rise in the number of computer crime cases and the government's inability to pursue all of these claims.[73] The civil remedy was designed to provide injured individuals with a remedy and to increase the deterrent value of the statute.[74] Employers enthusiastically embraced this civil remedy as a way to recapture compensatory damages or obtain injunctive relief against former employees.[75]

Increasing national reliance on computer networks mixed with concern over notorious and highly destructive reports of hacking led to further expansions of the statute.[76] Although the term "federal interest computer" was replaced with "protected computer" in 1996, subsequent amendments significantly broadened the term.[77] Addressing the interstate nature of computer networks, in 2008 Congress injected the phrase "affecting interstate commerce" into the definition of "protected computer" to permit jurisdiction as far as its Commerce Clause power allowed.[78] Currently, any

[72] *See* Violent Crime Control and Law Enforcement Act of 1994, PUB. L. NO. 103-322 tit. XXIX § 290001, 108 Stat. 1796 Title XXIX 2097-99 (1994) (codified as amended at 18 U.S.C. § 1030). The 1994 amendments were part of the larger Violent Crime Control and Law Enforcement Act of 1994. In addition to adding a civil provision, § 1030(g), other amendments expanded the statute to apply to computer damage incurred accidentally and even without negligence.

[73] Christine D. Galbraith, *Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites*, 63 MD. L. REV. 320, 329 (2004); 146 Cong. Rec. S10, 916 (daily ed. Oct. 24, 2001) (statement of Sen. Leahy).

[74] S. REP. NO. 101-544, at 9 (1990) (introducing the civil provision as a remedy that "would authorize private suits in an area that law enforcement has sometimes been reluctant to investigate or prosecute. Deterrence is another goal.").

[75] *See* Winn, *supra* note 30 (explaining the increase in CFAA claims by employers).

[76] Kyle W. Brenton, *Trade Secret Law and the Computer Fraud and Abuse Act: Two Problems and Two Solutions*, U. ILL. J.L. TECH. & POL'Y 429, 453 (2009).

[77] The USA Patriotic Act of 2001 expanded "protected computers" to include computers outside the United States if involved in interstate or foreign commerce. The 2008 amendment, part of the Identity Theft Enforcement and Restitution Act, removed the requirement of interstate communication, making any unauthorized access to any protected computer that retrieves any kind of information (either interstate or intrastate) punishable under the statute. A "protected computer" is any computer "which is used in . . . interstate or foreign commerce or communication." 18 U.S.C. § 1030(e)(2)(B) (2012). This broad definition encompasses nearly every computer since a connection to the internet satisfies this requirement. *See* Daniel J. Winters & John F. Costello, Jr., *The Computer Fraud and Abuse Act: A new weapon in the trade secrets litigation arena*, INTELLECTUAL PROPERTY, Vol. 44, No. 3 April 2005.

[78] S. REP. NO. 101-544, at 9 (1990) (explaining that the Commerce Clause was an appropriate addition to the CFAA due to "the interstate nature of computer networks, and the ease with which computer abuse, such as destructive computer viruses or worms, can spread across State lines"); *see also* United States v. Trotter, 478 F.3d 918, 921 (8th Cir. 2007) (explaining that computers' connection to the internet rendered them part of a system inexorably intertwined with interstate commerce and thus properly within the realm of

computer or device capable of connecting to the internet is a "protected computer" within the CFAA's scope.[79] Overall, the numerous amendments and legislative history of the relatively young CFAA indicate a conscious broadening of the CFAA in both scope and breadth.[80] However, these purposeful expansions are accurately attributed to Congress's desire to effectively prosecute serious interstate computer crimes in the face of evolving technology rather than an intent to displace existing state laws or preempt all computer crimes.[81]

F. Current Actions Triggering liability Under the CFAA

With all internet-accessible computers protected under the CFAA, the current version of the statute provides criminal and civil liability when an individual: (1) intentionally accesses a computer "without authorization" or "exceeds authorized access," and (2) engages in one of seven types of prohibited conduct.[82] The private, civil right of action is currently limited to felony violations under the criminal law.[83] A party bringing a private, civil action must establish two essential elements: (1) a violation of one of the seven proscribed activities resulting in damage or loss, and (2) a violation

Congress's Commerce Clause power) (citing *United States v. MacEwan*, 445 F.3d 237, 245 (3rd Cir. 2006)); *see* Buckman, *supra* note 51 (explaining, "since the advent of the Internet, almost all computer use has become interstate in nature.").

[79] 18 U.S.C. § 1030(e)(2); *see also* Cont'l Group, Inc. v. KW Prop. Mgmt., LLC, 622 F. Supp. 2d 1357, 1370 (S.D. Fla. 2009) ("[a] connection to the internet is 'affecting interstate commerce or communication.'").

[80] Matthew Kapitanyan, *Beyond Wargames: How the Computer Fraud and Abuse Act Should Be Interpreted In the Employment Context*, 7 I/S: J. L. & POL'Y FOR INFO. SOC'Y 405, 415–16 (2012).

[81] S. REP. NO. 104-357, at 5 (1996). "As computers continue to proliferate in businesses and homes, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the Computer Fraud and Abuse statute is up-to-date and provides law enforcement with the necessary legal framework to fight computer crime. [1996 amendments] will likely not represent the last amendment to this statute, but is necessary and constructive legislation to deal with the current increase in computer crime"; *see also* 139 Cong. Rec. S16421-03, 1993 WL 490040 ("It is important to update our laws to stay abreast of rapid changes in computer technology and computer abuse crimes") (statement of Senator Leahy, the sponsor of the bill). *See also* S. REP. NO. 101-544, at 11 (1990) (reporting that introducing the civil provision was not expected to incur any significant cost to the federal government).

[82] 18 U.S.C. § 1030(a)(1)-(7) (2008); *see* Andrew T. Hernacki, *A Vague Law in A Smartphone World: Limiting the Scope of Unauthorized Access Under the Computer Fraud and Abuse Act*, 61 AM. U. L. Rev. 1543, 1551 (2012) (summarizing each of the current subsections of the CFAA). The seven actions include: (1) obtaining national security information, (2) compromising the confidentiality of a computer; (3) trespassing in a Government computer; (4) accessing a computer to defraud and obtain value; (5) transmission or access that causes damage; (6) trafficking in passwords; and (7) extortion involving threats to damage computer). *Id.*

[83] *See* Winn, *supra* note 30, at 1405.

must involve one of five aggravating factors enumerated in the statute.[84] Employers typically bring a civil action under the aggravating factor of losses exceeding $5,000.[85] The least demanding CFAA provision allows liability for anyone who intentionally accesses and obtains information from any protected computer without authorization or by exceeding authorized accessed.[86]

Traditionally employer-employee and company-consumer relationships have been governed by tort and contract law, but employers are finding the CFAA's invitation to federal court an attractive lure.[87] The CFAA's civil provision allows employers to charge both the former employee and the former employee's new company and permits injunctive relief.[88] The civil provision opens the door to federal jurisdiction while supplemental jurisdiction permits the inevitable litany of accompanying state law claims to be adjudicated as well.[89]

Employers are often able to find relief under a CFAA claim with a much lower evidentiary standard compared with the same claim in state

[84] 18 U.S.C. § 1030(g). The aggravating factors are: (I) loss to one or more persons during any one-year period aggregating at least $5000 in value; (II) the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of one or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; and (V) damage affecting a computer used by or for an entity of the United States government in furtherance of the administration of justice, national defense, or national security. § 1030(c)(4)(A)(i)(I)-(V). *Id.*

[85] Robert C. Kain, *Federal Computer Fraud and Abuse Act: Employee Hacking Legal in California and Virginia, but Illegal in Miami, Dallas, Chicago, and Boston*, 87 FLA. B.J. 36, 38 (2013) (listing all the civil liabilities, but noting the typical basis for civil action).

[86] 18 U.S.C. § 1030(a)(2)(C). Because a "protected computer" is any computer with internet access, and "obtain" includes merely viewing information, any person who intentionally views information on a computer can potentially incur liability depending on how the court interprets authorization. *See* S. REP. NO. 99-432, at 6 (1986) (clarifying that "obtain" includes viewing information, and does not require any downloading or copying); *see also* United States v. Willis, 476 F.3d 1121, 1125–26 (10th Cir. 2007) (explaining that each of the statute's seven subsection addresses a different type of harm, and rejecting defendant's contention that § 1030(a)(2)(C) required anything more than intention to access a protected computer without authorization or by exceeding authorized use in order to obtain information).

[87] United States v. Nosal, 676 F.3d 854, 860 (9th Cir. 2012) (describing employment dispute as an area traditionally governed by tort and contract law); *see also* Thomas E. Booms, *Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act*, 13 VAND. J. ENT. & TECH. L. 543, 551 (2011). Examples of commonly ancillary state law claims include tortious interference with business relations, theft of trade secrets, breach of employment contracts, or breach of fiduciary duty.

[88] 18 U.S.C. § 1030(a), (g).

[89] *Id.*; *see* Brenton, *supra* note 76, at 451. The supplemental jurisdiction statute states that once a plaintiff gains access to federal court through federal question jurisdiction, as they would if stating a claim under the federal CFAA statute, they are able to ask the federal court to exercise supplemental jurisdiction over state law claims that form "part of the same case or controversy" as the plaintiff's federal claim. In a CFAA claim the same allegedly wrongful act will frequently give rise to all claims allowing the plaintiff's state law claims to satisfy the initial supplemental jurisdiction requirements. *Id.*

court.[90] Trade secret litigation provides an excellent example of how policy-driven balancing tests meted out in state courts are easily avoided through a CFAA claim.[91] Prevailing under a state court trade secret claim typically requires the employer to prove that (1) the inappropriately accessed information was a legally protected trade secret, (2) the employer took steps to protect the information's secrecy, and (3) the departing employee misappropriated the information.[92] In contrast, a CFAA claim automatically protects any information accessed through a computer, making it much easier for employers to successfully recover.[93] Recovering under broad interpretations of the CFAA is possible once an employer proves that an employee accessed a computer without authorization and demonstrates the necessary damages.[94]

III. RELEVANT DOCTRINES AND CANONS OF STATUTORY CONSTRUCTION

Doctrines and canons of statutory construction exist to ensure the constitutionality of statutes and to help courts effectuate legislative intent.[95] Constitutional guarantees to due process of law drive the void for vagueness and overbreadth doctrines by demanding that laws provide fair notice and do

[90] *See* Booms, *supra* note 87, at 550–51 (comparing the elements necessary to prove a trade secret claim under state law; CFAA claims do not require proof that the misappropriated data was a trade secret, just that the information came from a protected computer); *see also* Economic Espionage Act of 1996 18 U.S.C. § § 1831-39 (2006) PL 112-269, January 14, 2013, 126 Stat. 2442. The Economic Espionage Act (EEA) was enacted in 1996 and is the federal statute that addresses trade secret theft. The EEA largely tracks the Uniform Trade Secrets Act (most state statutes modeled after this as well). There is no private right of action under the EEA. *See* Cooper Square Realty Inc. v. Jensen, 04-CIV.01011 (CSH), 2005 WL 53284 at *1 (S.D.N.Y. Jan. 10, 2005) ("[C]ongressional intent . . . expressly and unambiguously demonstrates that Congress did not establish a private cause of action in the EEA").

[91] *See* Winters, *supra* note 77 (describing the strategic benefits of bringing a trade secret claim under the CFAA in order to sidestep obstacles and limitations imposed under the Illinois Trade Secret Act).

[92] 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, 158–59 (2008). Forty-seven states have adopted the Uniform Trade Secrets Act (UTSA) or some variation thereof, as the basis for its trade secret misappropriation cause of action. *Id*.

[93] Greg Pollaro, *Disloyal Computer Use and the Computer Fraud and Abuse Act: Narrowing the Scope*, DUKE L. & TECH. REV.12, 22 (2010).

[94] *See* Brenton, *supra* note 76, at 448–49. To be protected under a trade secret statute, information must be kept secret. Trade secret statutes' heightened evidentiary standards reflect careful balancing between safeguarding business information and guaranteeing employee mobility. In contrast, any information accessible through a computer may be protected under the CFAA. *Id*.

[95] Yule Kim, Cong. Research Serv., 97-589, *Statutory Interpretation: General Principles and Recent Trends*, at 3 (2008).

not significantly curtail protected activities.[96] The doctrine of constitutional doubt requires courts to avoid constructions that pose difficult constitutional questions and to construe statutes constitutionally whenever possible.[97] If a statute is susceptible to two different meanings—one constitutional and one unconstitutional— courts must choose the constitutional definition to save the statute.[98]

In addition to doctrines, courts frequently rely on canons of statutory construction to draw inferences about the meaning of statutory language.[99] The overriding objective of statutory construction is to effectuate Congressional purpose.[100] Even if the interpretive question involves only a provision of a larger statute, a court's duty is to construe the entire statute sensibly.[101] Briefly describing applicable doctrines and canons of statutory construction are necessary to appreciate why the CFAA must be narrowly interpreted.[102]

A. The Void for Vagueness Doctrine

The void for vagueness doctrine, rooted in the Due Process Clause, insists that criminal statutes: (1) provide notice to the public of what behavior is prohibited, and (2) include meaningful standards to prevent arbitrary or discriminatory enforcement.[103] The first prong of the void for

[96] *See* United States. v. Williams, 553 U.S. 285, 292–306 (2008) (describing the vagueness and overbreadth doctrines).

[97] Almendarez-Torrez v. United States, 523 U.S. 224, 237–38 (1998) (explaining that this canon is followed out of respect for Congress, which the court assumes "legislates in the light of constitutional limitations"); *see* INS v. St. Cyr, 533 U.S. 289, 299–300 (2001) ("[i]f an otherwise acceptable construction of a statute would raise serious constitutional problems, and where an alternate interpretation of the statute is 'fairly possible'…we are obligated to construe the statute to avoid such problems.").

[98] *Almendarez-Torrez,* 523 U.S. at 238; *see also* Boos v. Barry, 485 U.S. 312, 331 (1988) ("[t]he federal courts have the duty to avoid constitutional difficulties by doing so if such a [narrowing] construction is fairly possible"); *see also* Gonzales v. Carhart, 550 U.S. 124, 149 (2007) (explaining the canon of constitutional avoidance as, "[an] elementary rule . . . every reasonable construction must be resorted to, in order to save a statute from unconstitutionality.").

[99] Kim, *supra* note 95, at 3.

[100] *See* United States v. McAllister, 225 F.3d 982, 986 (8th Cir. 2000) (explaining that courts interpret statutes to give effect to the intent of Congress); *see* Kim, *supra* note 95, at 3.

[101] Gustafson v. Alloyd Co., 513 U.S. 561, 568 (1995) (explaining the court's duty to construe statutes, not isolated provisions).

[102] Chicksaw Nation v. United States, 534 U.S. 84, 94 (2001). Canons of statutory construction are not mandatory rules. They are guidelines designed to help courts determine Congressional intent. If other circumstances or evidence can strongly prove congressional intent, canons may be overcome. Additionally, some canons champion maxims that are incompatible with other canons, forcing a court to pick one over another. Nonetheless, when the language and legislative history is ambiguous, canons can provide guidance.

