NOTE

A HYBRID APPROACH TO ANALYZING AUTHORIZATION IN THE COMPUTER FRAUD AND ABUSE ACT

*Matthew Gordon**

The Computer Fraud and Abuse Act criminalizes certain actions involving the unauthorized use of a computer. Courts are split on how to interpret "authorization" under the Act. This note argues in favor of an approach that combines elements from three of the approaches different courts have used.

A HISTORY OF THE COMPUTER FRAUD AND ABUSE ACT

Over the past few decades, computers have become increasingly prevalent in our society.[1] Today, it is common for people to rely on computers, smartphones, and tablets as digital assistants that aid them in their various daily tasks.[2] Because of their efficiency, storage capacity, and increasing portability, the devices are ideal for storing business and personal information and data. Much of the information that users store on these devices is private in nature, such as trade secrets for businesses, financial information, or media for individuals. Users do not want this information to be available to every

---

* J.D. 2015, Boston University; B.A. Psychology 2012, Lehigh University. Thank you to Professor Gordon for guidance in writing this note, to the staff of the Boston University Journal of Science & Technology Law for their work preparing this note for publication, and to my family and friends for all of their support.

[1] The United States Census Bureau has indicated that in 2011, 75.6 percent of households had a computer, compared to 61.8 percent of households in 2003, and 8.2 percent in 1984. THOM FILE, U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES: POPULATION CHARACTERISTICS, 1, 1 (2013), *available at* http://www.census.gov/prod/2013pubs/p20-569.pdf (archived at http://perma.cc/6BJ9-VS8P). Additionally, 48 percent of Americans over the age of fifteen use smartphones. *Id.* at 11. A study by the Pew Internet and American Life Project found that 34 percent of adults over the age of eighteen own or use a tablet. KATHRYN ZICKUHR, PEW INTERNET PROJECT, TABLET OWNERSHIP 2013 1, 2 (2013), *available at* http://www.pewinternet.org/~/media//Files/Reports/2013/PIP_Tablet%20ownershttp://www.pewinternet.org/~/media//Files/Reports/2013/PIP_Tablet%20ownership%202013.pdf (archived at http://perma.cc/D8VM-BQNV).

[2] *See* FILE, *supra* note 1, at 11; ZICKUHR, *supra* note 1.

person who is able to access their device.

In the late 1970s and early 1980s, computers were rapidly becoming more widespread among businesses and consumers.[3] As the legitimate uses of computers became more numerous, the use of computers in committing crimes increased as well.[4] As the incidence of these crimes became more common, it became apparent which existing criminal statutes were insufficient to deal with the emerging issue of computer crime.[5]

> Any enforcement action in response to criminal conduct indirectly or directly related to computers must rely upon a statutory restriction dealing with some other offense. This requires the law enforcement officer, initially the agent, and then the prosecutor, to attempt to create a "theory of prosecution" that somehow fits what may be the square peg of computer fraud into the round hole of theft, embezzlement or even the illegal conversion of trade secrets.[6]

Congress passed the Computer Fraud and Abuse Act (CFAA) in 1986 to address these problems.[7] By including the CFAA as a separate provision in the Comprehensive Crime Control Act of 1984 instead of adding provisions about computers to existing criminal statutes, Congress was able to address computer related crimes in a single statute.[8] This better aided the CFAA in fulfilling Congress's intent "to provide 'a clearer statement of proscribed activity' to 'the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes by unauthorized access.'"[9]

The specific intention of the original 1986 version of the CFAA was to protect classified information on government computers and financial records or credit histories from financial institutions.[10] Although it was a step in the right direction, the CFAA in its original form was too limited in scope, leading

---

[3] There were estimated to be 5,000 desktop computers in America in 1978. S. REP. NO. 99-432, at 2 (1986). This amount was estimated to have increased to 5,000,000 by 1986. *Id.*

[4] A survey conducted by the American Bar Association in 1984 found that over 50% of its respondents had been victimized by some form of computer crime. *Id.* (citing AMERICAN BAR ASSOCIATION, TASK FORCE ON COMPUTER CRIME, REPORT ON COMPUTER CRIME (1984)).

[5] *Id.*

[6] *Id.* at 14.

[7] Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012).

[8] The Comprehensive Crime Control Act of 1984 was the first major revision to the United States Criminal Code to be implemented since the 1900s. *See* Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, 98 Stat. 1976; H. MARSHALL JARRETT & MICHAEL W. BAILIE, PROSECUTING COMPUTER CRIMES 1 (2d ed. 2010).

