2012

Ambiguity Killed the CFAA

Prakash S. Patel
Seton Hall Law

Ambiguity Killed the CFAA

Prakash S. Patel

The Computer Fraud and Abuse Act (hereinafter "CFAA") was originally enacted in 1984 to impose criminal penalties on hackers who attacked vulnerable computer systems by uploading threatening programs such as logic bombs, trapdoors, Trojan horses, viruses and worms. [1] The original 1984 law was criticized because it was narrowly tailored to cover only government computers and those involved in the operation of financial institutions. [2] As a result, Congress amended the language contained in the CFAA to also include non-government computers if they fall into the category of "protected computer[s]."[3] A "protected computer" is defined as any computer:

> exclusively for the use of a financial institution or the United States Government, or, in the case of a computer not exclusively for such use, used by or for a financial institution or the United States Government and the conduct constituting the offense affects that use by or for the financial institution or the Government; or which is used in or *affecting interstate or foreign commerce or communication*, including a computer located outside the United States that is used in a manner that affects interstate or foreign commerce or communication of the United States.[4]

Since the Internet is frequently used in interstate and foreign commerce, any computer or other electronic devices connected to the Internet become a "protected computer" under the amended CFAA definition.[5] Home computers that are solely used to watch videos and simple emailing, however, may not be considered "protected computers" since those activities are not used in

---

[1] 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, 160 (2008).
[2] Mary M. Calkins, *They Shoot Trojan Horses, Don't They? An Economic Analysis of Anti-Hacking Regulatory Models*, 89 Geo. L. J. 171, 179 (2000).
[3] Id. at 180.
[4] 18 U.S.C.S 1030 §§ 1030(e)(2)(A)-(B)(emphasis added).
[5] Liccardi, *supra* note 1, at 160.

interstate commerce. Employers have taken advantage of this significant change by bringing civil actions against disloyal employees who obtained confidential data from their computer systems.[6] In these situations, the CFAA is not the only weapon in an employer's arsenal since they may also bring a traditional trade secret claim under state law or the Federal statute. [7] Nevertheless, the CFAA is proving to be increasingly popular because the employer only needs to show that the employee accessed a computer system without or in excess of authorization and do not require that the employee actually obtained any information.[8] Part I of this article will give a short background on traditional state trade secret law to elicit why the CFAA is the preferred route for most litigants. Part II of this article analyzes the benefits and limitations of the CFAA in the context of civil claims and how it has been applied to classic employee misappropriation cases. Additionally, Part II analyzes CFAA issues in more recent cases involving social network site—MySpace. Finally, Part III discusses a consistent way courts can resolve the ambiguity in the CFAA.

I. Traditional State Trade Secret Law

Today, nearly all the states in the United States have laws that protect trade secrets.[9] Most states have adopted the Uniform Trade Secrets Act ("UTSA") as the basis for trade secret misappropriation causes of action.[10] However, many states have also adopted trade secret laws from the Restatement (First) of Torts as well as the Restatement (Third) of Unfair Competition. The UTSA and the Restatements both provide a definition of trade secret that is

---

[6] Thomas E. Booms, *Hacking into Federal Court: Employee "Authorization" Under the Computer Fraud and Abuse Act*, 13 Vand. J. Ent. & Tech. L. 543, 550 (2011).
[7] Liccardi, *supra* note 1, at 158.
[8] Id. at 157.
[9] ROBERT P. MERGES, PETER S. MENELL, & MARK A. LEMLEY, INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE 35 (Rev. 4th ed. 2007).
[10] UNIF. TRADE SECRETS ACT §§ 1-12 (amended 1985), 14 U.L.A. 537-659 (2005); 14 U.L.A. 18-19 (Supp. 2008) (listing the forty-seven jurisdictions that have adopted the UTSA).

essentially the same: a trade secret is information used in a party's business that derives economic value from its secrecy.[11] Whether information constitutes a trade secret is, in some states, a question of fact for the jury to decide.[12] In other states the question of whether the plaintiff's information constitutes a trade secret is a mixed question of law and fact.[13]

A plaintiff must prove three essential elements in a state trade secret misappropriation claim.[14] First, the plaintiff must show the information qualifies as a "trade secret" under the relevant state's definition of a trade secret.[15] Second, the plaintiff must show he made a reasonable effort to preserve the secrecy of the information.[16] Third, the plaintiff must show the defendant procured the trade secret through unlawful means.[17]

In order for the plaintiff to prevail on the first element he must demonstrate that the information qualifies as a trade secret by showing it meets the state's definition of a trade secret. UTSA defines a trade secret as information including "a formula, pattern, compilation, program, device, method, technique or process, that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use, and that is

---

[11] See UNIF. TRADE SECRETS ACT § 1(4)(i)-(ii) (amended 1985), 14 U.L.A. 538 (2005) ("'Trade Secret' means information…that derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons...."); RESTATEMENT (THIRD) OF UNFAIR COMPETITION §39 ("A trade secret is any information…that is sufficiently valuable and secret to afford an actual or potential economic advantage over others."); RESTATEMENT (FIRST) OF TORTS §757 cmt. b ("A trade secret may consist of…information which is used in one's business, and which gives him an opportunity to obtain an advantage over competitors who do not know or use it.").

[12] See Penalty Kick Management Ltd. V. Coca Cola Co., 318 F.3d 1284 (11th Cir. 2003); United Group of Nat. Paper Distributors, Inc. v. Vinson, 666 So. 2d 1338 (La. Ct. App. 2d Cir. 1996), writ denied, 679 So. 2d 1358 (La. 1996).

[13] See S & W Agency, Inc. v. Foremost Ins. Co., 51 F. Supp. 2d 959 (N.D. Iowa 1998); APAC Teleservices, Inc. v. McRae, 985 F. Supp. 852 (N.D. Iowa 1997); Mediacom Iowa, L.L.C. v. Incorporated City of Spencer, 682 N.W.2d 62 (Iowa 2004).