[103] Kolander v. Lawson, 461 U.S. 352, 357 (1983); *see also Williams*, 553 U.S. at 306 ("[w]hat renders a statute vague is . . . the indeterminacy of precisely what that fact is.

vagueness doctrine, the fair notice requirement, ensures that ordinary citizens can act in conformity with the law.[104] A statute can violate due process rights if citizens have to guess, or vary in their understanding of, a statute's meaning.[105]

The second prong of the void for vagueness doctrine focuses on how much discretion the statute gives to the government officials enforcing it.[106] A statute must direct law enforcement officials and triers of fact in a predictable and equitable application of its provisions.[107] A statute is unconstitutionally vague if its lack of guidelines could result in arbitrary or discriminatory enforcement.[108] For example, including a *mens rea* requirement in a statute can alleviate vagueness concerns by narrowing the scope of a statute and limiting prosecutorial discretion.[109]

A statute with language that is impermissibly vague can be saved through a narrow judicial interpretation.[110] Once a court interprets the meaning of a statute, the judicial interpretation becomes part of the statute's meaning.[111] The canon of constitutional avoidance directs a court to save a

Thus, we have struck down statutes that tied criminal culpability to whether the defendant's conduct was 'annoying' or 'indecent'—wholly subjective judgments without statutory definitions, narrowing context, or settled legal meanings.").

[104] City of Chicago v. Morales, 527 U.S. 58, n.14 (1999) (holding that an ordinance's definition of loiter, "to remain in any one place with no apparent purpose," was unconstitutionally vague because it drew no distinction between innocent conduct and conduct calculated to cause harm); *see* F.C.C. v. Fox Television Stations, Inc. 132 S.Ct. 2307, 2317 (2012).

[105] *See Fox Television Studios*, 132 S.Ct. at 2317 ("[a] fundamental principle in our legal system is that laws which regulate persons or entities must give fair notice of conduct that is forbidden or required.").

[106] *Kolander*, 461 U.S. at 357.

[107] Grayned v. City of Rockford, 408 U.S. 104, 108–09 (1972) (holding that if enforcement of a criminal statute can be done on an entirely subjective basis the statute is impermissibly vague).

[108] *Kolander*, 461 U.S. at 358; *see* Smith v. Goguen, 415 U.S. 566, 572–73 (1974) (describing the level of guidance necessary for a statute to be constitutional: it is within the province of the legislature, and not law enforcement, to make law, and they must fashion statute with enough guidance so that it is not left to the "personal predilections" of police or prosecutors).

[109] *Gonzales*, 550 U.S. at 149–50 (concluding that the word "deliberate" in an abortion statute helped alleviate vagueness concerns because by ensuring that doctors performing abortions would not face criminal liability if they delivered a fetus beyond the prohibited point in good faith).

[110] *Morales*, 527 at 61, n.31 (distinguishing the instant case from Boos v. Barry, 485 U.S. 312, 329–30 (1988), "[t]here, we noted that the text of the relevant statute, read literally, may have been void for vagueness. . . [w]e then found, however, that the Court of Appeals had 'provided a narrowing construction that alleviates. . . these difficulties'"); *but see id.* at 68–69 (if a federal court is interpreting a state statute, the federal court has no authority to construe the language of a state statute more narrowly than the construction given by that state's highest court).

[111] Wainwright v. Stone, 414 U.S. 21, 23 (1973) ("[w]hen a state statute has been construed to forbid identifiable conduct so that 'interpretation by (the state court) puts these

statute from unconstitutionality through a narrow interpretation when faced with the option of invalidating a statute due to vagueness or curing the vagueness through narrow interpretation.[112]

B. The Overbreadth Doctrine

Closely related to the void for vagueness doctrine is the doctrine of overbreadth.[113] The overbreadth doctrine prohibits a criminal law from sweeping so broadly that it also encompasses constitutionally protected activity.[114] A statute is overbroad if its language is so broad that sanctions apply to conduct that the government is not entitled to regulate.[115] If impermissible applications are substantial when compared to the statute's legitimate scope, the overbreadth doctrine can invalidate entire statutes.[116] Even statutes designed primarily to prohibit or target only criminal conduct cannot survive an overbreadth challenge if a protected right is substantially infringed.[117]

C. The Rule of Lenity

The rule of lenity is a canon of statutory construction for criminal statutes, but can also apply in civil contexts if the statute at issue has criminal and noncriminal applications.[118] This "junior version of the vagueness doctrine" assures that citizens have fair notice by resolving any ambiguity in a statute to only apply to clearly covered conduct.[119] The rule of lenity

words in the statute as definitely as if it had been so amended by the legislature,' claims of impermissible vagueness must be judged in that light.").

[112] *Boos*, 485 U.S. at 330–31(finding it "well settled" that federal courts have the power to adopt narrowing constructions of federal legislation); *see also* Kerr, *supra* note 3**,** at 1573.

[113] *See* Thornhill v. Alabama, 310 U.S. 88 (1940) (striking down an overly-broad Alabama statute against loitering or pickets outside a business).

[114] *Id. See also* Galbraith, *supra* note 73, at 323 (noting that the contract-based theory has "allowed website owners to utilize the CFAA to override the carefully balanced provisions of the copyright laws and improperly restrict speech in violation of the First Amendment.").

[115] Schwartzmiller v. Gardner, 752 F.2d 1341, 1346 (9th Cir. 1984) (holding that a law is overbroad if it prohibits not only acts the legislature may forbid, but also constitutionally protected conduct).

[116] Broadrick v. Oklahoma, 413 U.S. 601, 615–16 (1973).

[117] M. Katherine Boychuck, *Are Stalking Laws Unconstitutionally Vague or Overbroad?*, 88 NW. U.L. REV. 769, 773 (1994).

[118] *Id.* Statutes with criminal and noncriminal applications still need to be interpreted consistently; hence, the rule of lenity may be invoked even in a civil context. Because the CFAA has both criminal and civil provisions, the rule of lenity may apply. *See* Leocal v. Ashcroft, 543 U.S. 1, 11 n.8 (2004) (interpreting a term narrowly despite arising in a civil deportation case because, "we must interpret the statute consistently, whether we encounter its application in a criminal or a noncriminal context, the rule of lenity applies.").

[119] *Drew*, 259 F.R.D. at 463; *see Miller*, 687 F.3d at 204 (rejecting plaintiff's argument in a civil CFAA claim for a broad interpretation by holding "in the interest of providing fair warning of 'what the law intends to do if a certain line is passed,' we will

embodies two important policies.[120] First, citizens should be given fair warning in easily understood language of behavior that can result in criminal sanctions.[121] Due process prevents courts from construing laws in novel or surprising ways by criminalizing conduct not clearly defined in a statute.[122] Second, laws with criminal penalties are a reflection of society's condemnation and should be defined by legislatures, not courts.[123] Ambiguities in criminal statutes should be resolved in favor of the defendant to both afford notice and to ensure that the boundaries of criminal statutes are sketched by legislatures and not courts.[124] Before the rule of lenity applies, a court must conclude that there is serious ambiguity or uncertainty in the statute that normal methods of statutory construction cannot resolve.[125] Courts narrowly interpreting the CFAA frequently cite to the rule of lenity as a guiding principle.[126]

The instruction that ambiguity of criminal statutes should be resolved in favor of lenity interlocks with the presumption that Congress acts interstitially.[127] The balance between state and federal criminal jurisdiction

construe this criminal statute strictly and avoid interpretations not clearly warranted by the text"); *see also* Ratzlaf v. United States, 510 U.S. 135, 148 (1994) (finding that lenity principles demand resolution of ambiguities in criminal statutes in favor of the defendant); *see also* United States v. Lanier, 520 U.S. 259, 266 (1997) (determining that the touchstone for notice is whether the statute, either standing alone or as construed, made it reasonably clear at the relevant time that the defendant's conduct was criminal).

[120] United States v. Bass, 404 U.S. 336, 347–48 (1971).

[121] *Id*.

[122] *Drew*, 259 F.R.D. at 463; *see also Brekka*, 581 F.3d at 1134 (applying the rule of lenity to the CFAA because, "[t]he Supreme Court has long warned against interpreting criminal statutes in surprising and novel ways that impose unexpected burdens on defendants.").

[123] *Bass*, 404 U.S. at 347–48.

[124] *Id.* at 348.

[125] Reno v. Koray, 515 U.S. 50, 64–65 (1995). If courts are unable to deduce the meaning of a statute after examining the statutory text and available legislative sources, then the rule of lenity requires construing the statute in favor of the criminal defendant. *See also Clarity*, 698 F. Supp. 2d at 1316 (explaining that because the CFAA is criminal in nature and ambiguous, invoking the rule of lenity is appropriate and the rule favors the less harsh version on the defendant); *see also* Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966 (D. Ariz. 2008) (discussing the principles of statutory construction, specifically the rule of lenity in guiding the court's interpretation of the CFAA because it has both criminal and noncriminal applications).

[126] Lockheed Martin Corp. v. Speed, 2006 WL 2683058 at *7 (M.D. Fla. Aug. 1, 2006) (finding that the terms "without authorization" and "exceeds authorized access" were ambiguous and required applying the rule of lenity to produce a restrained, narrow interpretation); *see also* ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 612 (M.D. Tenn. 2010) (finding the CFAA unambiguous, but stating that even if the court found the CFAA ambiguous, the rule of lenity would require any ambiguity to be resolved in favor of the defendant); *see also* Dana Ltd. v. Am. Axle & Mfg. Holdings, Inc., 2012 WL 2524008 at *4 (W.D. Mich. June 29, 2012) (holding that because the CFAA is primarily a criminal statute, the rule of lenity requires any ambiguity to be resolved in favor of the defendant).

[127] Jones v. United States, 529 U.S. 848 (2000) (explaining that before a court chooses a harsher alternative, it should remember that unless Congress conveys its purpose

requires Congress to convey its purpose clearly if it intends for a statute to effect a significant change in the balance.[128] Absent a clear Congressional purpose, courts should not interpret statutes in ways that would significantly change the federal-state balance in the prosecution of crimes.[129]

D. The Plain Language Rule

The starting point in statutory construction is always the language of the statute itself. [130] The plain meaning rule states that if the language of a statute is clear, there is no need to look outside the statute to its legislative history to ascertain the meaning.[131] When a statute's language is unambiguous, the plain meaning rule will both start and end the judicial inquiry.[132] This canon crystallizes interpretational priorities: statutory language is primary, legislative history is secondary.[133] The one generally recognized exception to the plain language rule is that the plain meaning will be rejected if it would produce an absurd result.[134]

When the meaning of specific statutory language is at issue, courts will first look to see if the statute provides a definition.[135] A statutorily provided definition will govern if applicable in the context used.[136] If the

clearly, the interpretation should not significantly change the federal-state balance in the prosecution of crimes).

[128] *Bass*, 404 U.S. at 349; *see also* Brett Senior & Assocs. v. Fitzgerald, 2007 WL 2043377 at *4 (E.D. Pa. 2007) (finding it unlikely that Congress, given its concern "about the appropriate scope of Federal jurisdiction" in the area of computer crime, intended essentially to criminalize state-law beaches of contract) (quoting S. REP. NO. 99-432, at 3 (1986)).

[129] *Bass*, 404 U.S. at 349; *see also Shamrock*, 535 F. Supp. 2d at 966 ("such rule requires a court confronted with two rational readings of a criminal statute, one harsher than the other, to choose the harsher only when Congress has spoken in clear and definite language.").

[130] *McAllister*, 225 F.3d at 986 (explaining that the starting point in interpreting a statute is always the language of the statute itself); *see, e.g.,* Robinson v. Shell Oil Co., 519 U.S. 337, 340–41 (1997) (determining whether the language at issue has a plain and unambiguous meaning by looking "to the language itself, the specific context in which that language is used, and the broader context of the statute as a whole.").

[131] United States v. Gonzales, 520 U.S. 1, 6 (1997) (finding that the straightforward language of the statute left no reason to resort to legislative history).

[132] *Ratzlaf*, 510 U.S. at 147–48 ("[w]e do not resort of legislative history to cloud a statutory text that is clear.").

[133] Kim, *supra* note 95, at 41.

[134] *See, e.g.,* United States v. Granderson, 511 U.S. 39, 47 n.5 (1994) (dismissing an interpretation said to lead to an absurd result); *see also* Public Citizen v. Department of Justice, 491 U.S. 440, 454 (1989) ("[w]here the literal reading of a statutory term would compel an 'odd result'. . . we must search for other evidence of congressional intent to lend the term its proper scope.").

[135] Kim, *supra* note 95, at 5; *see* Colautti v. Franklin, 439 U.S. 379, 392 (1979).

[136] Kim, *supra* note 95, at 5; *see also* Orbit One Commc'ns, Inc. v. Numerex Corp., 692 F. Supp. 2d 373, 386 (S.D.N.Y. 2010) (rejecting a broad interpretation of the CFAA because it would be imprudent to interpret the CFAA in a manner inconsistent with its plain meaning and to transform the common law civil tort of misappropriation of confidential information into a criminal offense).

statute does not define the word but has an accepted meaning in the area of law addressed by the statute, the court will import the meaning from the whole term and not break down the component parts.[137] Words that are not defined and are not terms of art are customarily given their ordinary meanings, which are often derived from the dictionary.[138]

E. No "Mere Surplusage"

Congress acts purposefully in enacting and amending statutes.[139] Courts should presume that Congress intended each of a statute's terms to have meaning, and courts should give effect, if possible, to every clause and word of a statute.[140] Courts should avoid any interpretation that insinuates that the legislature was ignorant of the meaning of the language it employed.[141] When Congress amends a statute by altering words, it does so with the intent of changing the statute's meaning.[142] Prudentially, the converse of this rule creates a corollary canon: courts should not add language that Congress has not included.[143] On a slightly broader scale, this construction principle also applies to statutes as they stand in relation to each other. Congress will not enact duplicative statutes, so where other federal statutes would apply, the statute at issue should not.[144]

[137] Sullivan v. Stroop, 496 U.S. 478, 483 (1990) ("where a phrase in a statute appears to have become a term of art . . . any attempt to break down the term into its constituent words is not apt to illuminate its meaning.").

[138] F.D.I.C. v. Meyer, 510 U.S. 471, 476 (1994) (explaining that in the absence of a statutory definition, "we construe a statutory term in accordance with its ordinary or natural meaning"); *see also Drew*, 259 F.R.D. at 459 (finding that "[m]ost courts that have actually considered the issue of the meaning of the word 'access' in the CFAA have basically turned to the dictionary meaning.").

[139] Bailey v. United States, 516 U.S. 137, 145 (1995) (quoting Ratzlaf v. United States, 510 U.S. 135, 140–41 (1994) ("[j]udges should hestitate….to treat [as surplusage] statutory terms in any setting, and resistance should be heightened when the words describe an element of a criminal offense.").

[140] *Id.* at 146 (rejecting interpretation that would have made "uses" and "carries" redundant in statute penalizing using or carrying a firearm in commission of an offense because, "[w]e assume that Congress used two terms because it intended each term to have a particular, nonsuperfluous meaning.").

[141] Montclair v. Ramsdell, 107 U.S. 147, 152 (1883) (finding that a court has the duty, if possible, to avoid any construction of a statute "which implies that the legislature was ignorant of the meaning of the language it employed.").

[142] Stone v. INS, 514 U.S. 386, 397 (1995) (stating that when Congress acts to amend a statute, "we presume it intends its amendment to have real and substantial effect.").

[143] *Kim, supra* note 95, at 13.

[144] *Id.* at 13–14.

F. The Canon of Consistency

Avoiding due process concerns requires courts to interpret statutes with criminal and non-criminal applications consistently.[145] Additionally, a term or phrase appearing in several places in a statute should be interpreted with the same meaning each time it appears.[146] This construction principle should be employed when interpreting the CFAA as the statute not only has both criminal and civil applications, but repeats the same terms ("without authorization" and "exceeds authorized access") in several subsections.[147] This canon of construction means that once a court interprets a term or provision of the CFAA, that definition will govern all future CFAA cases in the jurisdiction.[148] Courts defining "authorization" in the context of a business dispute concerning monetary damages should be mindful that the decided definition will govern with equal force to a dispute involving criminal punishment.[149]

IV. THE CURRENT SPLIT

A court's interpretation of the CFAA dramatically affects whether an employee is liable for misusing information gained from company

[145] *See, e.g.,* United States v. Bigham, 812 F.2d 943, 948 (5th Cir. 1987) (noting that when Congress allows the same standard to govern criminal and civil cases, it is "of no significance . . . [w]hether a case is brought on the civil or criminal side of the docket.").