[9] JARRETT, *supra* note 8 (citing H.R. REP. NO. 98-894, at 6 (1984)).

[10] S. REP. NO. 99-432, at 3.

Congress to expand and amend the statute soon after.[11] The first set of amendments to the CFAA passed in 1986.[12] The Senate, concerned with balancing federal interests in stopping computer crimes with the states' interest in enacting their own statutes, made it clear in their Judiciary Committee report that they were rejecting the idea of a statute that was sweeping in scope.[13] In enacting the 1986 amendments, the Senate wanted to extend the CFAA only to cases involving "[f]ederal interest computers."[14] These were cases where there was a compelling federal interest such as where the Federal Government or a financial institution was involved, or where the crime was interstate in nature.[15]

Although Congress initially intended to limit the scope of the statute by applying it only to "federal interest computers," Congress further amended the CFAA in 1996, greatly broadening the statute's reach.[16] The purpose of the amendments was to strengthen the CFAA in order "to protect better the confidentiality, integrity, and security of computer data and networks."[17] The Senate Judiciary report indicated its intention to fill the gaps left open by the existing act, which was too narrow to properly deal with the way computer crime was evolving.[18]

One gap involved the types of computers that were protected under the CFAA.[19] Congress noted the limiting scope of the words "federal interest computers."[20] Under the then-existing law, non-classified information was only protected if it was stored on a computer used by the Federal Government or a financial institution.[21] This left unprotected any non-classified information that was stored on computers used by civilians or a state government.[22] To fill this gap, Congress changed the wording to "protected computer."[23]

Another gap Congress hoped this amendment would fill concerned privacy.[24] Under then-current law, the information stored on government computers was only protected from outsiders who gained access to those

[11] *Id.*

[12] *See* 18 U.S.C. § 1030.

[13] S. REP. NO. 99-432, at 4.

[14] *Id.* at 5.

[15] *Id.* at 4.

[16] *See* S. REP. NO. 104-357, at 1 (1996).

[17] *Id.* at 3.

[18] *Id.* at 3, 5.

[19] *Id.* at 4.

[20] *Id.*

[21] *Id.*

[22] *Id.*

[23] *Id.* at 13.

[24] *Id.* at 4.

computers.[25] There was no protection against government employees who abused their privileges to gain access to this confidential information.[26] Congress changed the wording of the statute in an effort to strengthen the protection from insiders abusing their access.[27] How to interpret the scope of this change has been the subject of disagreement by the courts, and is the topic of this note.

THE COMPUTER FRAUD AND ABUSE ACT TODAY

Today, the CFAA is much broader and more expansive than the original statute passed in 1986.[28] One indication of the breadth of the statute is in the CFAA's definitions.[29] The CFAA defines a "computer," for instance, as "an electronic . . . or other high speed data processing device performing logical, arithmetic, or storage functions."[30] This extends the definition to include not just personal computers, but tablets, smartphones, and any other computing device as well, provided that it does not fall within one of the few exceptions.[31]

The CFAA specifically addresses "protected computers," which it defines as "a computer 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."[32] Because so many communications over the Internet are interstate or international, virtually every computer falls under the jurisdiction of the statute.[33]

The CFAA today proscribes and applies civil and criminal liability for seven different actions a user may partake in when he "exceeds authorized access" or is "without authorization."[34] Several of these provisions still contain language indicating the CFAA's original intent to protect government information and financial data.[35] Many of the actions have been expanded to apply more generally to "protected computers."[36] One such provision is a prohibition on

[25] *Id.*

[26] *Id.*

[27] *See id.* at 6, 9-11.

[28] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012).

[29] *See id.* § 1030 (e).

[30] *Id.* § 1030 (e)(1).

[31] *See id*. "[S]uch term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device." *Id*.

[32] *Id.* § 1030(e)(2)(B).

[33] Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127 (W.D. Wash. 2000).

[34] 18 U.S.C. § 1030(a).

[35] *See id.* § 1030.