[14] MERGES, MENELL & LEMLEY, *supra* note 9, at 37.

[15] Id.

[16] Id.

[17] Id.

the subject of efforts that are reasonable under the circumstances to maintain its secrecy."[18] In a state that follows the UTSA, the plaintiff must satisfy *all* the elements of the UTSA test. The Restatement (First) of Torts lists several factors that courts may consider when determining whether a plaintiff's information is protectable as a trade secret.[19] Those factors are:

> (1) the extent to which the information is known outside of [the plaintiff's] business; (2) the extent to which it is known by employees and others involved in [the plaintiff's] business; (3) the extent of measures taken by [the plaintiff] to guard the secrecy of the information; (4) the value of the information to [the plaintiff's business] and to [the plaintiff's] competitors; (5) the amount of effort or money expended by [the plaintiff] in developing the information; (6) the ease or difficulty with which the information could be properly acquired or duplicated by others.[20]

None of these factors are outcome determinative and instead they are common law factors that are instructive guidelines to help courts determine whether a trade secret exists under state law.[21] Thus, the Restatement offers a more indeterminate balancing test whereas the UTSA offers more prescriptive requirements.

Both the UTSA and the Restatement (First) of Torts also require the plaintiff to have made reasonable efforts to maintain the secrecy of the information deemed to be a trade secret.[22] What constitutes "reasonable efforts" to maintain secrecy varies depending on the circumstance, the size of the company, and its economic resources.[23]

After proving the first two elements, the last element requires the plaintiff to show that the defendant misappropriated the trade secret in an unlawful or wrongful way.

---

[18] UNIF. TRADE SECRETS ACT § 1(4)(i) (amended 1985), 14 U.L.A. 538 (2005).
[19] RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939).
[20] RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939); See also Weigh Systems South, Inc. v. Mark's Scales & Equipment, Inc., 68 S.W.3d 299 (Ark. 2002).
[21] E.g., Learning Curve Toys, Inc. v. Playwood Toys, Inc., 342 F.3d 714, 722 (7th Cir. 2003).
[22] UNIF. TRADE SECRETS ACT § 1(4)(ii) (amended 1985), 14 U.L.A. 538 (2005); RESTATEMENT (FIRST) OF TORTS § 757 cmt. b (1939) (including "the extent of measures taken by [the plaintiff] to guard the secrecy of the information" among the six factors used to determine whether information is a trade secret).
[23] See, e.g., Rockwell Graphic Sys., Inc. v. DEV Indus., Inc. 925 F.2d 174 (7th Cir. 1991) (defining the meaning of reasonable efforts to maintain secrecy based on an economic analysis); Elmer Miller, Inc. v. Landis, 625 N.E.2d 338, 342 (Ill. App. Ct. 1993) (stating that reasonable efforts to maintain secrecy are different for a small entity than they are for a larger entity).

Pursuing a claim under traditional state trade secret claims is not an easy endeavor. Trade secret claims may be denied when plaintiff fails to establish that the information was indeed a "trade secret" in contemplation of the law. Furthermore, trade secret claims may be dismissed on the basis for failure to preserve the secrecy of the information. Therefore, many plaintiffs prefer to sue in Federal court under the CFAA because it lowers the burdens of pleading and proof compared to state trade secret laws.[24]

II. The Very Poorly Drafted Federal Statute: The CFAA

Congress originally intended the CFAA would be exclusively a criminal statute in order to protect confidential information stored on computers belonging to the United States government and financial institutions.[25] In 1994, however, Congress amended the CFAA to add a civil remedy to compensate for the monetary damage caused by criminal violations.[26]

The CFAA's civil remedy offers corporations and small businesses significant benefits against disloyal employees. First, the CFAA allows federal courts to hear cases under federal question jurisdiction without having employers to show the parties' diversity of citizenship.[27] Federal court is preferred for more complex trade secret litigation because it provides procedural benefits such as nationwide service of process.[28] This procedural benefit cannot be downplayed because often in complex trade secret litigation the plaintiff resides in one state, the defendant resides in a different state, and both the evidence of trade secret theft and key witnesses are in different states around the country. Litigating this complex type of case in state court might require filing motions and proceedings in multiple jurisdictions throughout the country in order

[24] Elizabeth A. Cordello, Commentary: Split Over Unauthorized Use Remains, Daily Rec. (Rochester, N.Y.), Nov. 16, 2009, available at 2009 WLNR 23220555 ("Aside from obtaining federal jurisdiction, the CFAA also is an attractive means to pursue former employees in non-compete or trade secret litigation because employers do not have to show the existence of an employment agreement, or that the disputed information is confidential.").
[25] Id. at 160.
[26] Id.
[27] Id. at 156.
[28] Id.

to depose key witnesses and obtain relevant evidence.[29] Nationwide service of process avoids this entire situation and saves substantial amounts of time.[30] Second, once in federal court, litigants may attach one or more state law claims for trade secret misappropriation under the federal courts supplemental jurisdiction.[31] Third, the pleading standards under the CFAA are much easier to meet then those of state trade secret claims.[32] Under state law, a plaintiff must prove that the misappropriated information constitutes a "trade secret".[33] While this may not be a significant hurdle in most instances, there is no such requirement under the CFAA, where the plaintiff must simply prove that the accessed information resided on a "protected computer". The last and most distinct advantage of the CFAA is that it protects *all* intangible computer data regardless of whether it is proven a trade secret under state law.[34]

While trade secret litigation can be very complex so can understanding the provisions of the CFAA. Under the current version of the statute, an *insider* of the company such as an employee or *outsider* such as a hacker may be civilly liable if he "knowingly causes the transmission of a program, information, code, or command, and as a result such conduct, intentionally causes damage without authorization, to a protected computer," or if an outsider "intentionally accesses a protected computer without authorization," and as a result, "recklessly causes damage" or negligently "causes damage."[35]

---

[29] See Roy E. Hofer & Susan F. Gullotti, *Presenting the Trade Secret Owner's Case in Protecting Trade Secrets* 1985, at 145, 160-61 (PLI patents, Copyrights, Trademarks, & Literary Prop., Course Handbook Series No. 196, 1985), *available at* WL, 196 PLI/Pat 145.
[30] Id.
[31] Liccardi, *supra* note 1, at 157.
[32] Id. at 156.
[33] See generally, Rockwell Graphic Sys., v. Dev Indus., Inc., 925 F.2d 174 (7th Cir. 1991).
[34] Id.
[35] Calkins, *supra* note 2, at 160.