[146] *Ratzlaf*, 510 U.S. at 143; *see also* Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007) (stating that "identical words and phrases within the same statute should normally be given the same meaning.").

[147] *Ratzlaf*, 510 U.S. at 143; *Nosal*, 676 F.3d at 859. Rejecting the government's suggestion that the court adopt the government's proposed definition of "exceeds authorized access" for the subsection at issue, and still use narrower interpretations for the other times it is used in the statute because that result would be inconsistent. Noting that because the phrase "exceeds authorized access" appears five times in the first seven subsections of the CFAA, the court must consider how its adopted interpretation will operate wherever the phrase appears. *Id*.

[148] *Bigham*, 812 F.2d at 948; *see* Hernacki, *supra* note 82, at 1548. The *mens rea* requirements vary within the provisions of the CFAA, but the *actus reas* usually involves either or both of the terms "without authorization" or "exceeds authorized access." For example, the fraud provision of the CFAA requires both intent to defraud and violative access that furthers the intended fraud; in contrast, another provision requires no *mens rea* and only violative access is required. In a case of first impression, if the court is dealing with the fraud provision in a civil case where the defendant has committed obvious wrongdoing, a broad interpretation of the term "unauthorized access" may make sense. However, this definition will carry over to all other CFAA cases. The definition which fit naturally in the context it was made may not be similarly appropriate if the next case consists of criminal liability and no wrongdoing.

[149] *See* Kerr, *supra* note 26, at 1641–42 (noting that courts are more likely to hold a defendant liable under an ambiguous statute when the stakes involve a business dispute between competitors than when government seeks to impose jail time on an individual. The problem becomes, these same definitions are then used in criminal settings where it is jail time, and not money damages, at stake.).

computers.[150] There are three primary ways that federal courts interpret the term "authorization."[151] Two of these interpretations are broad, focusing on the intent of the employee to determine whether the employee's actions furthered or frustrated the interests of the employer.[152] Courts following a broad, agency-based interpretation use principles of agency law and hold that authorization terminates whenever an employee acts against his employer's interests.[153] Courts endorsing the other broad view analyze authorization by examining underlying contractual obligations and company policies.[154] In contrast, the third approach takes a considerably more restrained view.[155] Instead of examining the employee's subjective intent, this narrow interpretation of the CFAA focuses objectively on whether the employer granted authorization to the employee.[156]

A. The Broad View of Agency Theory

The Seventh Circuit applies a broad view of agency theory that, grounded in principles of agency law, is the most employer-friendly interpretation of the CFAA.[157] This approach examines the status of an agency relationship between an employer and employee to determine whether access to a computer was authorized.[158] Under an employer-employee agency relationship, an employee owes a special duty of loyalty to his employer which requires him to act solely for the benefit of the employer.[159] An employee has "authorization" under the CFAA as long as his work furthers the interests of his employer.[160] Once an employee acts

[150] Audra A. Dial & John M. Moye, *Fourth Circuit Widens Split Over CFAA and Employees Violating Computer Use Restrictions*, 17 No. 11 CYBERSPACE LAW 1 (2012).

[151] *See generally* Kerr, *supra* note 26. Reacting to the courts inconsistent treatment of the CFAA, Professor Orin Kerr has proposed an alternate approach: the code-based approach. Under this view, access to a protected computer is unauthorized when a user circumvents a firewall or username/login screen to access the system. *Id*. While this approach has been extensively analyzed by commentators, it has not been expressly adopted by courts. Because this Comment analyzes how the CFAA has been treated in courts, the code-based approach falls outside the scope of this Comment. *See Drew*, 259 F.R.D. at 460 (determining that "[i]t is simply noted that, while defining "access" in terms of a code-based restriction might arguably be a preferable approach, no case has adopted it, and the CFAA legislative history does not support it.").

[152] Kapitanyan, *supra* note 80, at 433–34. To determine whether the employee's conduct was authorized or not, the broad view focuses on the employee's intent, whereas the narrow view focuses on the actions of the employer. *Id.*

[153] *Citrin*, 440 F.3d at 421.

[154] *Explorica*, 274 F.3d at 577. *See generally Brekka*, 581 F.3d at 1127.

[155] *Brekka*, 581 F.3d at 1127.

[156] *Id.*

[157] Field, *supra* note 48.

[158] *Citrin*, 440 F.3d at 418.

[159] Field, *supra* note 48, at 823.

[160] *See* Restatement (Second) of Agency, § 39 (1958) (stating that the agent is to act only for the principal's benefit).

adversely to his employer's interest, both the agency relationship and authorization under the CFAA immediately terminate.[161]

An agency interpretation of the CFAA requires no affirmative employer action for authorization to terminate.[162] Authorization is implicitly revoked whenever an employee accesses a computer for purposes that do not further his employer's interest.[163] Focusing entirely on the employee's state of mind, all it takes to terminate authorization and incur liability under this view of the CFAA is an employee action not wholly in the employer's best interests. [164] An employee acts "without authorization" under the CFAA when he breaches a state law duty of loyalty or fiduciary duty to the employer.[165]

The Seventh Circuit's decision in *Int'l Airport Centers, LLC v. Citrin* is generally heralded as the leading case for an agency-based interpretation of the CFAA, though the case was largely based on a district case decided a few years earlier.[166] *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.* was the first case to apply an agency theory of authorization to a CFAA claim addressing the exploits of a rogue employee.[167] Both companies in the self-storage business, Shurgard was an established industry leader while Safeguard had recently entered the market as a direct competitor.[168] Safeguard approached one of Shurgard's regional managers, Eric Leland, and offered him a position with their company.[169] While employed with Shurgard and in breach of his employment agreement, Leland used his employee access to email confidential and proprietary information to Safeguard representatives.[170] Leland continued to supply Safeguard with this type of information even after leaving Shurgard.[171]

[161] Field, *supra* note 48, at 823 (asserting that once an employee terminates the agency relationship by acting adversely to his employer's interests, he is also acting "without authorization" since authorization is a privilege tied inextricably to the agency relationship).

[162] Restatement (Second) of Agency § 112 (1958) ("[u]nless otherwise agreed, 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"); *see also* Kaplan, *supra* note 14.

[163] Restatement (Second) of Agency § 112 (1958).

[164] *Citrin,* 440 F.3d at 420–21; *see also* Shawn E. Tuma, "What Does CFAA Mean and Why Should I Care?" A Primer on the Computer Fraud and Abuse Act for Civil Litigators, 63 S. C. L. REV. 141, 176 (2011) (explaining how the agency theory relates to other interpretations of "without authorization"); *see* Urban, *supra* note 47, at 1399.

[165] Field, *supra* note 48, at 823–24 (discussing the evolution of the agency-based theory as a direct application of agency law to interpret authorization under the CFAA).

[166] Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc. 119 F. Supp. 2d 1121 (W.D. Wash. 2000) (this case has since been overruled by *LVRC Holdings v. Brekka*, 581 F.3d 1127 (9th Cir. 2009)).

[167] Kapitanyan, *supra* note 80, at 417.

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

[169] *Id.*

[170] *Id.*

[171] *Id.* at 1122.

Shurgard subsequently sued Safeguard for a litany of state tort claims as well as violations of the CFAA.[172]

Applying the standard set forth in the Restatement (Second) of Agency, the court concluded that because Leland's authorization terminated when his interests became adverse to Shurgard, he was without authorization when he obtained and sent the confidential information to Safeguard.[173] Once the court determined that Leland was "without authorization," it found no need to decide whether Leland had also "exceeded authorized use" under the CFAA since liability was established with proof of either term under the subsection alleged.[174] Reaching its conclusion based solely on the plain language of the statute, the court went on to cite additional support from the CFAA's legislative history.[175] Noting the narrowness of the original CFAA's scope, the court concluded that subsequent amendments evinced clear congressional intent to widen coverage to cover the type of misuse alleged by Shurgard.[176]

Citing *Shurgard* as authority, the Seventh Circuit officially adopted the agency theory in 2006.[177] In *Citrin* the employee breached his employment contract with International Airport Centers (IAC) by quitting his job to start a competing company.[178] Before returning IAC's company laptop, Citrin deleted all of the data by installing a secure-erasure program to guarantee the data would not be recoverable.[179] IAC sued Citrin, alleging he violated the CFAA by knowingly and intentionally causing damage to a protected computer without authorization.[180]

Analyzing Citrin's actions under principles of agency law, the court found that he unilaterally terminated his agency relationship with IAC the moment he resolved to quit and delete the files.[181] Citrin's authorization to access the laptop was inextricably tied to his agency status; without agency

[172] *Id.* In addition to the CFAA claims, Shurgard brought state law claims alleging misappropriation of trade secrets, conversion, unfair competition, and tortious interference with a business expectancy. *Id.*

[173] *Shurgard*, 119 F. Supp. 2d at 1125 (holding that, based on the Restatement (Second) of Agency, § 112 (1958), authority of employee ended when employee became an agent for a competing company. Once an employee's authority ends, he or she loses any prior authorization.).

[174] *Id.* at 1125 n.4.

[175] *Id.* at 1127 (analyzing the CFAA's legislative history to ensure that the court's finding would not produce an absurd result).

[176] *Id.* The court rejected Safeguard's argument that the CFAA was limited to large-scale, industry and government computers whose information could severely harm the public if the information was damaged. *Id.* The court found the Senate report's emphasis on the purpose of the CFAA to prevent individuals from abusing their right to use a computer demonstrated that a broad meaning was appropriate.

[177] *Citrin*, 440 F.3d at 421 (establishing that an employee acts without authorization for purposes of the CFAA when his intentions become adverse to his employer).

[178] *Id.*

[179] *Id.*

[180] *Id.*; *see also* 18 U.S.C. § 1030(a)(5)(A).

[181] *Citrin*, 440 F.3d at 419.

status he had no authority to access the computer.[182] The court held Citrin liable even though he was still an employee when he accessed the laptop and was not violating any company policies prohibiting him from deleting emails.[183] Acknowledging that under an agency view of the CFAA the difference between the terms "without authorization" and "exceeds authorized access" is "paper thin…but not quite invisible," the court quickly concluded that the principles of agency law rendered Citrin's actions "without authorization."[184]

B. The Broad View of Contract Theory

The other broad interpretation of the CFAA finds its roots in contract law, focusing on the contractual relationship between the parties.[185] The First, Fifth, and Eleventh Circuits use underlying contractual agreements and employee policies as the basis for analyzing authorization.[186] Liability under the CFAA may attach if a court finds that an employee accessed a protected computer in a way that was prohibited or in excess of limitations set by a contract or a clearly communicated employer policy.[187]

The First Circuit articulated this contract approach in *EF Cultural Travel BV v. Explorica, Inc.* by finding that an employment agreement could establish the parameters of authorized access under the CFAA.[188] EF Cultural Travel BV (EF), a well-established company, sued a newly-formed competitor company Explorica after discovering that Explorica had created a robot "scraper" to mine EF's website and undercut EF's prices.[189] Explorica's vice president Philip Gormley was a former vice president at EF.[190] Gormley voluntarily signed a confidentiality agreement that prohibited disclosure of any information "which might reasonably be construed to be contrary to the interests of EF" while employed with EF.[191] In his new position with Explorica, Gormley used his intimate knowledge of EF's business practices to direct the design of the computer scraper that was used to gather enough information to undercut EF's prices.[192]

The First Circuit held that Gormley's use of the scraper "exceeded authorized access" under the CFAA because its use breached the

[182] *Id.* at 420–21. Violating the duty of loyalty, or failing to disclose adverse interests, voids the agency relationship.

[183] *Id.*

[184] *Id.* at 420.

[185] Urban, *supra* note 47, at 1378.

[186] *Id.* at 1372.

[187] *Id.*

[188] *Explorica*, 274 F.3d at 578–79.

[189] *Id.* at 580.

[190] *Id.* at 582.

[191] *Id.*

[192] *Id.* at 579–80.

confidentiality agreement that Gormley signed with EF.[193] The court reasoned that Gormley acted contrary to EF's interests in violation of the confidentiality agreement when he used his insider knowledge of EF's business practices to the advantage of a competitor.[194] Once the First Circuit decided that Gormley exceeded his authorized access, it declined to examine whether he was also "without authorization" since the predicate claim required only one of the two terms.[195]

Starting from a contract-based interpretation of the CFAA, the Fifth and Eleventh Circuits extended the principles of contract law to base liability on employer policies that had been communicated to employees.[196] The Fifth Circuit reached this conclusion in *U.S. v. John*, a criminal case involving fraud.[197] Defendant John had authorization to access customer account information as an account manager for Citibank.[198] John attended trainings and was aware of the corporate policy prohibiting misuse of Citigroup's computer information and confidential customer information.[199] Disregarding these policies, John accessed Citigroup's computer system to obtain confidential customer information which she then provided to others who used the information to make fraudulent charges.[200] The court held that John exceeded her authorized access by violating Citibank's clearly communicated and well-established policies that prohibited accessing customer data in furtherance of a criminally fraudulent scheme.[201] Acknowledging the Ninth Circuit's contrary holding in *LVRC Holdings, LLC v. Brekka*, the Fifth Circuit explained the lack of notice issue predominant in *Brekka* was not at issue for John because she had reason to know that accessing data in furtherance of fraud was unauthorized.[202]

[193] *Id.* at 581–82.

[194] *Explorica*, 274 F.3d. at 582–83 (stating that "[a]ppellants would face an uphill battle trying to argue that it was not against EF's interests for appellants to use the tour codes to mine EF's pricing data.").

[195] *Id*. at 581 (concluding that because the defendant "exceeded authorized access," the court did not need to reach the more general arguments made about statutory meaning, including whether use of a scraper alone renders access unauthorized).

[196] United States v. John, 597 F.3d 263, 269 (5th Cir. 2010); *see also* United States v. Rodriguez, 628 F.3d 1258, 1260 (11th Cir. 2010).

[197] *John*, 597 F.3d at 269.

[198] *Id.* at 273.

[199] *Id.*

[200] *Id.*

[201] *Id.* Despite stating, "while we do not necessarily agree that violating a confidentiality agreement under circumstances such as those in *EF Cultural Travel BV* would give rise to criminal culpability . . ." the court found that John knew that her access in furtherance of a criminally fraudulent scheme was outside her permitted access. *Id.*

[202] *Id.* at 273–74. The Ninth Circuit was primarily concerned that unless an employer affirmatively rescinded computer access, an employee would have no reason to know that personal use of a company computer would constitute a criminal violation. The Fifth Circuit concluded notice was not an issue in this case because John had reason to know that accessing company data to further a criminal act could incur criminal liability. *Id.*

The Eleventh Circuit adopted the broad, contract-based interpretation of the CFAA in *United States v. Rodriguez*.[203] Rodriguez was charged with intentionally accessing a computer without authorization or exceeding authorized access, and obtaining information from a department or agency of the United States.[204] While working for the Social Security Administration (Administration), Rodriguez repeatedly accessed multiple non-business related accounts despite a clearly-stated employer policy prohibiting non-business use of company computers.[205] This policy warned employees that they faced criminal penalties if they violated policies on authorized use of databases.[206] Although Rodriguez refused to sign a written acknowledgement of the policy, he attended mandatory office trainings and received office memorandums and daily alerts on company computers that all served to reinforce the policy.[207] Examining the plain language of the CFAA and the Administration's policies, the court ultimately concluded that even though there was no formal written agreement in place, accessing information in violation of a corporate computer-use policy equated to "exceeding authorized access" under the CFAA.[208]

Courts have also applied a contract-based approach to cover network service provider agreements.[209] Under this application of a contract-based theory, once someone uses a computer in a way that violates his contract with the provider, he has "exceeded his authorized use" and is in violation of the CFAA.[210] Applying this approach to terms of service agreements allows website owners and service providers to establish criminal liability through terms of service.[211] These terms of service cases appear to hold that a provider has subjective and nearly total power to decide which types of access constitute unauthorized access with respect to data available to the public through the internet.[212] Allowing criminal liability to hinge on terms of service agreements that are rarely read, difficult to comprehend, and

[203] *Rodriguez*, 628 F.3d at 1260.