[36] *See id.*

"intentionally access[ing] a computer without authorization or exceed[ing] authorized access and thereby obtain[ing] information.[37] The current version of the CFAA expands its reach to information on any "protected computer," not just on those used by the government or financial institutions.[38]

The CFAA's list of proscribed acts extends beyond merely protecting information.[39] In addition to protecting information from unauthorized use of "protected computers," the CFAA, as its name would suggest, prohibits the furtherance of fraud if done by a person who "knowingly accesses a protected computer without authorization or exceeds authorized access."[40] Congress also aimed to prevent damage done to computers by including a provision prohibiting the unauthorized transmission of codes or commands that damage protected computers.[41] This provision applies mainly to hackers or users who would send computer viruses.[42] Similarly, another provision that prohibits trafficking passwords through which a computer can be accessed without authorization was implemented to target hackers.[43] Finally, Congress sought to prevent extortion by those who threaten to do damage to or obtain information without authorization from protected computers.[44]

THE "AUTHORIZATION" ISSUE

All seven provisions of the CFAA that proscribe prohibited acts use either the words "without authorization," "exceeds authorized access," or both.[45] The CFAA provides a definition of "exceeds authorized access." However, it fails to define "without authorization," or even "authorization."[46] It is difficult to determine a clear meaning of "authorization" from the statute's text.[47] Once a user is granted access to a computer, is he authorized to use the information found on it regardless of purpose? Is the user authorized to use that information for only specific tasks laid out by whoever granted the authorization? Is the user authorized to use the information only in a way that furthers the purpose for which he was granted access?

---

[37] *Id.* § 1030(a)(2).

[38] *Id.*

[39] *See id.* § 1030(a).

[40] *Id.* § 1030(a)(4).

[41] *Id.* § 1030(a)(5).

[42] *See id.*

[43] *Id.* § 1030(a)(6).

[44] *Id.* § 1030(a)(7).

[45] *Id.* § 1030(a).

[46] *Id.* §1030(e). "[T]he term 'exceeds authorized access' means to access a computer with authorization and to use such access to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter." *Id.* §1030(e)(6).

[47] *See id.* §1030.

Because each provision of the CFAA requires that an act be done "without authorization" or that an act "exceeds authorized access," understanding the meaning of "authorization" is crucial to effectively applying the statute.[48] The federal courts are divided on whether to take a broad or narrow approach to interpreting the definition of "authorization."[49] Academics and the courts have divided their approaches into three categories: a narrow code-based approach, a broader contract-based approach, and an even broader agency-based approach.[50] Each of these approaches has merit; however, none of them are flawless. In this note, I will discuss the benefits and drawbacks of each approach and then suggest an approach that combines elements of all three.

CODE-BASED APPROACH

The narrowest established approach to interpreting the meaning of "authorization" is the code-based approach.[51] The code-based approach only restricts the access of information but does not protect against its misuse or misappropriation.[52] Under this approach, a user is without authorization if the computer itself prevents the initial access through code-based security, such as a password.[53] A user would gain unauthorized access if he or she has found a way to circumvent the password, such as guessing it randomly.[54] On the other hand, if a user has been granted access to the computer by the authorizer, he or she is "authorized" to use any of the information on it, regardless of purpose.[55]

While no court has explicitly adopted the code-based approach, some have taken approaches consistent with its reasoning, sometimes referring to it as looking at the "plain meaning" of the statute.[56] These courts argue that this interpretation comes from the text itself.[57] Courts that argued that this approach follows the text's plain meaning point to the fact that the CFAA distinguishes between the terms "without authorization" and "exceeding

[48] *See id.* §1030(a).

[49] Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 615 (E.D. Pa. 2013).

[50] *Id.* at 615-16.

[51] *See id.* at 616.

[52] *See* United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012).

[53] Katherine Mesenbring Field, Note, *Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 825 (2009).

[54] *Id.*

[55] *See id.*

[56] Garrett D. Urban, Note, *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, 1380 (2011).

[57] *See Nosal*, 676 F.3d at 863; Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1343 (N.D. Ga. 2007); Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108, at *14-15 (M.D. Fla. Aug. 1, 2006).

authorization," and even uses both terms throughout the statute.[58] Courts that make this distinction, such as the Florida District Court, argue that the existence of the two separate terms indicates that it was Congress's intent for these terms to be used separately.[59]

In one case, the Ninth Circuit defined the word "authorization" as "permission or power granted by an authority."[60] It then differentiated between "without authorization" and "exceeds authorized access" by stating:

> an individual who is authorized to use a computer for certain purposes but goes beyond those limitations is considered by the CFAA as someone who has "exceed[ed] authorized access." On the other hand, a person who uses a computer "without authorization" has no rights, limited or otherwise, to access the computer in question. In other words, for purposes of the CFAA, when an employer authorizes an employee to use a company computer subject to certain limitations, the employee remains authorized to use the computer even if the employee violates those limitations.[61]

A Florida district court differentiated the terms, stating that one who is "without authorization" is either an outsider or an insider without any permission to access the computer, while one who "exceeds authorized access" is an insider who has been granted permission to access the computer but has gone beyond that permitted access.[62]