The CFAA provides corporations and small businesses six civil causes of action against insiders or outsiders who misappropriate confidential information. A insider or outsider may be civilly liable if he or she:

1. "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information contained in a financial record of a financial institution…,"[36] or
2. "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains information from any protected computer,"[37] or
3. "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access, and by means of such conduct furthers the intended fraud and obtains anything of value, unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period;"[38] or
4. "knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer;"[39] or
5. "intentionally accesses a protected computer without authorization, and as a result of such conduct, recklessly causes damage;"[40] or
6. "intentionally accesses a protected computer without authorization, and as a result of such conduct causes damage and loss."[41]

The CFAA provides civil relief in the form of compensatory damages or injunctive relief to any person who suffers damage or loss.[42] In order to get civil relief, a litigant must satisfy a two part test. First, the party must prove there is a violation of the CFAA giving rise to one of

[36] Id. § 1030(a)(2)(A).
[37] Id. § 1030(a)(2)(C).
[38] Id. § 1030(a)(4).
[39] Id. § 1030(a)(5)(A).
[40] Id. § 1030(a)(5)(B).
[41] Id. § 1030(a)(5)(C).
[42] Id. § 1030(g).

the six causes of action enumerated in the statute resulting in damage or loss.[43] Second, the violation must involve at least one of the following aggravating factors, which includes:

I. loss to 1 or more persons during any 1-year period (and, for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting from a related course of conduct affecting 1 or more other protected computers) aggregating at least $5,000 in value;[44] or

II. the modification or impairment, or potential modification or impairment, of the medical examination, diagnosis, treatment, or care of 1 or more individuals;[45] or

III. physical injury to any person;[46] or

IV. a threat to public health or safety;[47] or

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;[48] or

VI. damage affecting 10 or more protected computers during any 1-year period.[49]

Notwithstanding the convoluted nature of the CFAA's provisions, it is proving to be a powerful weapon for the protection of electronic data stored on computers and cell phones.[50] Despite some clear advantage to state trade secret law, courts are sharply divided whether to interpret the CFAA provisions and key terms broadly or narrowly. The scope and demeanor of this interpretation, moreover, is both outcome determinative of the breadth and application of the CFAA.

---

[43] Liccardi, *supra* note 1, at 162.
[44] Id. § 1030(c)(4)(A)(i)(I).
[45] Id. § 1030(c)(4)(A)(i)(II).
[46] Id. § 1030(c)(4)(A)(i)(III).
[47] Id. § 1030(c)(4)(A)(i)(IV).
[48] Id. § 1030(c)(4)(A)(i)(V).
[49] Id. § 1030(c)(4)(A)(i)(VI).
[50] Liccardi, *supra* note 1, at 162.

III. The Broad, Narrow, and Contract-Based Approaches in Interpreting "Authorization"

The focal point of many federal court decisions are on the terms "without authorization" and "exceeds authorized access."[51] Federal courts are currently split in determining whether to apply a broad view, narrow view, or a contract-based approach to these two terms.[52] The broad view rests on principles of agency law.[53] It asserts that when an employee has authorization but then misuses or steals confidential computer data, he acts contrary to his employer's interest and therefore loses authorization.[54] The narrow view can be characterized as an objective approach.[55] It reasons that an employee who is given permission to access an employer's computer retains that permission even if the employee misappropriates company data thereafter. [56] Courts have also adopted the contract-based approach that relies on the existent of an explicit or implied contract that defines the user's authorization.[57] This latter approach is useful in situations where there is an express contract, such as between an employer and an employee, or between a website user and the website's operating terms of service agreements outlining what is and is not authorized.[58]

A. Review of the Broad View and its Criticisms

The seminal case *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*,[59] was the first to expressly adopt the broad interpretation of the CFAA. In *Shurgard*, both the plaintiff

---

[51] Booms, *supra* note 6, at 551.
[52] Id.
[53] Id.
[54] Id.
[55] Id. at 552.
[56] Id.
[57] *See generally* Southwest Airlines Co. v. Farechase, Inc., 318 F. Supp 2d 435, 439-40 (N.D. Tex. 2004); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 247-51 (S.D.N.Y. 2000), *aff'd*, 356 F.3d 393 (2d Cir. 2004).
[58] Id.
[59] 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

and defendant were direct competitors in the self-storage business.[60] Plaintiff alleged that the defendant was hiring away key employees to obtain the plaintiff's trade secrets.[61] The defendant offered a job to Eric Leland, a manager for Shurguard, and before officially leaving Shurgard's employment, Mr. Leland sent emails to the defendant regarding trade secrets and confidential information belonging to the plaintiff.[62] The plaintiff sued under various provisions of the CFAA, including § 1030(a)(2)(C), which prohibits "intentionally access[ing] a computer without authorization or exceed[ing] authorized access, and thereby obtain[ing]…information from any protected computer."[63] The defendant sought a motion to dismiss on the grounds that the plaintiff did not allege that Mr. Leland accessed the information without authorization.[64] The district court adopted the plaintiff's agency theory, relying upon the Second Restatement of Agency, which essentially states "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."[65] The court held that even though Mr. Leland was initially authorized, he lost that authorization when he allegedly obtained and sent the proprietary information to the defendant via e-mail.[66] The Shurgard court's agency approach interpreting the term "authorization" quickly spread to other district courts.[67]