[204] *Rodriguez*, 628 F.3d at 1263; *see also* 18 U.S.C. § 1030(a)(2)(B). This less-frequently invoked CFAA provision applied because Rodriguez's employer was the Social Security Administration, which is a government agency.

[205] *Rodriguez*, 628 F.3d at 1263.

[206] *Id.* at 1260.

[207] *Id.*

[208] *Id.*

[209] *See e.g.,* Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 252–53 (S.D.N.Y. 2000) (holding defendant company acted without authorization when it violated posted restrictions, terms of use, on plaintiff's website); *see also* Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 450 (E.D. Va. 1998) (finding that LCGM's use of AOL to send bulk-emails in violation of AOL's terms of service constituted access in excess of authorization).

[210] *See* Hernacki, *supra* note 82, at 1555.

[211] *See* Kerr, *supra* note 3, at 1582.

[212] *See* Winn, *supra* note 30, at 1411–12.

subject to change without notice led one district court to declare the CFAA unconstitutionally vague.[213]

In *United States v. Drew*, the court overturned the defendant's misdemeanor CFAA conviction after a jury acquitted her of the felony CFAA charges.[214] The court denied Drew's original motion to dismiss the felony CFAA charges finding the scienter element in the felony provision saved the statute's constitutionality.[215] However, once the felony charge disappeared, the court concluded that the CFAA's misdemeanor provision failed both prongs of the void for vagueness doctrine, and due process could not be afforded to citizens if every breach of a terms of service provision could be criminally actionable.[216]

C. The Narrow View of the CFAA

Under a narrow view of the CFAA, accessing data without authorization occurs only when initial access is not permitted because misuse of information is not within the statute's scope.[217] Once an employee is granted authorization to access an employer's computer, that employee does not violate the CFAA regardless of how he or she subsequently uses the data.[218] The narrow view determines whether authorization existed by looking solely at the actions of the employer, whereas the broad views examine the employee's motives.[219]

[213] *Drew*, 259 F.R.D. at 449 (overturning misdemeanor conviction under CFAA based on defendant exceeding the scope of authorized access as defined by MySpace's terms of service agreement); *see also* David A. Puckett, *Terms of Service and the Computer Fraud and Abuse Act: A Trap for the Unwary?,* 7 OKLA. J.L. & TECH. 53 (2011) (dividing terms of service agreements into four categories to demonstrate different practical and constitutional problems when applied to CFAA claims: wholly unexpected terms of service, utterly vague terms of service, spectacularly complex terms of service, and terms of service that abut First Amendment freedoms).

[214] *Drew,* 259 F.R.D. at 451.

[215] *Id.* The scienter element present in the 18 U.S.C. § 1030(c)(2)(B)(ii) felony charge is the requirement that the accessing of a computer without authorization is intentional.

[216] *Id.* at 464. Anyone who uses a computer connected to the internet and views information has already met two of the three elements to § 1030(a)(2)(C). The third element requires intentionally accessing the computer's information either without authorization or by exceeding authorized access. Concluding that it would be unconstitutional to hold every person who intentionally violates a terms of service agreement criminally liable, the court held that the defendant's CFAA misdemeanor conviction was unconstitutionally vague. The court found that the CFAA provision violated both prongs of the void for vagueness doctrine due to the lack of minimal guidelines to govern law enforcement and due to deficiencies in notice which meant that people of "common intelligence" would not be on notice that a breach of a terms of service agreement can bring criminal charges. *Id.*

[217] Kapitanyan, *supra* note 80, at 426.

[218] *Federal Judge Highlights Dissention Over Computer Fraud and Abuse Act*, CIRCUIT SPLIT BLOG (May 22, 2012) http://www.circuitsplits.com/2012/05/ federal-judge-highlights-dissension-over-computer-fraud-and-abuse-act.html.

[219] *See Nosal*, 676 F.3d at 860.

In a severe departure from broad views, the Ninth Circuit adopted a narrow interpretation of the CFAA in *Brekka* and used the recent case *U.S v. Nosal* to reaffirm its position.[220] This unflinchingly narrow interpretation has quickly picked up steam, garnering support from several other circuits and numerous district courts.[221]

In *Brekka*, LVRC brought several state tort claims and a CFAA claim against former employee Christopher Brekka.[222] Alleging that Brekka emailed LVRC files to his personal account without authorization, LVRC argued Brekka was either without authorization, or exceeded his authorized access, the moment he decided to use the computer in a way adverse to his employer's interest.[223] Invoking several canons of statutory construction, the Ninth Circuit affirmed summary judgment in favor of Brekka, holding that he did not violate the CFAA.[224]

First, without a statutory definition for "authorization," the court consulted a dictionary to determine the ordinary, common meaning of the word.[225] Defining authorization to mean permission, the court concluded that because LVRC gave Brekka permission to use the company computer, he had authorization to access company files.[226] Next, the court examined the plain language of the statute for any evidence to support LVRC's argument that Congress implied an agency relationship, but found none.[227] Entirely

[220] *Brekka*, 581 F.3d at 1127; *see also Nosal*, 676 F.3d at 863–64.

[221] *See infra* note 246 (summarizing district courts that use a narrow interpretation of the CFAA).

[222] *Brekka*, 581 F.3d at 1129. Plaintiffs alleged that Brekka accessed LVRC's computers during both his employment with LVRC and after he left the company. Finding that LVRC failed to establish a genuine issue of material fact as to whether Brekka accessed the LVRC website without authorization after he left the company, the court focused on Brekka's authorization during the time he was employed with plaintiff.

[223] *Id.* LVRC was limited to the agency theory since Brekka did not have a written employment agreement, nor did LVRC promulgate employee guidelines that would prohibit employees from emailing LVRC documents to personal computers.

[224] *Id.* at 1135.

[225] *Id.* at 1132–33 (applying the fundamental canon of statutory construction to define "without authorization." Unless otherwise defined, words will be interpreted as taking their ordinary, contemporary, common meaning.).

[226] *Id.* at 1133. *See also Lockheed*, 2006 WL 2683058 at *5 (M.D. Fla. 2006). The court explained the difference between the two terms "without authorization" and "exceeds authorized access" under a narrow interpretation of the CFAA:

> [T]hus it 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).

Id.

[227] *Brekka*, 581 F.3d at 1135 (rejecting an agency interpretation because, "[N]othing in the CFAA suggests that a defendant's liability for accessing a computer without

unpersuaded by LVRC's *Citrin* line of reasoning, the court decided that the plain language, canon of consistency, and the rule of lenity all pointed strongly to a narrow interpretation where authorization depends on actions taken by the employer and not the employee.[228] The court reasoned that narrowly interpreting the CFAA was necessary in order to avoid interpreting a criminal statute in a surprising or unexpected way.[229]

In the recent criminal case *U.S. v. Nosal*, the Ninth Circuit reaffirmed its holding in *Brekka* by not only denouncing broad interpretations of the CFAA, but urging circuit courts applying broad interpretations to reconsider.[230] After Nosal left his job at Korn/Ferry, he convinced current Korn/Ferry employees to use their authorized log-in information to steal information for use in Nosal's new business venture.[231] The government charged Nosal and his co-conspirators with numerous CFAA counts.[232]

Declaring that the CFAA failed to provide a remedy for misappropriated information where authorization by the employer had not been rescinded, the court held that Nosal's co-conspirators did not violate the CFAA when they retrieved confidential information through company use accounts.[233] The court rejected the government's proposed broad reading of the CFAA, finding a broad interpretation would transform the CFAA "from an anti-hacking statute into an expansive misappropriation statute." [234] The court countered the government's interpretation by reasoning, "[I]f Congress meant to expand the scope of criminal liability to everyone who uses a computer in violation of computer use restrictions—which may well include everyone who uses a computer—we would expect it to use language better

authorization turns on whether the defendant breached a state law duty of loyalty to an employer.").

[228] *Brekka*, 581 F.3d at 1129–35. First, the court engaged in a plain language reading of the statute, construing the term "without authorization" to mean "without permission." Explicitly rejecting the agency theory because it essentially equates the terms "without authorization" and "exceeds authorized access," the court explained that because Congress included two separate phrases, the only way one would not be rendered meaningless is if it meant different things. Lastly, the court concluded that the agency theory also violated of the rule of lenity, which requires courts to limit the reach of criminal statutes to the clear import of their text and construe any ambiguity against the government. *Id*.

[229] *Id.* at 1135. 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.

[230] *Nosal*, 676 F.3d at 862.

[231] *Id.* at 856 (explaining that Korn/Ferry employees had authorization to access the database, but Korn/Ferry had a policy forbidding disclosing confidential information).

[232] *Id.* at 856.

[233] *Id.* at 863–64 (finding that the plain language of the CFAA expressly prohibits improper access of computer information; it does not prohibit misuse or misappropriation).

[234] *Id.* at 857.

suited to that purpose."[235] Additionally, the Ninth Circuit found no evidence in either the statutory language or history of the CFAA to indicate an intentional displacement of the traditional state tort and contract laws typically governing employer-employee relationships.[236] Unimpressed by the broad interpretations' willingness to hang criminal liability on violations of private computer use policies, the court found the implications appallingly unconstitutional, and used canons of statutory construction and the rule of lenity to settle on its narrow holding.[237] Countering the dissent's claim that the majority's feared "parade of horribles" was unfounded, the court cited to a recent Florida district court case that involved a CFAA claim based on an employee's personal use of a company computer.[238]

The Fourth Circuit recently staked its claim on the narrow side of the split when it decided *WEC Carolina Energy Solutions, LLC v. Miller*.[239] The court held that an employee does not violate the CFAA by downloading confidential information later used in a competing business if, at the time the information is downloaded, the employee was authorized to access the system.[240] Conscious of the canon of consistency and the statute's criminal provisions, the court examined the plain language and construed the statute strictly to avoid an unanticipated or surprising result.[241] The court explicitly

[235] *Id.* (citing the presumption that Congress acts interstitially; unless Congress conveys its purpose clearly, a statute will not be deemed to have significantly changed the federal-state balance in the prosecution of crimes).

[236] *Nosal*, 676 F.3d at 860 (explaining that employer-employee and company-consumer relationships are traditionally governed by tort and contract law and that the government's proposed interpretation would unacceptably allow private parties to manipulate computer use and employment policies into a basis for criminal law).

[237] *Id.* at 856–64. Deciding that a broad reading of the CFAA would render it unconstitutional for a myriad of reasons; primarily lack of notice. "Millions of unsuspecting individuals would find that they are engaging in criminal conduct." *Id.* It is impermissible to allow employers to base criminal liability in what would otherwise be, at most a state tort or contract claim. This could transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved.

[238] *Id.* at n.6 The *Nosal* majority cited *Lee v. PMSI, Inc.*, No. 8:10 CV 2904 T 23TBM, 2011 WL 1742028 (M.D. Fla. May 6, 2011), as an example of the type of unacceptable claims that could come from a broad interpretation of the CFAA. *Id.* In *Lee*, an employer counterclaimed against an employee's wrongful termination suit. The counterclaim alleged that the employee violated the CFAA when she used a company computer for personal reasons like accessing Facebook and sending personal emails, in violation of a computer-use policy. Although the district court dismissed the claim, the *Nosal* majority noted that, "it could not have done so if 'exceeds authorized access' included violations of private computer use policies." *Id.*

[239] *Miller*, 687 F.3d at 204 (originally plaintiff brought one CFAA claim and nine state law claims to the district court, alleging that defendant had breached his employment agreement by using company information for a competitive purpose. When the district court dismissed the CFAA count for failure to state a claim, it declined to exercise jurisdiction over the remaining state law claims. In a footnote, the court described nine alternative available state law remedies that remained available for plaintiffs.).

[240] *Id.*

[241] *Id.* at 207.

rejected the agency and contract views, finding both theories not only contravene Congressional purpose, but are also unnecessary since state law remedies already exist.[242]

The Sixth Circuit relied heavily on the *Brekka* court's interpretation of the term "authorization" in *Pulte Homes, Inc. v. Laborers' International Union of North America*.[243] The court affirmed the dismissal of the plaintiff's complaint citing *Brekka* as persuasive authority.[244] The decision strongly suggests the Sixth Circuit would choose a narrow interpretation of the CFAA as it found the defendants' use of public communication systems to contact the plaintiffs defeated allegations that the access was "without authorization."[245] Meanwhile, numerous district courts within the Sixth Circuit have openly embraced the narrow view.[246]

> Our conclusion here likely will disappoint employers hoping for a means to rein in rogue employees. But we are unwilling to contravene Congress's intent by transforming a statute meant to target hackers into a vehicle for imputing liability to workers who access computers . . . in bad faith, or who disregard a use policy. . . Providing such recourse not only is unnecessary . . . but is violative of the Supreme Court's counsel to construe criminal statutes strictly.

Id.

[242] *Id.* at 206 (describing the deficiencies of an agency theory: "[S]uch a rule would mean that any employee who checked the latest Facebook posting or sporting event scores in contravention of his employer's use policy would be subject to the instantaneous cessation of his agency and, as a result, would be left without any authorization to access his employer's computer systems.").

[243] Pulte Homes, Inc. v. Laborers' Int'l Union of N. Am., 648 F.3d 295 (6th Cir. 2011) (holding that the defendant had not accessed information without authorization under the CFAA because plaintiff's information was open to the public and did not need authorization to access).

[244] *Id.* at 307.

[245] *Id.* The heavy reliance on the Ninth Circuit's narrow interpretation of the CFAA suggests that if the Sixth Circuit ever squarely addresses the meaning of "without authorization" in an employment dispute, it would adopt a narrow view.

[246] *See Dana*, 2012 WL 2524008 at *5 (W.D. Mich. June 29, 2012) (holding that there was no violation of the CFAA because defendants were still employed with Dana Ltd at the time they downloaded company information which they subsequently took with them to work for a competitor, they were authorized to access the information in question); *see e.g. Ajuba*, 871 F. Supp. 2d at 687 (holding that allegations that an employee lost any authorization he had to access the employer's computers, or, exceeded his authorization when he accessed the computers in violation of confidentiality and use limitations, failed to state a claim under the CFAA); *see e.g. ReMedPar*, 683 F. Supp. 2d at 609 (construing "without authorization" narrowly, and dismissing CFAA claim based on use of information that employee was authorized to obtain in a fashion that was adverse to the employer's interests); *see e.g.* Black & Decker, Inc. v. Smith, 568 F. Supp. 2d 929, 934–35 (W.D. Tenn. 2008) (rejecting *Citrin's* agency analysis, and dismissing the CFAA claim that was based not on the employee's accessing of information, but on his later misuse of the information, holding "[C]ongress did not intend to create a private cause of action against employees whose crime . . . merely involved the use of ordinary email in a manner disloyal to their employer and in breach of their employment contract.").