The Ninth Circuit adopted a narrow approach in *LVRC Holdings LLC v. Brekka*.[63] In this case, Brekka, an employee who obtained a password to the LVRC's website through the course of his employment, logged in and obtained LVRC's confidential statistical data.[64] Brekka emailed the data to his and his wife's personal email accounts and subsequently used it in his own consulting businesses.[65] The court reasoned that because LVRC gave Brekka the password, it authorized him to access and use the information on that

---

[58] *Lockheed*, 2006 U.S. Dist. LEXIS 53108, at *14. "The CFAA targets access 'without authorization' in six separate offenses (§§1030(a)(1), (a)(2), (a)(3), (a)(4), (a)(5)(A)(ii), (a)(5)(A)(iii)), only three of which also reach persons 'exceeding authorized access' (§§ 1030(a)(1), (a)(2), (a)(4)). Thus, it is plain from the outset that Congress singled out two groups of accessers, those 'without authorization' . . . and those exceeding authorization." *Id.*

[59] *Id.*

[60] LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009) (citing RANDOM HOUSE UNABRIDGED DICTIONARY, 139 (2001)).

[61] *Id.*

[62] *Lockheed*, 2006 U.S. Dist. LEXIS 53108, at *14-15.

[63] *Brekka*, 581 F.3d at 1137.

[64] *Id.* at 1129.

[65] *Id.* at 1129-30.

website.[66] The court ultimately held that because Brekka was authorized to access the computers during his employment with LVRC, he did not violate the CFAA.[67]

A Florida court conducted a similar analysis in *Lockheed Martin Corp. v. Speed*.[68] In this case, Speed and two other employees of Lockheed used their access to Lockheed's computer systems to copy hundreds of confidential documents and gave them to a competitor.[69] Following the code-based approach's logic, the court held that because Lockheed permitted these employees to access the computer, they were not "without authorization," and because Lockheed allowed these employees to access the specific information at issue, they did not "exceed authorized access."[70] Ultimately, the court held that because the defendants were neither "without authorization" nor "exceeding authorized access," Lockheed was not entitled to relief under the CFAA.[71]

Most of the support for the narrow interpretation of the code-based approach derives from the fact that it is the only interpretation that effectively reconciles the use of the two different terms.[72] The broader interpretations of "without authorization" consider how the computer and the information stored on it are used, causing the two terms to overlap.[73] By defining "authorization" as the initial permission to access, the code-based approach maintains the distinction between "without authorization," where no permission has been granted, and "exceeds authorized access," where initial permission has been granted but the terms of that permission have been violated.[74]

The code-based approach has the benefit of providing a clear rule that is easy to follow and not open to discretion.[75] As one scholar pointed out, the CFAA is a criminal statute, and a broader approach to interpreting "authorization" may run into due process concerns by failing to give proper notice that someone is breaking the law.[76] Meanwhile, the code-based

[66] *Id.* at 1133.

[67] *Id.* at 1137.

[68] *See* Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108 (M.D. Fla. Aug. 1, 2006).

[69] *See id*. at *2-4.

[70] *Id.* at *15.

[71] *Id.* at *28.

[72] *See* Diamond Power Int'l, Inc. v. Davidson, 540 F. Supp. 2d 1322, 1342 (N.D. Ga. 2007).

[73] *Id.* at 1342-43.

[74] *Id.* at 1343.

[75] *See* Samantha Jensen, Note, *Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail*, 36 HAMLINE L. REV. 81, 96-97 (2013).

[76] Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2258 (2004). This is especially problematic for the agency approach, under which a court might find a

approach provides a clear rule that makes a definite distinction between what is or is not "authorized."[77] In addition, the code-based approach would interpret "authorization" in a way that is consistent with the rule of lenity.[78]

The code-based approach has received criticism for being too restrictive in its interpretation of "authorized access" and thus insufficient to protect against the acts it aims to prevent.[79] A problem with the code-based approach arises with respect to 18 U.S.C. § 1030(a)(5)(A), which makes it a crime to "knowingly cause[] the transmission of a program, information, code, or command, and as a result of such conduct, intentionally cause[] damage without authorization, to a protected computer."[80] Unlike the other provisions that refer to gaining access "without authorization," this provision prohibits causing damage "without authorization."[81] Under a code-based interpretation of "authorization," a wrongdoer would not be liable under the CFAA for any intentional destruction or damage caused, so long as he did not circumvent a password or other coded security measure in the process.[82] This is precisely what occurred in *Trademotion, L.L.C. v. Marketcliq, Inc.*: in this case, Anderson, Trademotion's former Vice President of Internet Marketing, had full administrative access to their website and account management code.[83] Using this access, Anderson deleted files from Trademotion's computers and inserted code into their online software to divert emails form prospective customers to the defendant company.[84] The court held that because his access was unrestricted, "Anderson was fully authorized to access the computer and code,

defendant criminally liable for going against a company policy, even if there is no explicit contract provision against his actions. *Id.*

[77] *See* Jensen, *supra* note 75, at 96-7.