Judge Posner in the Seventh Circuit solidified *Shurgard's* agency theory by adopting it in the case *International Airport Centers, L.L.C. v. Citrin*.[68] In *Citrin*, the defendant was an

---

[60] Id.
[61] Id.
[62] Id. at 1123.
[63] Id. § 1030(a)(2)(C).
[64] Shurgard, F. Supp. 2d at 1124.
[65] Id. at 1125 (quoting RESTATEMENT (SECOND) OF AGENCY § 112 (1958)).
[66] Id.
[67] *See, e.g.*, George S. May Int'l Co. v. Hostetler, No. 04 C 1606, 2004 WL 1197395, at *3 (N.D. Ill. May 28, 2004); HUB Grp., Inc. v. Clancy, No. Civ. A. 05-2046, 2006 WL 208684, at *3 (E.D. Pa. Jan. 25, 2006); Int'l Sec. Mgmt. Grp., Inc. v. Sawyer, No. 3:06CV0456, 2006 WL 1638537, at *20-21 (M.D. Tenn. June 6, 2006).
[68] 440 F.3d 418 (7th Cir. 2006).

employee of International Airport Centers ("IAC") who decided to leave the company to go into work for himself.[69] IAC had given the defendant a company laptop for work.[70] Prior to leaving IAC, the defendant installed a "secure-erasure" program on the company laptop and deleted all of the data belonging to IAC for which there were no duplicates.[71] Judge Posner relied on agency principles and cited *Shurgard* as authority to reverse the district court's dismissal of the action under the CFAA.[72] Judge Posner held that since the defendant "resolved to destroy files that incriminated himself and other files that were also the property of [IAC] his employer, in violation of the duty of loyalty that agency law imposes," his authorization to use the company laptop had terminated and he was in violation of the CFAA.[73]

A central problem with the expansive interpretation of the term authorization in the civil context is that it has also expanded interpretation of other terms in the CFAA that would also broaden criminal liability for defendants.[74] For example, in *Citrin*, a central issue was whether the defendant "knowingly cause[d] the *transmission* of a program, information, code, or command, and as a result of such conduct, intentionally caused damage without authorization, to a protected computer.[75] The defendant argued that simply erasing a file from a computer is not a "transmission."[76] Judge Posner agreed in dicta by stating "[p]ressing a delete or erase key in fact transmits a command, but it might be stretching the statute too far (especially since it provides criminal as well as civil sanctions for its violation) to consider any typing on a computer

[69] Id. at 419.
[70] Id.
[71] Id.
[72] Id. at 420.
[73] Id. at 420.
[74] Warren Thomas, *Lenity on me: LVRC Holdings LLC v. Brekka Points the Way Toward Defining Authorization and Solving the Split Over the Computer Fraud and Abuse Act*, 27 Ga. St. U. L. Rev. 379, 380-81 (2011).
[75] Citrin, 440 F.3d at 419 (citing 18 U.S.C § 1030(a)(5)(A)(i) (emphasis added)).
[76] Id.

keyboard to be a form of "transmission" just because it transmits a command to the computer.[77] If such broad interpretations of terms such as *transmission* or *authorization* remain unchecked, they could cause chaos among litigants and threaten defendants with greater criminal and civil liability then the CFAA contemplated.[78]

Another problem with reading agency principles into the CFAA is that employers will always have a federal cause of action whenever employees access the company computer with so called "adverse interests." Employees routinely use "protected computers" throughout their workday to check personal email, weather, or fantasy football and under the broad view if these activities are done without permission and inadvertently cause damage, it may give rise to CFAA liability. Moreover, the broad construction of the CFAA will place an undue administrative burden on federal courts because it will force them to resolve disputes brought by employers against employees, suits traditionally in the province of state courts, which also seem too implicate the state more so than federal interests.

B. The Narrow View and its Criticisms.

While *Shurgard, Citrin*, and their progeny have applied a broad application of the term "without authorization", other courts have applied a more narrow interpretation. In *Lockheed Martin Corp. v. Speed*[79] the court was not persuaded by the analysis in either *Citrin* or *Shurgard* and instead chose to narrowly interpret the term "without authorization."[80] The plaintiff, Lockheed Martin Corporation, filed suit against three former employees who allegedly copied confidential and proprietary information before resigning from their positions and accepting employment at a rival defense contractor who was conspiring to gain an unfair advantage over

---

[77] Id.
[78] Id.
[79] No. 6:05-CV-1580-ORL-31, 2006 WL 2683058 (M.D. Fla. Aug. 1, 2006).
[80] Id. at *4 ("Both cases rely heavily on extrinsic materials, particularly the Second Restatement of Agency (*Citrin* and *Shurgard*) and legislative history (*Shurgard*), to derive the meaning of "without authorization").

Lockheed to get bids for an Air Force contract.[81] Lockheed essentially alleged that the former employees knowingly and with the intent to defraud accessed a protected computer without authorization or by exceeding their authorization and obtained anything of value worth more than $5,000 and recklessly caused damage.[82] Lockheed attempted to argue, as in *Citrin* and *Shurgard*, that the employees terminated their authority when they accessed confidential data with intent to steal and deliver the data to a competitor.[83] The court refused to adopt the agency theory and instead relied on the "plain language" of the CFAA[84] and essentially grouped employees in three categories: (i) employees acting *with* authorization; (ii) employees acting *without* authorization; and (iii) employees who *exceed* their authorization.[85] Applying a plain dictionary definition of authorization, the court held the "employees accessed *with* authorization"[86] and did not exceed their authorization because Lockheed had given the employees permission to access the company computer for the precise data at issue.[87]

A federal district court in Maryland in the case *International Association of Machinists and Aerospace Workers v. Werner-Masuda* followed the reasoning in *Speed*.[88] In that case, defendant Werner-Masuda, the Secretary-Treasurer of a Local Chapter of the plaintiff Union had signed an agreement that gave her access to the Union's online membership database.[89] The defendant later gave confidential membership information to the Union of Independent Flight

---

[81] Id. at *1.
[82] Id.
[83] Id. at *4.
[84] Id. at *5.
[85] Id. ([I]t is plain from the outset that Congress singled out two groups of accessers, those "without authorization" (or those below authorization, meaning those having no permission to access whatsoever-typically outsiders, as well as insiders that are not permitted any computer access) and those exceeding authorization (or those above authorization, meaning those that go beyond the permitted access granted to them-typically insiders exceeding whatever access is permitted to them).
[86] Id. (Specifically, defendant Speed had "complete access," defendant Fleming had "unrestricted access," and defendant St. Romain had "access' to the files).
[87] Id. at 5 (emphasis added).
[88] 390 F. Supp. 2d 479 (D. Md. 2005).
[89] Id. at 483.