V. ANALYSIS

Broad interpretations of the CFAA miss the mark in just about every possible way.[247] Agency and contract-based interpretations raise serious constitutional concerns and demolish Congress's intended scope by turning an objective access statute into a series of murky subjective inquiries.[248] Broad interpretations disregard established canons of statutory construction and produce unexpected results not in accordance with Congressional intent or due process.[249] Additionally, broad interpretations fail to restrict the CFAA to the types of crime intended by Congress.[250] Adjudicating claims outside the intended scope disrupts Congress's delicate federal-state balance and undermines traditional state powers.[251]

A narrow interpretation is the only way to ensure that the CFAA remains constitutional and avoids surprising results.[252] Following well-established canons of constructions, narrow interpretations comprehensively define the statute's terms to provide notice to employees and guidelines for enforcement.[253] Narrow interpretations also effectuate Congressional intent by restricting the CFAA to types of claims not found in other statutes and leaving existing state laws undisturbed.[254] The CFAA requires a narrow interpretation.[255]

[247] *See generally infra* Part V (explaining how broad interpretations are unconstitutionally vague, overbroad, do not follow canons of statutory construction, do not effectuate Congressional intent, raise federalism concerns, and overstep Congressional spheres of lawmaking, and onto traditional state powers).

[248] *See infra* Part V.A–B (arguing broad interpretations render the CFAA unconstitutionally vague and overbroad).

[249] *See supra* Part II.A, Parts IV.A–B (comparing the actual purpose for the CFAA to fight new types of computer misuse crimes with broad interpretations' application of the statute to address employee misappropriation).

[250] *See supra* Part II.A, Part IV.A–B (comparing the type of crime Congress intended to target with the CFAA to the types of crimes adjudicated under agency and contract-based interpretations of the statute).

[251] *See supra* Part II.A, *infra* Part V.D–E (comparing Congress's carefully restricted scope of the CFAA with broad interpretations' expansive reach which overlaps hugely with traditional state laws Congress meant to leave undisturbed).

[252] *See supra* Part III.A–B, *infra* Part V (explaining requirements that all criminal statutes must meet in order be constitutional and demonstrating that while broad interpretations fall short, a narrowly interpreted CFAA remains constitutional).

[253] *See infra* Part V.A–C (showing how selected canons of statutory construction lead to a narrow interpretation, which, in turn meets the constitutional requirements for the vagueness and overbreadth doctrines).

[254] *See supra* note 47, *infra* Part V.D (explaining the CFAA's purpose as a gap-filler statute and demonstrating how broad interpretations inappropriately allow claims already addressed by existing state laws).

[255] *See infra* Parts V–VI (concluding a narrow interpretation is necessary to effectuate Congressional intent and keep the statute constitutional).

A. The Void for Vagueness Doctrine Requires a Narrow Interpretation of the CFAA

Broad interpretations of the CFAA are unconstitutionally vague.[256] To avoid due process concerns, the CFAA's statutory language and judicial interpretations must define "authorization" to give employees sufficient notice of prohibited behavior and enough definiteness to guide enforcement.[257] At first blush, the statutory terms "without authorization" and "exceeds authorized access" do not appear unduly ambiguous.[258] Narrow interpretations of the CFAA give employees notice of criminal conduct and curb arbitrary enforcement by incorporating the commonly understood definitions of the two critical terms.[259] Conversely, injecting principles of agency or contract law gives these critical terms unorthodox and unclear meanings that fail to adequately notify employees of what behavior is criminal and leave the statute vulnerable to arbitrary enforcement.[260]

Broad interpretations of the CFAA violate the notice prong of the void for vagueness doctrine because they fail to define "authorization" in a way that gives employees clear notice of prohibited computer activities.[261] Nothing in the statutory language of the CFAA hints that authorization depends on an agency relationship or an underlying contract.[262] Moreover, by removing an objective definition of "authorization," broad interpretations remove the required notice of prohibited behavior.[263] Transforming "authorization" into a subjective inquiry gives employees no reliable or predictable way to determine if they have authorization.[264] Employees cannot act in conformity with the CFAA when the statute's meaning varies

[256] *See supra* notes 234–237 and accompanying text (rejecting broad interpretations because they impermissibly expanded the scope of the CFAA).

[257] *See supra* text accompanying note 103 (describing what the void for vagueness doctrine requires from criminal statutes to be constitutional).

[258] *See supra* text accompanying notes 225–226 (explaining that plain language, commonly understood, and dictionary definitions define "without authorization" and "exceeding authorized access" respectively as no permission, and going beyond what is permitted).

[259] *See supra* note 228 (describing why a narrow interpretation of the CFAA was necessary to keep it within the bounds of constitutionality); *see also supra* text accompanying notes 239–242 (explaining the Fourth Circuit's narrow reading of the CFAA).

[260] *See supra* note 216 (describing why agency and contract-based interpretations fail to provide a clear definition for the CFAA's critical terms).

[261] *See supra* note 103 and accompanying text (detailing the notice required under the void for vagueness doctrine and showing such notice is enough to allow citizens to conform their behavior to lawful conduct).

[262] *See supra* Part II.F (describing the statutory language of the CFAA); *see also supra* note 82 (describing the statute).

[263] *See supra* note 237 (describing why a broad interpretation lacks the notice required for all criminal statutes).

[264] *See supra* text accompanying notes 162–164 (establishing that under agency theory, authorization depends entirely on the employee's mental state).

according to the personal predilections of each employer.[265] Broad interpretations engender too much unpredictability in place of the notice required by the vagueness doctrine.[266]

Agency-based applications of the CFAA were established in cases featuring former employees whose tortious malfeasance made notice a nonissue.[267] Despite the fact that agency law does not translate or practically apply to the nuanced pragmatisms of everyday employment, the holding from *Citrin* governs in at least the First Circuit.[268] In the First Circuit, terminating an employee's authorization after any breach of loyalty would likely mean that an employee who takes ten minutes to peruse social media sites has terminated her access if her employer decides that act was adverse to the company's interest.[269] Unbeknownst to the employee, her authorization would be terminated even after closing out of the website and returning to work.[270] Weeks, months, or years of diligent work later, the employee's access is still seemingly terminated because she has been "without authorization" since acting contrary to her employer's interest.[271]

A myriad of innocuous activities like checking the news, weather, or emailing a friend could suddenly carry criminal penalties under agency-based interpretations of the CFAA.[272] No court applying agency law to the CFAA has considered the effect of momentary work distractions or has decided what type of act is sufficiently adverse to terminate an employee's authorization.[273] The confusion and vagueness compounds when employers decide, maybe even retroactively, when authorization terminates.[274] What

[265] *See supra* text accompanying notes 162–164 (establishing that under agency theory, authorization depends entirely on the employee's mental state).

[266] *See supra* note 237 (describing why a broad interpretation lacks the notice required for all criminal statutes).

[267] *See supra* notes 157–184 and accompanying text (summarizing the emergence of agency-based interpretations of the CFAA in cases like *Explorica*, *Shurgard*, and *Citrin*).

[268] *See supra* text accompanying note 173 (holding that an employer's subjective view of an employee's adverse act terminates authorization immediately).

[269] *See supra* text accompanying notes 177–184 (demonstrating how the holding from *Citrin* could apply to a less extreme, but very typical employment situation).

[270] *See supra* notes 177, 182 (applying agency law to immediately terminate authorization upon an employee's adverse thought or action with no discussion of when authorization might reinstate).

[271] *See supra* notes 177, 182 (applying agency law to immediately terminate authorization upon an employee's adverse thought or action with no discussion of when authorization might reinstate).

[272] *See supra* text accompanying notes 162–165 (explaining how terminating authorization depends on the employer's subjective view of what employee actions do not further the interest of the company).

[273] *See supra* text accompanying notes 157–184 (summarizing main agency cases; none address the issue of reinstating an employee's authorization).

[274] *See supra* text accompanying notes 157–184 (case law has not yet addressed this kind of ex post-facto application in an agency interpretation of the CFAA. However, it is a logical extension of current holdings, and if allowed, would trigger even more due process concerns.).

one employer may tolerate—occasional non-business-related web browsing—another might find an outrageous and blatant misuse of company time and resources.[275] Within the spectrum of typical employee behavior, agency interpretations of the CFAA simply do not provide employees with sufficient notice of authorization.[276]

Proponents of contract-based interpretations of the CFAA claim that an employee's signature on a contract or a clearly communicated company policy fulfills any notice requirement.[277] This argument misses the mark because nothing in the language of the CFAA puts an ordinary employee on notice that authorization is revoked and criminal liability triggered by breaching a private contract.[278] Absent express statutory language to the contrary, an ordinary employee would reasonably expect that breaching a private agreement could result in exposure to civil liability, not imprisonment.[279] Unless the underlying agreement specifically delineates employee actions that terminate "authorization," notice is not there.[280]

Additionally, many company policies or employment contracts contain vague terms or provisions.[281] For example, generic terms prohibiting "non-business purposes," or limiting computer use to "legitimate company business," provide insufficient notice to employees of what computer use is prohibited.[282] Countless employees sit in front of computers all day; without detailed instructions to guide them through prohibited uses or what is permitted if done off the clock, employees could inadvertently breach a contract while reading the news online over lunch.[283] Like the agency approach, a contract-based interpretation of the CFAA is vague because employees do not have sufficient notice of prohibited behavior when

[275] *See supra* text accompanying notes 162–165 (explaining how terminating authorization depends on the employer's subjective view of what employee actions do not further the interest of the company).

[276] *See supra* notes 103–105 (requiring all criminal statutes to provide enough definiteness to put ordinary people on notice as to what conduct is prohibited so they can conform their behavior accordingly).

[277] *See supra* text accompanying note 202 (explaining notice is not an issue when the defendant had reason to know that accessing data to further a criminal act could incur criminal liability).

[278] *See supra* Part II.F (explaining current provisions of the CFAA); *see also* note 82 (describing the statute).

[279] *See supra* note 87 and accompanying text (describing breaches of contracts as an area traditionally governed by contract law).

[280] *See supra* notes 209–213 and accompanying text (describing various problems with allowing contract drafters to establish criminal penalties).

[281] *See supra* text accompanying note 191 (describing how the underlying contract term that was breached in *Explorica* prohibited disclosing information "contrary to the interests of EF").

[282] *See supra* note 104 (failing to distinguish between innocent conduct and conduct calculated to cause harm can render a statute vague).

[283] *See supra* note 104 (failing to distinguish between innocent conduct and conduct calculated to cause harm can render a statute vague).

authorization depends on an employer's subjective interpretation of an underlying agreement.[284]

In contrast to the broad approaches' vacillating definition of "authorization," a narrow interpretation of the CFAA ensures that employees have notice of prohibited conduct.[285] Due process concerns of notice are alleviated through a narrow interpretation's objective definition of "authorization."[286] A narrow interpretation requires employers to take affirmative action to restrict or rescind authorization instead of arbitrary employee activity or an employer's subjective intent immediately terminating authorization.[287] An ordinary employee understands that information accessed by entering false information or circumventing security measures would be unauthorized.[288] A narrow interpretation of the CFAA is the only way to ensure that employers have the notice required of all criminal statutes.[289]

The inherent uncertainty plaguing the broad interpretations' definition of "authorization" also leaves the CFAA highly susceptible to arbitrary and discriminatory enforcement in violation of the vagueness doctrine's second prong.[290] Almost any employee action could be construed to terminate authorization when an employer subjectively defines the agency relationship or interprets a broadly-drafted contract.[291] Under an agency interpretation, an employee's inadvertent termination of his agency status means that each time he subsequently accesses a company computer, he is "without authorization," which violates the CFAA.[292] Similarly, contract-based interpretations could unwittingly catch millions of employees in technical breach of broadly-drafted, vaguely-worded employment

[284] *See supra* note 202 (explaining how unsuspecting employees could incur civil and criminal liability under agency-interpretations of the CFAA because employers do not need to inform employees when authorization has terminated).

[285] *See supra* note 233 (defining the term authorization by its commonly understood definition, permission, gives employees notice that accessing a company computer without permission is prohibited).

[286] *See supra* text accompanying notes 217–219, 226 (using the commonly understood definitions of authorization to mean permission).

[287] *See supra* note 107 (explaining that a statute is impermissibly vague if enforcement depends on a completely subjective standard).

[288] *See supra* note 233 (defining the term authorization by its commonly understood definition, permission, gives employees notice that accessing a company computer without permission is prohibited).

[289] *See supra* notes 110–112 and accompanying text (discussing how courts can save a potentially vague statute through a narrow interpretation).

[290] *See supra* text accompanying notes 106–108 (detailing the second prong of the void-for-vagueness test).

[291] *See supra* text accompanying notes 161–165, 210–211 (illustrating that terminating authorization depends on the employer's subjective view of what employee actions do not further the interest of the company or on how an employer interprets an employment agreement).

[292] *See supra* note 173 and accompanying text (explaining that terminating agency relationship contemporaneously terminates any authorization).

agreements.[293] Using the CFAA, employers, service providers, and the government can target whomever they want by deciding either that agency status has terminated or by interpreting an underlying contract to find a breach.[294] Without guidelines to ensure that only serious computer misuse crimes are prosecuted, broad interpretations of the CFAA are unconstitutionally vague.[295]

Unlike broad interpretations, a narrow interpretation of the CFAA removes the threat of arbitrary or discriminatory enforcement by eliminating unsuspecting and innocent employees from the statute's scope.[296] The subjective definition of "authorization" under broad interpretations provides neither sufficient notice to employees nor the predictability in enforcement that due process requires.[297] These interpretations of the CFAA are unconstitutionally vague.[298] Until Congress acts, courts are faced with the responsibility of constitutionally interpreting the CFAA.[299] A narrow interpretation is the only way the CFAA passes constitutional muster under the vagueness doctrine.[300]

B. The Overbreadth Doctrine Requires a Narrow Interpretation of the CFAA

Broad interpretations hurl the CFAA into the depths of unconstitutional overbreadth.[301] Agency and contract-based interpretations of the CFAA render the statute overbroad by criminalizing an incredible range of conduct in which normal, law-abiding citizens regularly engage.[302] Keeping lawful and constitutionally protected behavior out of the CFAA's

[293] *See supra* text accompanying notes 211–213 (allowing service providers to draft agreement contracts which result in criminal sanctions gives them complete power).

[294] *See supra* notes 213–216 and accompanying text (criminally prosecuting a woman for breaching MySpace's terms of service agreement).

[295] *See supra* note 237 (finding broad interpretations unconstitutionally vague by transforming entire categories of otherwise innocent behavior into federal crimes).

[296] *See supra* text accompanying notes 234–235 (explaining how broad interpretations transform the CFAA from a criminal hacking statute into an expansive misappropriation statute).

[297] *See supra* notes 106–108 and accompanying text (drawing no distinction between innocent conduct and conduct calculated to cause harm renders a statute unconstitutionally vague).

[298] *See supra* note 237 (outlining the different ways that broad interpretations fail to provide notice and encourage arbitrary enforcement).

[299] *See supra* notes 110–112 and accompanying text (directing courts to save a statute from vagueness through a narrow interpretation if plausible).

[300] *See supra* note 103 and accompanying text (explaining the vagueness doctrine and what is required in order for a statute to be in compliance with the Constitution).

[301] *See supra* text accompanying notes 27, 114–116 (describing the CFAA as the primary federal statute used to combat computer crime. A statute will be overbroad if its sanctions apply to constitutionally protected activity.).