Attendants ("UIFA") which was competing against the International Association of Machinists and Aerospace Workers ("IAM").[90] The plaintiff alleged that the defendant had violated the CFAA because she exceeded her authorization under her signed agreement with IAM.[91] The court held that under the plain meaning of the statute, the defendant did not exceed her authorized access because in her capacity as a Secretary-treasurer, she was given permission to access the membership list and IAM did not terminate her authorization at any point.[92]

The Ninth Circuit in *LVRC Holdings LLC v. Brekka* also rejected the agency approach followed by *Citrin* and *Shurgard* and instead applied an objective standard.[93] In *Brekka* the employer accused the employee, Christopher Brekka ("Chris"), of e-mailing confidential company data to his personal e-mail account.[94] The court affirmed the district court's grant of summary judgment in favor of the defendant-employee because he was authorized to use LVRC's computers while he was employed at LVRC and therefore he could not have accessed a computer "without authorization" when he emailed documents to himself prior to leaving LVRC.[95] The court also held that the employee did not "exceed authorized access" because he was entitled to obtain the documents.[96]

The proponents of the "narrow view" set out several rationales as to why "authorization" should be interpreted narrowly in employer-employee misappropriation cases. First, the CFAA's silence as to the meaning of "authorization" compels the court to start with the plain meaning of the statute and its terms.[97] The court stated, "it is a fundamental canon of statutory construction" that when a statute does not define a particular term, words will be interpreted in their "ordinary,

[90] Id.
[91] Id. at 495.
[92] Id. at 499.
[93] 581 F.3d 1127, 1134 (9th Cir. 2009).
[94] Id. at 1129.
[95] Id.
[96] Id.
[97] Id. at 1132

contemporary, common meaning."[98] The court looked to the dictionary definition of authorization and concluded that it is defined as "permission or power granted by an authority"[99] and authorize means "to endorse, empower, justify, permit by or as if by some recognized or property authority."[100] Based on this definition, the court concluded that an employer grants an employee "authorization" to access a company computer when the employer gives the employee permission to use it.[101]

Second, the rule of lenity and canon of avoiding absurd results favor a narrow construction of the CFAA.[102] The rule of lenity states that courts should resolve any ambiguity in a criminal statute in favor of the defendant.[103] The Supreme Court has warned against interpreting criminal statutes in unanticipated and novel ways that impose unexpected burdens on defendants.[104] Since employees would have no reason to know that making personal use of a company computer is a breach of a "fiduciary duty of loyalty" to an employer it would be improper for courts to interpret the CFAA in such an unanticipated manner.[105] Moreover, the rule of lenity applies in the civil context because when a statute has "both criminal and noncriminal application, courts must interpret both contexts consistently."[106] Courts have also found that reading agency principles into the CFAA may hand down potentially absurd results therefore the narrow interpretation is a more sensible approach.[107] The *Lockheed* court noted that reading agency principles into the CFAA will give employers a federal cause of action whenever employees access the company computer with "adverse interests" and accidentally

[98] Id. (quoting *Perrin v. United States*, 444 U.S. 37, 42 (1979).
[99] Id. at 1133(quoting RANDOM HOUSE UNABRIDGED DICTIONARY, 139 (2001)).
[100] Id. (quoting WEBSTER'S THIRD INTERNATIONAL DICTIONARY, 146 (2002)).
[101] Id.
[102] Id. at 1134.
[103] Rewis v. United States, 401 U.S. 808, 812 (1971).
[104] Brekka, 581 F.3d at 1134 (citing United States v. Santos, 553 U.S. 507, 513 (2008)).
[105] Id. at 1135.
[106] Id.
[107] Lockheed Martin Corp. v. Speed, No. 6:05-CV-1580-ORL-31, 2006 WL 2683058 at 7 (M.D. Fla. Aug. 1, 2006).

cause some type of damage or loss.[108] It is common for employers to routinely use "protected computers" with adverse interests unrelated to an employer's business throughout the workday[109] whether it be checking the weather, news, sports, or their Facebook. These types of activities, if done without permission and accidentally causing damage, may give rise to CFAA liability under the broad agency interpretation of "authorization."[110]

Third, the legislative history and congressional intent support a finding of narrow construction.[111] Congress initially enacted the CFAA to create a cause of action against computer hackers.[112] The U.S. District Court for the Southern District of New York has stated that "Congress was endeavoring to outlaw computer hacking and electronic trespassing [and] not providing a new means of addressing the unfaithful employee [misappropriation] situations."[113] Furthermore, in 1986 Congress amended the CFAA to narrow the sweep of the statute by removing one of the "murkier grounds of liability, under which a person's access to computerized data might be legitimate in [one] circumstance, but criminal in [another nearly identical] circumstance."[114] The amendment eliminated any reference to a defendant's *purpose* for accessing information, and instead focused solely on access.[115] Also, the Senate reports emphasize that Congress was more concerned with "outsiders" such as computer hackers rather

---

[108] Id.
[109] Id.
[110] Id.
[111] *See generally* ReMedPar, Inc. v. AllParts Med., LLC, 683 F. Supp. 2d 605, 613 (M.D. Tenn. 2010) ("Congress did not intend the CFAA to extend to situations where the access was technically authorized but the particular use of the information was not."); Jet One Group, Inc. v. Halcyon Jet Holdings, Inc., No. 08-CV-3980 (JS)(ETB), 2009 WL 2524864, at 6 (E.D.N.Y. Aug. 14, 2009) ("The statute, read as a whole, strongly indicates that Congress' intent was to prohibit the act of accessing a computer without authorization - not misusing data that one had a lawful right to access.").
[112] Id.
[113] Major, Lindsey & Africa, LLC v. Mahn, No. 10 Civ. 4239(CM), 2010 WL 3959609, at 6 (S.D.N.Y. Sep. 7, 2010).
[114] Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966 (d. Ariz. 2008) (emphasis added).
[115] US Bioservices Corp. v. Lugo, 595 F. Supp. 2d 1189, 1193 (D. Kan. 2009).

than "insiders" such as employees when passing the CFAA.[116] Therefore, it is clear that Congress intended to eliminate hacking instead of regulating or monitoring an employee's subsequent use of computer data after initial access is granted.[117]

Lastly, the proponents of the narrow view cite that efficient judicial administration requires courts to interpret the CFAA narrowly.[118] A broad interpretation of the CFAA places an undue burden on the federal court system because it forces them to resolve cases brought by employers against employees, suits which are traditionally within the province of state courts.[119] Furthermore, because of the federal courts supplemental jurisdiction they will also have to hear derivative claims related to the CFAA claim arising from the same case or controversy and therefore cause the federal system to be both inefficient and expensive to maintain.[120]

The narrow view has very few criticisms noted in court opinions because it is a more sensible and clear approach to the interpretation of the CFAA. However, one major criticism is that the narrow view does not provide the flexibility to combat the ever-evolving world of computer crimes.[121] Taking the more narrow approach of "authorization" would preclude courts to find liability in the infrequent circumstances that may warrant it.[122] Furthermore, the narrow view would preclude many suits arising from disloyal employees for the sole benefit of reducing

---

[116] Gast, 535 F. Supp. 2d at 966.
[117] Id.
[118] Id. at 967.
[119] Id.
[120] See Sarah Boyer, *Computer Fraud and Abuse Act: Abusing Federal Jurisdiction?*, 6 Rutgers J. L. & Pub. Pol'y 661, 662 ("The issues of 'unauthorized use' or 'damage or loss'…should be construed narrowly' in order to keep the claims out of federal court. Otherwise the courts will be overrun with claims by employers against former employees.").
[121] United States v. Nosal, No. CR 08-00237 MHP, 2009 WL 981336, at 7 (N.D. Cal. Apr. 13, 2009).
[122] Id.

the federal case load.[123] This could potentially eliminate the benefit of a uniform body of law in the disloyal employee scenarios.[124]

C. The Contract-Based Approach and its Limitations

The First Circuit in *United States v. Czubinski* used the contract-based approach in interpreting the term "authorization."[125] The defendant Czubinski was employed as a Contact Representative for the Taxpayer Services Division of the Internal Revenue Service ("IRS").[126] To perform his duties as an employee he would regularly access information from the IRS's computer database which included looking at individuals' private income tax return information.[127] The IRS's Rules of Conduct, which was signed by Czubinski, clearly stated that employees who had passwords and access codes were *not allowed* to access files outside the course of their official duties.[128] He knowingly disregarded IRS rules by looking at confidential information obtained by performing unauthorized searches outside the scope of his duties.[129] An internal IRS audit revealed that Czubinski accessed information regarding: the joint tax return of an assistant district attorney who had been prosecuting Czubinski's father on an unrelated felony offense and his wife; tax returns of two individuals involved in the David Duke presidential campaign; and the tax return of a woman Czubinski had dated a few times; and tax returns of other various individuals.[130] However, the government admitted that he did not do "anything more than knowingly disregard IRS rules by observing the confidential information he accessed" because he never used the data.[131] At trial, a jury convicted Czubinski of violating 18 U.S.C.

---

[123] Booms, *supra* note 6, at 557.
[124] Id.
[125] 106 F.3d 1069 (1st Cir. 1997).
[126] Id. at 1072.
[127] Id.
[128] Id. (emphasis added).
[129] Id.
[130] Id.
[131] Id.

§1030 (a)(4) that required that he access the computer either without authorization or in excess of authorization, and obtain something of value.[132] The court agreed that Czubinski exceeded his authorized access, which the IRS rules of conduct clearly outlined, but reversed his conviction because he did not deprive the IRS of any property of value when he exceeded his authorization.[133] While the court may have dismissed his convictions, the holding supports the proposition that employers are able to "contractually define the limits of authority," and courts can use these contracts to determine whether an individual has surpassed his authorized access.[134] More importantly, the First Circuit concluded its discussion with a warning of the CFAA's terms and the inherent danger it presents because "[Czubinski's conduct], although offensive to the morals or aesthetics of federal prosecutors, cannot reasonably be expected to form the basis of a federal felony."[135]

Twelve years later the federal district court in *United States v. Drew*[136] reiterated this vagueness warning. This case raises the real possibility that the Supreme Court may choose to rule on the vagueness in the CFAA for the first time to provide some clarity for the future. Lori Drew, an adult resident of O'Fallon, Missouri, allegedly created a conspiracy to intentionally access a computer used in interstate commerce without and or in excess of authorization in order to obtain information for the purpose of committing the tortious act of intentional infliction of emotional distress upon a 13-year old girl named Megan Meier through the social networking website MySpace.[137] Megan was a classmate of Lori Drew's daughter, Sarah.[138] Pursuant to the conspiracy, the conspirators established a profile for a fictitious 16 year old male named "Josh

[132] Id. at 1078.
[133] Id.
[134] Id.
[135] Id. at 1079.
[136] 259 F.R.D. 449, 452-54 (C.D. Cal. 2009).
[137] Id. at 452.
[138] Id.