[302] *See supra* note 152 (explaining how broad views terminate authorization based on an employee's intent regardless of subsequent actions).

reach and sidestepping overbreadth concerns requires a narrow interpretation.[303]

Allowing criminal liability to hinge on an employee's subjective intent at any given moment renders an agency-based interpretation of the CFAA improperly overbroad by capturing hoards of legitimate behavior and producing uncertain results.[304] Agency interpretations of the CFAA transform substantial amounts of innocent employee conduct into actionable malfeasance by turning an employee's subversive thought—however fleeting or harmless—into a total termination of access.[305] To the agency interpretation's logical conclusion, every employee giving notice spends her last two weeks incurring potential civil and criminal liability each time she accesses a computer.[306] Sweeping so much plainly legitimate activity into a criminal statute's scope makes an agency-based interpretation of the CFAA unconstitutionally overbroad.[307]

A contract-based interpretation of the CFAA is overbroad because it allows private parties to determine criminal conduct and allows the government to prosecute constitutionally protected behavior that is otherwise non-punishable.[308] Granting employers and service providers unilateral power to construct agreements where breaches result in criminal and civil liability encourages even broader underlying contracts.[309] Determining liability based on the mere breach of an agreement instead of analyzing the validity of the underlying agreement elicits vagueness concerns, overbreadth

[303] *See supra* text accompanying notes 228–229 (discussing how keeping the CFAA constitutional requires a limiting interpretation).

[304] *See supra* note 213–216 and accompanying text (explaining that holding a misdemeanor as a violation of the CFAA is unconstitutionally overbroad and vague).

[305] *See supra* text accompanying notes 234–235 (explaining that broad interpretations transform the CFAA from a criminal hacking statute into an expansive misappropriation statute).

[306] *See supra* notes 234–237and accompanying text (illustrating how a broad interpretation of the CFAA can capture lots of legitimate activity. An employee's two-week notice of termination, even though customary, is still adverse to the employer's interest. Under a broad, contact-based interpretation of the CFAA, the act of giving notice immediately terminates the employee's authorization. Even if the employee still has valid log-in information and can access computer files, any access past the adverse act is without authorization.).

[307] *See supra* text accompanying notes 115, 161 (hinging authorization on an employer's subjective view of adverse to his interest increases the likelihood that much of an employee's subsequent legitimate behavior is also unauthorized).

[308] *See supra* text accompanying notes 115, 209–212 (comparing government's inability to prohibit constitutionally protected behavior with an employer or service provider's ability to write any terms they desire).

[309] *See supra* text accompanying notes 115, 209–212 (drafting contracts to provide maximum protection for the employer encourages using broad and vague terms, can also improperly restrict speech in violation of the First Amendment).

concerns, and the potential to substantially infringe on constitutionally protected behavior.[310]

Tying criminal liability to the terms of privately drafted agreements runs a severe risk of curbing First Amendment freedoms.[311] If an employment contract prohibits employees from expressing pro-choice views, an employee could be held criminally liable under a broad interpretation of the CFAA for emailing a friend to express a pro-choice view—even if done on his own time from a personal email account—if the email was sent from a company computer.[312] Individuals are free to commit to this type of contract provision with other private parties.[313] However, the government cannot use the CFAA to indirectly prosecute behavior that it cannot directly punish.[314] The Free Speech Clause restricts government regulation of private content-based speech; the government cannot make an end-run around the United States Constitution by using an employee's breach of a private contract to punish the same constitutionally protected expression.[315]

Terms of service agreements containing the same type of provision could severely impinge freedom of speech by restricting seemingly public sites and inhibiting the free flow of information.[316] Contract-based interpretations of the CFAA impermissibly allow private parties to determine criminal penalties, and allow the government to control otherwise constitutionally protected behavior.[317] The implications of a contract-based interpretation of the CFAA are appallingly and unconstitutionally overbroad.[318]

[310] *See supra* notes 103, 186 (showing how the due process required for all criminal statutes per the vagueness doctrine is not examined under a contract-based interpretation of the CFAA).

[311] *See supra* notes 115–117 (explaining that statutes are overbroad if they violate a constitutionally protected right).

[312] *See supra* text accompanying note 187 (breaching an employment agreement under a contract-based interpretation of the CFAA renders an employee's subsequent computer access either without authorization or exceeding authorized access).

[313] *See supra* notes 113–117, 213–216 and accompanying text (describing how broad interpretations of the CFAA can infringe on constitutionally protected rights).

[314] *See supra* text accompanying note 114 (explaining that statutes are overbroad if sanctions apply to conduct that the government is not entitled to regulate).

[315] *See supra* notes 113–117, 213–216 and accompanying text (describing how broad interpretations of the CFAA can infringe on constitutionally protected rights).

[316] *See supra* note 114 and accompanying text (explaining that statutes are overbroad if they violate a constitutionally protected right).

[317] *See supra* note 114 and accompanying text (explaining that statutes are overbroad if sanctions apply to conduct that the government is not entitled to regulate). *See also* text accompanying note 123 (proscribing criminal conduct falls to legislatures and not private parties).

[318] *See supra* note 114 and accompanying text (explaining that statutes are overbroad if sanctions apply to conduct that the government is not entitled to regulate).

The CFAA is already set up to capture millions of Americans who use computers daily.[319] A narrow interpretation of the CFAA is required in order to keep the prohibited behavior limited to illegal activity and not in violation of the overbreadth doctrine.[320]

C. Canons of Statutory Construction Require a Narrow Interpretation of the CFAA

Broad interpretations of the CFAA run completely contrary to basic canons of statutory construction that exist to help guide a court to Congress's intended purpose.[321] Unsurprisingly, courts ignoring these canons to arrive at a broadly interpreted result also ignore the CFAA's intended purpose.[322] Agency and contract-based interpretations veer inappropriately into Congress's stead of lawmaking by disregarding widely established canons like the rule of lenity, the plain language rule, no mere surplusage, and the canon of consistency to get to a desired result.[323] In contrast, courts seeking to effectuate the plain language of the CFAA in consonance with other canons of statutory construction end up with a narrow interpretation.[324] Recognizing that these statutory tools exist to help courts uncover the true legislative intent, courts narrowly interpreting the CFAA stay faithful to these canons.[325] Sticking to these established statutory canons results in a constitutionally sound, congressionally supported, narrow, interpretation of the CFAA.[326] Consequently, broad interpretations that thwart these established canons are entirely incorrect.[327]

[319] *See supra* notes 77–79 and accompanying text (describing that the CFAA's scope includes all computers).

[320] *See supra* note 216 and accompanying text (concluding a narrow interpretation is necessary in order to keep the CFAA from capturing unsuspecting and innocent behavior).

[321] *See supra* Part II.A, text accompanying note 99, and Part IV.A–B (comparing the purposes of the CFAA and canons of statutory construction with a broad interpretation).

[322] *See supra* Part II.A, text accompanying note 99, and Part IV.A–B (comparing the purposes of the CFAA and canons of statutory construction with a broad interpretation).

[323] *See infra* Part V.C (explaining how broad interpretations of the CFAA disregard canons of statutory construction and distort Congressional intent).

[324] *See supra* Part II.A, Part III.C–F, and Part IV.C (comparing the purposes of the CFAA and canons of statutory construction with a narrow interpretation).

[325] *See infra* Part V.C (arguing that narrow interpretations faithfully follow established canons of statutory constructions and lead to effectuating the actual intent behind the CFAA).

[326] *See infra* Part V.C (arguing that narrow interpretations faithfully follow established canons of statutory constructions and lead to effectuating the actual intent behind the CFAA).

[327] *See infra* Part V.C (arguing that narrow interpretations faithfully follow established canons of statutory constructions and lead to effectuating the actual intent behind the CFAA).

1. The Rule of Lenity Requires a Narrow Interpretation of the CFAA

The rule of lenity's application to the CFAA is appropriate and necessary.[328] The constitutional requirement of fair notice coupled with the divisive split in authority overwhelmingly satisfies the rule's stringent prerequisites.[329] The CFAA's primary use in civil contexts does not discount the rule of lenity's application; it is a criminal statute, and citizens are required to have fair notice of criminal conduct.[330] Furthermore, the CFAA's extreme ambiguity is evidenced by the disparate and inconsistent definitions accorded to "authorization" across the three views.[331] All three theories have plunged headfirst into the CFAA's legislative history and all have emerged clutching selective excerpts to support their view.[332] Even with the cautioned use of the rule of lenity as one of last resort, its use is necessary to keep the CFAA in alignment with constitutional standards.[333]

Applying the rule of lenity to the CFAA produces results consistent with a narrow view.[334] Resolving ambiguity in favor of the defendant requires constraining the scope of the CFAA to only apply to conduct that is clearly prohibited.[335] A narrow interpretation accomplishes this by limiting the CFAA's scope to its commonly understood meaning.[336] Broad interpretations inappropriately breathe agency and contract law into the CFAA when neither body of law is found in the statute's plain language or the legislative history.[337] Additionally, the broad interpretations' inherent

[328] *See supra* note 125 and accompanying text (describing the rule of lenity's use as a canon of statutory construction as one of last resort; to be invoked only when there is serious ambiguity in the statute).

[329] *See supra* text accompanying notes 125–126, 150–156 (comparing the rule of lenity's prerequisites and the current split in authority over the definition of "authorization" in the CFAA).

[330] *See supra* text accompanying notes 27, 103 (describing the CFAA as primarily a criminal statute, and explaining that all statutes with criminal applications are subject to the vagueness doctrine).

[331] *See supra* text accompanying notes 150–156 (describing the current circuit court split over the definition of "authorization" in the CFAA).

[332] *See supra* notes 175–176, 228–235 and accompanying text (comparing broad interpretations supporting legislative history with narrow interpretation's supporting legislative history).

[333] *See supra* text accompanying notes 125–126, 150–156 (comparing the rule of lenity's prerequisites and the current split in authority over the definition of "authorization" in the CFAA).

[334] *See supra* text accompanying note 237 (interpreting the CFAA narrowly and consistently with the rule of lenity).

[335] *See supra* text accompanying note 119 (applying the rule of lenity requires choosing the interpretation most protective of the defendant to ensure sufficient notice).

[336] *See supra* notes 217–219 and accompanying text (describing how a narrow interpretation of the CFAA applies).

[337] *See supra* notes 84, 152–154 and accompanying text (comparing the plain language of the statute with overview of broad views' application).

lack of notice produces surprising and unexpected results.[338] Employees who understand "authorization" to mean permission would be surprised if authorization terminated abruptly and without notice through agency or contract law, especially if employees are still able to access company accounts or accurately log into a company computer.[339] Lastly, broad interpretations of the CFAA incorrectly favor plaintiffs by allowing an employer's subjective motivation to dictate criminal and civil liability.[340]

When a statute like the CFAA produces such varying and inconsistent results, the rule of lenity is required to make sure that due process requirements are being met and that rulemaking stays in the legislative sphere.[341] The rule of lenity directs courts to choose a narrow interpretation of the CFAA because out of the three interpretations currently in play across jurisdictions, it is the one most protective of defendants.[342]

2. The Plain Language of the CFAA Requires a Narrow Interpretation

The plain language of the CFAA prohibits improper access to information.[343] A court tracking the plain language of the CFAA will limit claims to those alleging improper access because that is as far as the statutory language extends.[344] A narrow interpretation follows the plain language rule by correctly restricting the CFAA's scope to its statutory language and supplementing only undefined terms with commonly understood meanings.[345] Broad interpretations extend impermissibly beyond any plain language interpretation of the CFAA by incorporating "purpose" or "use" and subjective intent into a statute that deals objectively with access.[346]

[338] *See supra* note 229 and accompanying text (explaining that employees would be surprised if they were suddenly subject to criminal sanctions despite continued access to company computers).

[339] *See supra* note 128 (explaining that an employee breaching an employment contract or terms of service agreement would not expect that breach to result in criminal liability).

[340] *See supra* notes 82, 152–154 and accompanying text (comparing the plain language of the statute with overview of broad views' application).

[341] *See supra* notes 224–227 and accompanying text (describing why a narrow interpretation stays true to the statutory language and is most protective of defendants).

[342] *See supra* notes 227–229 and accompanying text (describing why a narrow interpretation stays true to the statutory language and is most protective of defendants).

[343] *See supra* note 82 (describing the CFAA).

[344] *See supra* notes 82, 226 and accompanying text (explaining a plain language definition of the CFAA).

[345] *See supra* notes 139–142 and accompanying text (describing that Congress acts purposefully in choosing words for statutes).

[346] *See supra* note 11 (focusing on how an employee uses the accessed information to determine liability).

Broad interpretations construe the CFAA as if it reads "exceeds authorized use" instead of "exceeds authorized access."[347] Agency and contract-based interpretations examine the subsequent purpose and use for the improperly accessed information instead of following the statute's directive and examining whether access was authorized.[348] What an employee does with the information taken from a computer is separate from how an employee accessed the information in the computer and the CFAA speaks only to the latter.[349] Interpreting the CFAA according to the statute's plain language requires a narrow interpretation.[350]

Broad interpretations of the CFAA not only violate the letter of the plain language rule by inserting extraneous words into the statute, they also violate the spirit of the rule by directly contradicting Congressional intent.[351] Congress originally included "use" in the statute but replaced it with "exceeds authorized access" in the first round of amendments.[352] Agency and contract-based interpretations are incorrect because persistent incorporation of "use" flagrantly returns the CFAA to a version Congress has expressly revoked.[353]

With no definition of "without authorization" in the CFAA, the plain language rule directs courts to define the term in accordance with its ordinary meaning.[354] Courts narrowly interpreting the CFAA follow this fundamental rule and look to dictionaries and common usage to define "authorization" as "permission or power granted by authority."[355] In the employment context, an employer grants access by providing an employee with a user name and password.[356] Once an employee has this access, any subsequent improper access would fall under the CFAA provision "exceeding authorized access."[357] Only non-employees, employees without initial access, and

[347] *See supra* text accompanying note 173 (basing liability on an employee's adverse intent).

[348] *See supra* text accompanying note 173 (basing liability on an employee's adverse intent).

[349] *See supra* notes 229, 233 (describing the difference between basing liability on access or improper motive).

[350] *See supra* text accompanying notes 27, 130–138 (comparing the language of the CFAA to the plain language doctrine).

[351] *See supra* notes 59–60 and accompanying text (describing why Congress removed "use" from the CFAA in 1986).

[352] *See supra* text accompanying note 59 (describing the language of the original CFAA).

[353] *See supra* note 60 (describing why Congress removed "use" from the CFAA in 1986).

[354] *See supra* notes 137–138 and accompanying text (directing a court to use an ordinary, commonly understood meaning for an undefined statutory term).

[355] *See supra* note 246 (summarizing how various courts have come to the same definition of "authorization" under a narrow interpretation).

[356] *See supra* text accompanying notes 217–219 (describing a narrow interpretation of the CFAA).

[357] *See supra* text accompanying note 240 (finding an employee with access cannot be without authorization under the CFAA).

employees with revoked authorization qualify as "without authorization" under the CFAA.[358] This narrow, straightforward reading of the CFAA accurately and objectively focuses the inquiry on access.[359]

The plain language of the CFAA directs courts to objectively analyze whether an employee's access was authorized by framing the statute in terms of "access."[360] Narrow interpretations undertake this objective analysis in consonance with the plain language by focusing on the actions taken by an employer to grant or deny access.[361] Broad interpretations instead embark on a subjective assessment of the employee's intent.[362] This subjective analysis is completely unwarranted because the CFAA contains no language suggesting that liability hinges on a breach of contract or termination of an agency relationship.[363] Broad interpretations predicating liability on a subjective assessment of an employee's subsequent use of information are beyond the scope of the CFAA and contrary to its plain language.[364] While other obligations owed to an employer like company policies, employment agreements, or fiduciary duties may prohibit misuse of computer accessed information, the plain text of the CFAA does not.[365] Broad interpretations violate the plain language of the CFAA by failing to limit the statute's scope to the statutory language.[366]

The statutory language of the CFAA expressly prohibits improper access of computer information.[367] This is precisely the definition and scope under a narrow interpretation of the CFAA.[368] Following the plain language rule, narrow interpretations appropriately restrict the CFAA to claims alleging improper access.[369] Claims alleging misuse are correctly dismissed

[358] *See supra* text accompanying notes 217–219 (describing a narrow interpretation of the CFAA).