Evans" on the website www.myspace.com.[139] The conspirators also posted a photo of a boy on this website without that boy's knowledge or consent.[140] The conduct violated the terms of service of the MySpace website which prohibited providing information that the user knew was false or misleading.[141] The website also prohibited including a photograph of another person without that person's consent.[142] Lori Drew and the other conspirators contacted Megan through the "Josh Evan" fake profile and flirted with her for several days.[143] Later, "Josh" informed Megan that he was moving and told her "he no longer liked her" and that "the world would be a better place without her."[144] Megan committed suicide after reading that message.[145] After learning that Megan had killed herself, Lori Drew quickly deleted the "Josh Evans" Myspace profile.[146]

The prosecutor charged Lori Drew with one count of conspiracy in violation of 18 U.S.C. §371 and three counts of violating a felony portion of the CFAA which prohibits accessing a computer without authorization or in excess of authorization and obtaining information from a protected computer where the conduct involves an interstate or foreign communication and the offense is committed in furtherance of a crime or tortious act.[147] At the beginning of the court's opinion, it noted that nothing in the legislative history of the CFAA suggests that Congress envisioned a cyberbullying prosecution under the statute.[148] Judge Wu of the Central District of California addressed the central issue raised by *Drew*: whether a computer user's intentional violation of one or more provision in an Internet website's terms of service satisfies the first

---

[139] Id.
[140] Id.
[141] Id. at 454.
[142] Id.
[143] Id. at 452-453.
[144] Id.
[145] Id.
[146] Id.
[147] Id. at 452.
[148] Id. at 451.

element of the CFAA's section 1030(a)(2)(C): whether the defendant intentionally accessed a computer either *without authorization* or in *excess of their authorization*.[149] Judge Wu noted that three important terms are not sufficiently defined within the first element: "intentionally," "access a computer", and "without authorization" and that the latter two terms have caused considerable amount of controversy as to their meaning.[150] More importantly the court noted that the interpretation of the term "without authorization" has taken a number of different approaches in the federal court system including the agency approach, the broad approach and the contract based approach.[151] Judge Wu chose to examine "without authorization" in the breach of contract context where most courts have held that an intentional or conscious violation of a website's terms of service will render the access unauthorized.[152] Under this interpretation, the court held "that an intentional breach of the [MySpace Terms of Service] can potentially constitute accessing the MySpace computer/server without authorization and/or in excess of authorization under the statute" satisfying the first element of Section 1030(a)(2)(C).[153] *Drew*'s ruling is consistent with other cases such as *EF Cultural Travel BV v. Zerfer Corp.*,[154] which has held that "a lack of authorization could be established by an explicit statement on the website restricting access."[155]

---

[149] Id. at 458 (emphasis added).
[150] Id. (citing EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 582 n.10 (1st Cir. 2001) ("Congress did not define the phrase 'without authorization,' perhaps assuming that the words speak for themselves. The meaning, however, has proven to be elusive."); (Southwest Airlnes Co. v. BoardFirst, L.L.C., 2007 WL 4823761 at *12-13, 2007 U.S. Dist. LEXIS 96230 at *36 (N.D. Tex. 2007) ("The CFAA does not define the term 'access'.").
[151] Id. at 460; *See generally* Citrin, 440 F.3d 418, 420-21; Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1124-25; United States v. Phillips, 477 F.3d 215, 219 (5th Cir.), *cert. denied*, 552 U.S. 820 (2007).
[152] Id. (citing Southwest Airlines Co. v. Farechase, Inc., 318 F. Supp 2d 435, 439-40 (N.D. Tex. 2004); Register.com, Inc. v. Verio, Inc., 126 F. Supp. 2d 238, 247-51 (S.D.N.Y. 2000), *aff'd*, 356 F.3d 393 (2d Cir. 2004)).
[153] Id. at 461.
[154] 318 F.3d 58, 63 (1st Cir. 2003).
[155] Id. (In this case, a travel agency, Explorica, hired Zefer Corp. to build a computer program that could take travel prices from its competitor's website and place them into an Excel spreadsheet, allowing Explorica to easily undercut those prices. The issue before the court was whether the device that copied prices over constituted "exceeded authorized access," since the public had access to the websites and anyone could take the time to put together a list of prices themselves. The court noted that the competitor's website did not contain any explicit ban on devices such

After the court established that Drew's conscious violation of the MySpace Terms of Service constituted a violation under the CFAA, the next issue was whether the CFAA withstands the void-for-vagueness doctrine.[156] The void-for-vagueness doctrine has two prongs: (1) the offense must have "relatively clear guidelines" so an ordinary person can understand what conduct is illegal; and (2) the law must give some minimal "objective criteria" to assist law enforcement agencies in its application.[157] The court, quoting Justice Holmes, observed that, as to criminal statutes, there is a "fair warning" requirement:

> "Although it is not likely that a criminal will carefully consider the text of the law before he murders or steals, it is reasonable that a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed. To make the warning fair, so far as possible the line should be clear.[158]

Judge Wu concluded that basing a CFAA violation upon the conscious violation of a website's terms of service runs afoul of the void-for-vagueness doctrine, because of the absence of minimal guidelines to govern law enforcement and because of actual notice deficiencies.[159]

The court states four arguments to conclude that the CFAA neither explicitly states nor implicitly suggests that breaches of contract are criminalized.[160] First, the language contained in the CFAA does not explicitly state that the CFAA has "criminalized breaches of contract" in the context of website terms of service.[161] Normal breaches of contract are not subject to criminal

---

as the one used in this case, but if it did, the ban notice would serve as an "explicit statement on the website restricting access.").
[156] Drew, 259 F.R.D. at 462.
[157] Id. at 462-63.
[158] Id. at 463 (J. Holmes) (quoting McBoyle v. United States, 283 U.S. 25, 27 (1931)).
[159] Id. at 464.
[160] Id.
[161] Id.

prosecution.[162] Therefore, "ordinary people" may expect to be exposed to civil claims for violating a contractual provision but they would not expect criminal prosecution.[163] Second, Section 1030 is ambiguous in explaining which violations if any constitute unauthorized access.[164] The court found that if any conscious breach of a website's terms of service is sufficient to establish a violation of the CFAA, the law would afford too much discretion to the police and too little notice to citizens who wish to use the Internet.[165] Third, by allowing website owners to define when a CFAA violation occurs will ultimately put the website owners in the position of the "lawmaker" which will only lead to further vagueness problems.[166] For example, the MySpace Terms of Service prohibits its members from posting in "band and filmmaker profiles…sexually suggestive imagery or any other unfair…[c]ontent intended to draw traffic to the profile."[167] It is unclear from this provision what "sexually suggestive imagery" and "unfair content" means or entails.[168] Finally, a level of indefiniteness arises when applying contract law in general and/or other contractual requirements within the applicable terms of service to any criminal prosecution.[169] For example, the MySpace Terms of Service included an arbitration clause for "any dispute" arising between the service provider and a visitor/member/user. [170] Therefore, before a breach of a term of service can be found or the ability of MySpace to terminate the visitor/member/user's access to the site can be determine, the issue would be

[162] Id. (*See generally* United States v. Handakas, 286 F.3d 92, 107 (2d Cir. 2002), *overruled on other grounds in*, United States v. Rybicki, 354, F.3d 124, 144 (2d Cir. 2003)(en banc)).
[163] Id.
[164] Id.; *See also* Computer Fraud and Abuse Act, 18 U.S.C. § 1030.
[165] Drew, 259 F.R.D. at 465.
[166] Id.
[167] Id.
[168] Id.
[169] Id.
[170] Id.

subject to arbitration.[171] This would raise the question as to whether a finding of breach of authorization can be made without arbitration.[172]

The *Drew* decision is significant because it recognizes the limitations of the CFAA. The result of the opinion is a blow to the prosecutors who were desperate to charge Drew with anything following the public outrage the story generated. The decision was a good one because turning Terms of Service breaches into a federal crime could have potentially opened a Pandora's box of prosecution for even trivial matters and would convert innocent Internet users into misdemeanant criminals.

III. Proposal: Courts Should Apply the Rule of Lenity to Resolve Ambiguity

This article displays how absurd the results are between Federal courts attempting to interpret the CFAA. Until the circuit split gets resolved or Congress decides to amend the statute, the courts should apply the rule of lenity in favor of the defendant.[173]

The rule of lenity rests upon two foundations. First, it is founded on the fundamental principle that no citizen should be subjected to punishment that is not clearly prescribed.[174] Accordingly, "a fair warning should be given to the world in language that the common world will understand, of what the law intends to do if a certain line is passed."[175] Second, the rule rests on the principle that the power of punishment is vested in the legislative, not in the judicial

---

[171] Id.
[172] Id.
[173] See generally, Busic v. United States, 446 U.S. 398 (1980); Staples v. United States, 511 U.S. 600 (1994); United States v. Cruz, 805 F.2d 1464 (11th Cir. 1986); United States v. Lowe, 860 F.2d 1370 (7th Cir. 1988); United States v. Mitchell, 39 F.3d 465 (4th Cir. 1994); Gun South, Inv. v. Brady, 711 F. Supp. 1054 (N.D. Ala. 1989), decision rev'd on other grounds, 877 F.2d 858 (11th Cir. 1989).
[174] United States v. Santos, 128 S. Ct. 2020, 2025 (2008); Bingham, Ltd. v. U.S., 545 F. Supp. 987 (N.D. Ga. 1982), judgment rev'd on other grounds, 724 F.2d 921 (11th Cir. 1984); United States v. Blankenship, 923 F.2d 1110 (5th Cir. 1991).
[175] Arthur Andersen LLP v. United States, 544 U.S. 696, 703 (2005) (quoting McBoyle v. United States, 283 U.S. 25, 27 (1931) (Holmes, J.)); See also United States v. Aguilar, 515 U.S. 593, 600 (1995).

department.[176] Quite simply, within our constitutional framework the legislative power, including the power to define criminal acts and to prescribe the punishments to be imposed upon those found guilty of them, resides wholly with the Congress.[177]

The rule of lenity, however, only applies if after reviewing all sources of legislative intent, a statute remains ambiguous.[178] The Supreme Court has also stated that "[t]he rule of lenity applies only if, after seizing everything from which aid can be derived, we can make no more than a guess as to what Congress intended. To invoke the rule, we must conclude that there is a grievous ambiguity or uncertainty."[179] Many critics have stated the CFAA is ambiguous because it was poorly written from the beginning. Also, most judges attempting to interpret the statue would agree that the CFAA is very unclear and vague. This article has proved that there is certainly some irreconcilable ambiguity in interpreting the terms "without authorization" and "exceeds authorization". Therefore, courts should apply a more consistent and clear approach to these terms by applying the rule of lenity.

IV. Conclusion

Congress originally enacted the CFAA as a criminal statute to combat the growing threat of computer hackers. The pivotal point of many federal court decisions are on the terms "without authorization" and "exceeds authorization". Most courts interpret these two terms using the broad view, the narrow view, or the contract-based approach. The CFAA's ambiguity has led to absurd results. Since the CFAA is primarily a criminal statute and since it creates both civil and criminal liability for violators, courts should apply principles of strict construction of criminal laws to interpret the statute.

---

[176] United States v. Wiltberger, 18 U.S. 76, 95 (1820).
[177] Whalen v. United States, 445 U.S. 684, 689 (1980).
[178] See generally, Beecham v. U.S., 511 U.S. 368 (1994); United States v. Shabani, 513 U.S. 10 (1994); United States v. McDonald, 692 F.2d 376 (5th Cir. 1982).
[179] Muscarello v. United States, 524 U.S.125, 138-39 (1998) (internal quotations, omissions, and citations omitted).