[359] *See supra* text accompanying notes 217–219 (describing a narrow interpretation of the CFAA).

[360] *See supra* text accompanying note 219 (focusing liability on the affirmative actions of an employer).

[361] *See supra* text accompanying note 233 (failing to revoke an employee's access means they are not without authorization under the CFAA).

[362] *See supra* text accompanying note 152 (focusing on the employee's intent to determine liability under broad interpretations of the CFAA).

[363] *See supra* notes 27, 227 (illustrating the actions prohibited under the CFAA and noting that nothing in the language indicates agency or contract law applies).

[364] *See supra* notes 57–67 and accompanying text (removing "use" as a basis for liability in an early amendment).

[365] *See supra* notes 57–67 and accompanying text (limiting actions proscribed by the statutes to unauthorized access or access that exceeds authorization).

[366] *See supra* notes 57–67 and accompanying text (limiting actions proscribed by the statutes to unauthorized access or access that exceeds authorization).

[367] *See supra* note 233 (determining the plain language meaning of the statutory language).

[368] *See supra* notes 225–227 and accompanying text (narrowly interpreting the language so that it only applies to conduct clearly proscribed by the CFAA's plain language).

[369] *See supra* text accompanying notes 217–219 (describing a narrow interpretation of the CFAA).

under narrow interpretations since "use" is neither in the CFAA's vernacular nor part of the commonly understood definition of "authorization."[370]

3. *The Canon "No Mere Surplusage" Requires a Narrow Interpretation of the CFAA*

The broad, agency-based interpretation of the CFAA violates the canon of construction "no mere surplusage" by collapsing the distinction between "without authorization" and "exceeding authorized access."[371] Applying the canon of no mere surplusage to the CFAA reminds courts that Congress chooses statutory language purposefully and would not have included both of the terms "without authorization" and "exceeds authorized access" in the CFAA if they simply meant the same thing.[372] Any court applying agency theory to the CFAA blatantly ignores the duty to effectuate Congressional intent by rendering the term "exceeds authorized access" superfluous.[373] The agency-based interpretation's clear violation of no mere surplusage makes it an incorrect interpretation of the CFAA.[374]

A careful examination of the CFAA's structure and its legislative history reveals why an agency interpretation is so egregious.[375] Quite simply, the difference between unauthorized access and exceeding authorized access matters.[376] The terms were not meant as synonyms.[377] Senate reports indicate that Congress associated the term "without authorization" with outsiders, and "exceeds unauthorized access" with insiders.[378] The CFAA was structured purposefully to reflect these two separate groups of violators: insiders and outsiders are treated differently.[379] Congress generally viewed insiders as less culpable than outsiders and the various subsections and penalty schemes

[370] *See supra* notes 225– 229 and accompanying text (narrowly interpreting the language so that it only applies to conduct clearly by the CFAA's plain language).

[371] *See supra* text accompanying notes 139–140 (presuming Congress uses words purposefully and courts should give effect to every word if possible).

[372] *See supra* note 140 and accompanying text (assuming that because a statute included both "uses" and "carries," Congress intended each word to have a distinct meaning).

[373] *See supra* note 228 (rejecting an agency approach because it renders part of the statute meaningless).

[374] *See supra* note 228 (rejecting an agency approach because it renders part of the statute meaningless).

[375] *See supra* Part II.A–B (targeting outsiders in the CFAA but also including insiders in certain circumstances).

[376] *See supra* notes 65–66 (explaining the purpose between having two separate phrases in the CFAA).

[377] *See supra* notes 65–66 (explaining the purpose between having two separate phrases in the CFAA).

[378] *See supra* notes 60–67 and accompanying text (demonstrating Congress used the term "without authorization" to apply to outsiders and the term "exceeds authorized access" to apply to insiders with an existing level of authorization).

[379] *See supra* notes 60–67 and accompanying text (demonstrating Congress used the term "without authorization" to apply to outsiders and the term "exceeds authorized access" to apply to insiders with an existing level of authorization).

reflect this sentiment.[380] For example, an early amendment removed the term "exceeds authorized access" from a subsection that previously contained both terms because Congress wanted to limit applicability to outsiders.[381] Congress's conscientious use of two separate terms—each with its own unique definition—demonstrates why any interpretation that transposes or conflates the meaning of the two terms is incorrect.[382]

Agency theory eliminates any distinction between the terms "without authorization" and "exceeds authorized access."[383] Terminating authorization immediately upon any employee act that does not further the employer's interest defines "without authorization," but renders "exceeds authorized access" meaningless.[384] The employee either has authorization when accessing his employer's computer system to further the company's interests, or he has no authorization upon acting adversely to his employer's interest.[385] The employee can never "exceed authorized access;" he is either authorized or unauthorized.[386] Eliminating an entire explicitly defined term indicates that an agency-based interpretation of the CFAA is inappropriate.[387]

Beyond compressing two distinct statutory terms into one, agency-based interpretations completely invert Congress's intent for outsiders to be categorized as acting "without authorization" with insiders acting to "exceed[ ] authorized access."[388] By terminating current employees' authorization upon adverse acts, agency-based interpretations of the CFAA hold that current employees act "without authorization" instead of "exceeding

[380] *See supra* note 65 (outlining the CFAA which imposes the most severe penalty on a subsection that uses the term "without authorization" but not "exceeds authorized access); *see also* note 32 (comparing subsections of the statute that include both terms "without authorization" and "exceeds authorized access" with subsections that only use the term "without authorization"); *see also* note 226 (differentiating the terms "without authorization" and "exceeds authorized use").

[381] *See supra* notes 66–67 (expressing concern that leaving insiders in this subsection would expose them to liability for computer misuses which should not rise to the level of criminal conduct).

[382] *See supra* note 227 (explaining it is incorrect to interpret a statute in a way that leaves part of the language in the statute meaningless).

[383] *See supra* note 228 (rejecting an agency approach because it renders part of the statute meaningless).

[384] *See supra* text accompanying notes 173–174 (holding that the defendant, who was an employee at the time of the alleged access, was "without authorization" after terminating his agency relationship).

[385] *See supra* text accompanying notes 162–164 (explaining how an employee is either authorized or unauthorized under an agency-based interpretation of the CFAA).

[386] *See supra* text accompanying notes 162–164 (explaining how an employee is either authorized or unauthorized under an agency-based interpretation of the CFAA).

[387] *See supra* text accompanying notes 139–142 (explaining that Congress chooses statutory language carefully and any interpretation that ignores part of the statutory language does not effectuate Congressional intent).

[388] *See supra* notes 65–67, 173 (comparing Congressional intent in using two separate terms for insiders and outsiders, with an agency-based interpretation which applies the terms incorrectly).

authorized access" which Congress intended for insiders.[389] Similarly contravening Congressional intent under a contract-based interpretation of the CFAA, the First Circuit in *Explorica* held that a former employee (outsider) had "exceeded authorized access" (Congress's designated term for insider) by accessing a public website.[390] Agency courts for the most part unabashedly ignore this canon of statutory construction, unconcerned with the distorted CFAA they leave in their wake. Courts attempting to address the canon of no mere surplusage under an agency-based interpretation the CFAA have struggled to articulate any meaningful difference between the two terms.[391]

An agency-based interpretation of the CFAA is incorrect because it inverts Congressional intent and fails to distinguish between separate phrases in the statute.[392] On the other hand, a narrow interpretation of the CFAA gives sensible and distinct constructions to "without authorization" and "exceeds authorized access" in accordance with Congressional intent.[393] Under a narrow interpretation, a person is "without authorization" only when initial access is not permitted, and a person "exceed[s] authorized access" when initial access is permitted, but the access of certain information is not permitted.[394] This narrow view gives each term a distinct meaning and supports Congress's intended application by applying "without authorization" to outsiders and applying "exceeds authorized access" to insiders.[395]

4. *The Canon of Consistency Requires a Narrow Interpretation of the CFAA*

Courts broadly interpreting the CFAA do not appear overly concerned with the canon of consistency.[396] However, ignoring this canon is

[389] *See supra* note 173 and accompanying text (holding that once an employee acts adversely to his employer, he is "without authorization" and leaving no situation where an employee could ever "exceed authorized access" like Congress intended).

[390] *See supra* text accompanying notes 193–194 (finding under a contract-based interpretation that the employee had broken a confidentiality agreement by acting adversely to the employer's interests).

[391] *See supra* text accompanying note 184 (admitting the difference was "paper-thin" and using *Explorica*'s holding as evidence of the distinction in terms).

[392] *See supra* notes 162–165 and accompanying text (holding an employee is "without authorization" once they act adversely to their employer); *see also* notes 188–194 and accompanying text (applying a contract-based interpretation of the CFAA producing results incongruent with Congressional intent).

[393] *See supra* note 226 (explaining in differences in the two terms under a narrow interpretation).

[394] *See supra* note 226 (explaining in differences in the two terms under a narrow interpretation).

[395] *See supra* note 227 (rejecting the agency theory because it equates the two terms contravening Congressional intent).

[396] *See supra* Part V.A–B (describing how broad definitions fail to consider how precedent will affect situations outside the one at issue).

a grievous error when interpreting a statute like the CFAA.[397] Congress dictated that the same meaning should be applied throughout the statute by providing one definition for "exceeds authorized access" and using the term in multiple sections.[398] Although the CFAA repeats the same terms continuously, the elements for each subsection vary.[399] Each subsection's unique elemental composition requires that courts use caution when interpreting a term since that term's definition will apply to the entire statute.[400]

Courts broadly interpreting the CFAA in civil contexts are quick to adopt definitions that work for the immediate case but could not translate across subsections or to a criminal context without violating other constitutional protections.[401]

A narrow interpretation of the CFAA is the only way for courts to successfully apply consistent definitions across subsections and effectuate Congressional intent.[402] The Ninth Circuit recognized this in *Nosal* when it rejected the government's proposed broad definition of "exceeds authorized access."[403] Although the definition was proposed for the fraud provision charged in the case, the court correctly considered how the definition would affect other subsections of the statute.[404] Inserting the proposed meaning into the broadest subsection of the CFAA containing the term "exceeds authorized access," (a subsection requiring only that a person who "exceeds authorized access" obtain information from a protected computer), the court wisely declined the government's definition.[405] Since obtaining information

[397] *See supra* notes 32, 82–83 and accompanying text (describing Congress's repeated use of the same terms—i.e. "without authorization" and "exceeds authorized access"—throughout the CFAA as well as noting the statute's criminal and civil applications).

[398] *See supra* notes 145–148 and accompanying text (stating that identical words and phrases within a statute should be given the same meaning).

[399] *See supra* notes 65, 82–83 and accompanying text (describing the different sections of the CFAA).

[400] *See supra* notes 145–149 and accompanying text (illustrating why a court should take care when interpreting statutes with criminal and civil applications).

[401] *See supra* Part V.A–B (describing how broad definitions fail to consider how precedent will affect situations outside the one at issue and are in violation of the void for vagueness and overbreadth doctrines).

[402] *See supra* notes 147–148 (describing how the *mens rea* requirements vary within subsections of the CFAA).

[403] *See supra* notes 148, 237–238 and accompanying text (applying the canon of consistency to eliminate a proposed broad interpretation of the CFAA; deciding instead to narrowly interpret "exceeds authorized access" to stay in compliance with the canon of consistency).

[404] *See supra* notes 148, 237–238 and accompanying text (applying the canon of consistency to eliminate a proposed broad interpretation of the CFAA; deciding instead to narrowly interpret "exceeds authorized access" to stay in compliance with the canon of consistency).

[405] *See supra* notes 82, 237–238 (finding § 1030(a)(2)(C) to be the broadest subsection of the CFAA because it does not require any intent beyond intentionally "exceed[ing] authorized access" to view information on a computer).

from a protected computer translates into viewing any information on any computer, the court correctly surmised that adopting the government's definition would impermissibly "transform whole categories of otherwise innocuous behavior into federal crimes simply because a computer is involved."[406]

Broad interpretations of the CFAA cannot be applied consistently without triggering constitutional concerns.[407] Criminal statutes require due process and applying restrictive, consistent, definitions to the CFAA is the only way to ensure the statute is constitutional.[408] In order to consistently define "without authorization" and "exceeds authorized access" in civil and criminal contexts and across subsections, a narrow interpretation of the CFAA is required.[409]

D. Broad Interpretations Defeat the Intended Scope of the CFAA

Broad views mistakenly cite to the CFAA's expansive amendments as proof that the statute was meant to apply widely.[410] Broad views contend that narrow interpretations ignore the consistent amendments that Congress has enacted to broaden its application.[411] This argument misinterprets the statute's amendments and overlooks the subject of the CFAA.[412] While the CFAA has undoubtedly broadened in scope, these expansions reflect Congress's effort to keep the CFAA relevant in the face of quickly evolving technology; they are not an effort to subsume existing state laws.[413]

Congress knew even before 1984 that attempting to combat computer crime with one statute would be an ongoing effort and one likely to involve frequent amendments.[414] The widely-criticized original version was so narrowly drawn that it proved unusable.[415] Although the first round of

[406] *See supra* note 236 (explaining that the government's proposed broad definition of "exceeds authorized access" under the fraud section would make any violation of a private agreement subject to criminal liability under the CFAA).

[407] *See supra* note 237 (outlining various ways that a broad interpretation of the CFAA raises constitutional concerns).

[408] *See supra* note 228 (interpreting the CFAA narrowly results in consistent definitions that meet the due process demanded from all criminal statutes).

[409] *See supra* note 228 (interpreting the CFAA narrowly results in consistent definitions that meet the due process demanded from all criminal statutes).

[410] *See supra* note 176 and accompanying text (defending a broad interpretation of the CFAA due to its expansive amendments).

[411] *See supra* note 176 and accompanying text (defending a broad interpretation of the CFAA due to its expansive amendments).

[412] *See supra* notes 47, 81 (describing the purpose of the CFAA as one to combat new types of computer crimes).

[413] *See supra* note 81 (admitting that frequent amendments might be necessary in order to keep the CFAA relevant).

[414] *See supra* note 81 (admitting that frequent amendments might be necessary in order to keep the CFAA relevant).

[415] *See supra* notes 51–52 and accompanying text (describing the difficulties encountered in the original statute).

amendments in 1986 was expansive, it was entirely remedial and necessary to reset the CFAA's bounds in order for the statute to achieve its designed purpose.[416] Expansive amendments were necessary to protect confidential information in public and private sector computers and to make it an effective tool against computer crime which is interstate in nature.[417] Yet, throughout all of the technical changes implemented over the years, Congress has never once altered the CFAA's purpose or narrow scope.[418] The amendments only expand the CFAA's application in order to keep it relevant and applicable to new types of computer crimes, not to override existing statutes.[419]

Congress deliberately did not preempt the field of computer crime when the CFAA was originally enacted, and it continues to amend the statute without exercising its preemption power.[420] Not exercising its preemption power is evidence of Congressional intent to preserve the narrow scope of the CFAA.[421] Even the most expansive amendments came with estimates from the Departments of Justice and Treasury stating that the changes would not result in any significant cost to the federal government.[422] If Congress meant for the vigorous application of the CFAA in employment contexts, the estimates of costs incurred would not be negligible.[423] Congress has not wavered from its original intent to limit the CFAA to crimes involving a compelling federal interest.[424] Broad views fail to recognize that even capturing just one federally compelling computer criminal would still require an extremely broad reach.[425]

[416] *See supra* Part II.C (amending the CFAA was necessary to make it an effective tool to combat computer crimes).

[417] *See supra* note 52 (expanding the CFAA's scope to protect more financial information).

[418] *See supra* Part II.C (amending the CFAA was necessary to make it an effective tool to combat computer crimes).

[419] *See supra* Part II.C (amending the CFAA was necessary to make it an effective tool to combat computer crimes).

[420] *See supra* notes 128–129 and accompanying text (demanding that if Congress intends to preempt or drastically alter the federal-state balance, it must speak clearly).

[421] *See supra* notes 128–129 and accompanying text (presuming that Congress meant to preserve the federal-state balance by not including a clear preemption provision in the CFAA).

[422] *See supra* note 81 (noting that Congress did not expect the introduction of the civil provision to incur any significant costs to state or federal government).

[423] *See supra* notes 29–30 (noting the surge in number of claims after the civil provision was introduced).

[424] *See supra* note 70 (limiting the scope of the CFAA to crimes involving a compelling federal interest).

[425] *See supra* notes 77–79 and accompanying text (noting the interstate nature of computer crimes).

The expansive reach of the Commerce Clause is necessary to effectively combat the insidious, interstate nature of computer crime.[426] An expansive definition for "protected computer" reflects technological advances that have rendered even the smallest devices capable of storing large amounts of data.[427] The civil provision was added to boost the deterrent value of the statute and to allow private companies to recover for purposeful damages.[428] Despite all of the expansions, the narrative woven throughout the legislative history is one of concern for potential damage to the nation's financial, educational, and scientific information at the hands of malicious hackers or insidious viruses.[429] Nowhere are those same concerns echoed for employees who misappropriate data.[430] Despite mountains of legislative history to the contrary, broad interpretations continue to inaccurately equate the inclusion of the Commerce Clause in the CFAA with a green light for an expansive scope.[431]

Broad interpretations capture employee behavior that Congress intended to keep outside the CFAA's reach by welcoming disgruntled employer claims.[432] Although insiders have firmly been in the CFAA's range since its inception, Congress took steps to ensure that even objectionable authorized employee actions would not be prosecuted under the CFAA unless clearly criminal.[433] Recognizing the potential gray-area for employees with access to company computers, Congress raised the *mens rea* in an early amendment to eliminate accidental access from the statute's reach.[434] Further, senate reports caution that employees who briefly exceed their access should be subject to administrative rather than criminal proceedings.[435]

[426] *See supra* notes 47, 78 (describing the purpose of the CFAA was to effectively combat serious computer misuse crimes and acknowledging those were mainly interstate in nature).

[427] *See supra* notes 77–80 and accompanying text (noting the interstate nature of computer crimes and always-evolving technology).

[428] *See supra* text accompanying notes 71–74 (explaining why the civil provision was added to the CFAA).

[429] *See supra* notes 34–36 (discussing the types of computer crime targeted by the CFAA).

[430] *See supra* notes 57–62 and accompanying text (attempting to eliminate misbehaving employees from the CFAA's scope unless the behavior was clearly criminal).

[431] *See supra* Parts II.C, II.E (justifying the expansive amendments as necessary in order to keep the CFAA effective as a tool to combat compelling federal interest crimes of serious compute misuse).

[432] *See supra* note 49 (describing the difference in types of computer crimes).

[433] *See supra* notes 65–67 and accompanying text (stating a preference for administrative sanctions for employee misconduct instead of prosecution under the CFAA).

[434] *See supra* notes 65–67 and accompanying text (eliminating insider liability for accidental access).

[435] *See supra* note 67 (deciding employees who briefly exceeded authorized use should be subject to administrative sanctions rather than punished under the CFAA, especially in situations where the computer is not clearly delineated to communicate which access is prohibited).

Congress meant to exclude the behavior now openly litigated under agency and contract-based interpretations of the CFAA by taking steps to avoid situations where employees could face liability for slight unauthorized use.[436] Broad interpretations allow liability to hang from even slight or unknowing employee missteps if contrary to an employer's interest or in breach of a company policy.[437] A brief lapse in diligence under an agency interpretation or a slight breach of company policy under a contract interpretation and an employer can haul an employee to federal court in jurisdictions adopting broad views.[438] The inherent uncertainties in these broad, subjective views create the exact situation Congress did not want the statute to cover.[439] Accordingly, broad, subjective views are not correct interpretations of the CFAA.[440]

Broad views also demolish the purpose of the CFAA by misunderstanding the type of crime targeted by the statute and adjudicating claims far outside the intended scope.[441] A proper claim under the CFAA features behavior that is criminal *because* it misuses a computer whereas broad interpretations allow claims in which the computer merely facilitates a traditional crime.[442] Jurisdictions using a broad interpretation incorrectly allow employers to haul employees into court for traditional state law crimes labeled as a CFAA claim due to the incidental involvement of a computer.[443] Emailing, downloading, or otherwise copying information to use in competition with an employer is not the new, emerging computer crime the CFAA was created to combat.[444] The new, emerging type of crime that the

[436] *See supra* note 67 (deciding employees who briefly exceeded authorized use should be subject to administrative sanctions rather than punished under the CFAA, especially in situations where the computer is not clearly delineated to communicate which access is prohibited).

[437] *See supra* notes 152–154 and accompanying text (describing liability under broad interpretations).

[438] *See supra* notes 152–154 and accompanying text (describing liability under broad interpretations).

[439] *See supra* note 67 (deciding employees who briefly exceeded authorized use should be subject to administrative sanctions rather than punished under the CFAA, especially in situations where the computer is not clearly delineated to communicate which access is prohibited).

[440] *See supra* note 67 (deciding employees who briefly exceeded authorized use should be subject to administrative sanctions rather than punished under the CFAA, especially in situations where the computer is not clearly delineated to communicate which access is prohibited).

[441] *See supra* Part II.A**,** text accompanying note 172 (comparing the type of crime targeted under the CFAA with a broad interpretation's holding of liability in misappropriation claim).

[442] *See supra* Part II.A and accompanying text (describing the different types of computer crimes).

[443] *See supra* note 237 (correctly dismissing a CFAA claim that should have been filed in a state court).

[444] *See supra* notes 36–47 (comparing actual crimes targeted by the CFAA to traditional crimes already adequately covered by state laws addressing employee misconduct).

CFAA was created to combat includes hacking, spreading viruses, and intentionally incapacitating or compromising the functionality of a computer.[445] Misappropriation, unfair competition, tortious interference, and breach of contract actions all existed well before the advent of computers and remain actionable regardless of any computer involvement.[446] Broad interpretations allow claims that predate computers and misinterpret the level of computer involvement needed to trigger a CFAA claim.[447] Broad interpretations are wrong because these are not the crimes Congress intended for the CFAA.[448]

Broad views horrendously abuse the CFAA by penalizing a wide swath of less-than-criminal behavior and adjudicating incorrect types of crimes under a computer misuse statute targeted primarily at compelling federal interest crimes.[449] Simply by sticking to an objective analysis and the statutory language, narrow interpretations correctly dismiss these employment cases, allowing focus and resources to remain trained on the real target of the CFAA: crimes of computer misuse.[450] Even though narrow interpretations require dismissing the kind of misappropriation claims typically seen in agency or contract-based interpretations, employers are not left without redress.[451] Employers are simply forced to re-file in state court, or back in federal court basing jurisdiction on complete diversity, where the claims should have initially been filed.[452] Broad interpretations are clearly incorrect applications of the CFAA because they hijack federal judicial resources and undermine traditional state powers by adjudicating inappropriate claims.[453]

[445] *See supra* notes 41–47 and accompanying text (creating the CFAA in order to effectively prosecute computer crimes that were not susceptible to prosecution under traditional, existing criminal statutes).

[446] *See supra* notes 36–47 and accompanying text (comparing crimes targeted by the CFAA and crimes traditionally governed by states).

[447] *See supra* notes 36–47 and accompanying text (comparing crimes targeted by the CFAA and crimes traditionally governed by states).

[448] *See supra* notes 41–47 and accompanying text (creating the CFAA in order to effectively prosecute computer crimes that were not susceptible to prosecution under traditional, existing criminal statutes).

[449] *See supra* notes 234–235 and accompanying text (interpreting the CFAA narrowly in order to avoid criminalizing a wide range of innocent activity).

[450] *See supra* notes 239–242 and accompanying text (describing a narrow interpretation of the CFAA).

[451] *See supra* notes 239–242 and accompanying text (describing that breaching an employment agreement premised on misuse was an inappropriate CFAA claim since the defendant was authorized to access the computer and that appropriate state law remedies were still available).

[452] *See supra* notes 239–242 and accompanying text (describing that breaching an employment agreement premised on misuse was an inappropriate CFAA claim since the defendant was authorized to access the computer and that appropriate state law remedies were still available).

[453] *See supra* text accompanying note 235 (interpreting the CFAA narrowly in order to avoid criminalizing a wide range of innocent activity).

E. Broad Interpretations of the CFAA Evoke Federalism Concerns

Broad interpretations far surpass the CFAA's intended gap-filling function by displacing large expanses of state laws.[454] Without clear congressional intent, courts should not interpret statutes in a way that tremendously shifts the federal-state balance.[455] Yet that is exactly what courts broadly interpreting the CFAA do.[456] Broad interpretations allow employers to create federal jurisdiction for any dispute involving a computer.[457] Computers play increasingly prominent roles in society; if all it takes to transpose an existing state action into a CFAA claim is the involvement of a computer, a majority of state claims could soon be extinct.[458] Broad interpretations transform the CFAA into a universal federal cause of action by allowing employers to completely bypass a wide berth of state laws.[459] This is an incorrect application of the CFAA because Congress sought to balance the statute against existing remedies, not to completely displace them. [460]

Not only do broad interpretations of the CFAA usurp traditional state powers, they disturb carefully constructed policy preferences and undermine substantive law.[461] For example, states' policy-driven trade secret statutes become meaningless when employers can label the same action a CFAA claim and circumvent carefully constructed evidentiary burdens.[462] Broad interpretations allow employers to enlist the CFAA to protect information that state trade secret law does not protect.[463] This undermines deliberate

[454] *See supra* text accompanying note 47 (describing the CFAA's role as a gap-filler to be used when prosecution under existing statutes would be difficult due to computer technology).

[455] *See supra* notes 128–129 and accompanying text (requiring clear congressional intent before a court's interpretation of a statute alters established policy preferences).

[456] *See supra* notes 128–129 and accompanying text (requiring clear congressional intent before a court's interpretation of a statute alters established policy preferences).

[457] *See supra* note 172 and accompanying text (broadly interpreting the CFAA to allow traditional state law claims like misappropriation, breach of contract, and theft of trade secrets to be litigated in federal court).

[458] *See supra* note 172 and accompanying text (broadly interpreting the CFAA to allow traditional state law claims like misappropriation, breach of contract, and theft of trade secrets to be litigated in federal court).

[459] *See supra* note 237 (interpreting the CFAA broadly allows an otherwise state law claim access to federal court if a computer is involved).

[460] *See supra* Part II.D (detailing the intended scope of the CFAA).

[461] *See supra* notes 90–94 and accompanying text (comparing the higher evidentiary standards typically found in state trade secret statutes to a CFAA claim).

[462] *See supra* notes 90–94 and accompanying text (comparing the higher evidentiary standards typically found in state trade secret statutes to a CFAA claim).

[463] *See supra* notes 90–94 and accompanying text (comparing the higher evidentiary standards typically found in state trade secret statutes to a CFAA claim).

policy goals and encourages employers to avoid seeking redress in state courts.[464]

If Congress meant for federal law to provide redress for misappropriation claims, it would have provided a civil cause of action in the Economic Espionage Act (EEA) enacted in 1996.[465] Congress's incorporation of traditional trade secret law requirements into the federal Act suggests an appreciation and support for the policies driving trade secret law and a desire to maintain traditional requirements.[466] Not providing a private cause of action suggests Congress affirmatively intended to not interfere with or displace traditional state trade secret law.[467] Moreover, it is evident that the appropriate scope of the CFAA does not include these claims because Congress does not enact duplicative statutes and the EEA covers misappropriation claims.[468]

Courts narrowly interpreting the CFAA correctly deduce that absent explicit congressional intent, the CFAA should not displace substantial portions of state law.[469] These courts do not say misbehaving employees are never liable, just that they are not liable under the CFAA unless they abuse access privileges.[470] Courts using a narrow interpretation recognize the CFAA's intended scope and respectfully decline jurisdiction over claims that fall outside of it.[471] A narrow interpretation of the CFAA is the only way to ensure that the statute does not eclipse large portions of state law.[472]

VI. CONCLUSION

The CFAA is a criminal statute intended to target new forms of computer crimes when no other state or federal statutes apply.[473] Its function as an effective deterrent to internal and external hacking depends on its constitutionality and consistent application. Under broad interpretations, the

[464] *See supra* notes 90–94 and accompanying text (comparing the higher evidentiary standards typically found in state trade secret statutes to a CFAA claim).

[465] *See supra* note 90 (implementing the EEA in 1996 but providing no private cause of action).

[466] *See supra* note 90 (implementing the EEA in 1996 but providing no private cause of action).

[467] *See supra* note 90 (implementing the EEA in 1996 but providing no private cause of action).

[468] *See supra* note 144 and accompanying text (explaining if another statute would apply, the one at issue should not).

[469] *See supra* notes 127–129 and accompanying text (presuming Congress acts interstitially and will not displace existing law without explicit intent).

[470] *See supra* notes 234–236 and accompanying text (arguing a broad interpretation of the CFAA would displace large amounts of existing state law).

[471] *See supra* notes 234–236 and accompanying text (arguing a broad interpretation of the CFAA would displace large amounts of existing state law).

[472] *See supra* notes 234–236 and accompanying text (arguing a broad interpretation of the CFAA would displace large amounts of existing state law).

[473] *See supra* Part II (detailing the legislative purpose of the CFAA).

CFAA's fairly narrow purpose is distorted beyond recognition until it is stripped of its intended function and its constitutionality.[474] A narrow interpretation of the CFAA is the only way the statute remains constitutional.[475]

A narrow interpretation correctly prioritizes plain language and the rule of lenity over reading agency or contract law into definitions.[476] Following these canons of construction, a narrow interpretation of the CFAA provides the predictability and notice that due process requires and that broad interpretations lack.[477] Utilizing canons of constructions and abiding by established doctrines, a narrow interpretation effectuates Congressional intent and avoids the harmful implications of broad interpretations like criminalizing innocent behavior and displacing state laws. Until the Supreme Court or Congress step in, courts must interpret the CFAA constitutionally and in line with Congressional intent. The plethora of issues surrounding broad interpretations makes a narrow interpretation of the CFAA the only correct choice.

[474] *See infra* Part V (explaining why broad interpretations of the CFAA are unconstitutionally vague and overbroad; how broad interpretations fail to effectuate Congressional intent and incorrectly trample existing state laws).

[475] *See infra* Part V.A–B (arguing that a narrow interpretation of the CFAA remains constitutional by meeting due process requirements and limiting the statute's scope to only cover punishable conduct).

[476] *See infra* Part V.C (arguing that only a narrow interpretation follows established canons of construction and, in doing so, is able to accomplish Congress's intended purpose).

[477] *See infra* Part V.A–B (arguing that a narrow interpretation of the CFAA remains constitutional by meeting due process requirements and limiting the statute's scope to only cover punishable conduct).