[78] The rule of lenity, a canon of statutory interpretation, is an attempt by courts to avoid due process concerns by reading ambiguous criminal statutes in favor of the defendant. *See* United States v. Santos, 553 U.S. 507, 514 (2008).

[79] *See* Urban, *supra* note 56, at 1380 n.66.

[80] *See* Computer Fraud and Abuse Act 18 U.S.C. § 1030(a)(5)(A). The CFAA defines "damage" as "any impairment to the integrity or availability of data, a program, a system, or information." *Id.* § 1030(e)(8). This would extend the term to include any deletion of files on a protected computer.

[81] *Id.* § 1030(a)(5)(A).

[82] *See id.* § 1030(a)(5)(A). One scholar has argued that "without authorization" for the purpose of this provision means "without *permission*," and argues that the statute should be amended as such in order to avoid the unintended results of the narrow interpretation of the code-based approach as it relates to this provision. Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1661 (2003).

[83] *See* Trademotion, L.L.C. v. Marketcliq, Inc., 857 F. Supp. 2d 1285, 1291 (M.D. Fla. 2012).

[84] *Id.* at 1289.

and, as such, his doing so cannot be 'without authorization' under the Act."[85]

Despite the benefits of the code-based approach, the narrow interpretation has the unintended result of undermining the CFAA's ability to prevent one of the acts for which it was intended.[86] As a result, the code-based approach cannot be the definitive approach to interpreting "authorization" for the purposes of the CFAA.

CONTRACT-BASED APPROACH

Some courts, such as those in the First Circuit, acknowledging that the code-based approach may be too restrictive, take a somewhat broader approach to interpreting "without authorization" based on law governing contracts.[87] Unlike the code-based approach, the contract-based approach looks beyond how the computer is accessed, and instead looks to the purpose for which it was accessed.[88] If the purpose for which the computer was accessed is different from, or in excess of, the purpose for which permission was granted, the courts will find that the user is "without authorized access" or "exceeds authorized access."[89] Courts look at the existence of a contract to define the limits of authorization and decide if the user has exceeded their authority.[90]

Courts using this approach will look to whether there is an express or implied contract between the user and the party with the authority to grant access.[91] One issue which has not yet been resolved is what types of documents may be used as contracts for the purpose of this approach.[92] Cases where courts use the contract-based approach usually involve employment contracts with confidentiality agreements or employee handbooks.[93] Courts have also used terms-of-service agreements between Internet providers and their account holders in defining authorization.[94] Under the contract-based approach, courts will establish the boundaries of what is "authorized" by looking at whether the user has violated the terms of the contract.[95] If the user has violated the terms of the contract, the court will find that the user "exceeds authorization" or is "without authorization."[96]

---

85 *Id.* at 1291.

86 *See* Urban, *supra* note 56, at 1381.

87 Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 615 (E.D. Pa. 2013).

88 United States v. John, 597 F.3d 263, 272 (5th Cir. 2010).

89 *Id.*

90 Field, *supra* note 53, at 828.

91 *Id.* at 827.

92 *Id.*at 827-29.

93 *Id.* at 827.

94 *See* Am. Online, Inc. v. LCGM, Inc., 46 F. Supp. 2d 444, 452 (E.D. Va. 1998).

95 *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 581-82 (1st Cir. 2001).

96 *Id.*

Another issue that has not been resolved is how specific the terms of a contract must be to define the limits of authorization. Employment contracts may come in different forms and varying degrees of specificity. Whereas one company may have vague language giving a general sense that sharing trade secrets is forbidden, another company may have more meticulous language outlining which specific acts are not permitted.[97] Generally, the more specific the terms of the contract, the more likely the court will use them in making their determination. In fact, some courts have stated that they require the terms of the governing contract to explicitly state which acts are forbidden.[98]

Courts do not always require that the contract be express and may also recognize the existence of implied contracts in the form of widely known company policies in making their determinations.[99] In *United States v. John*, John, an account manager at Citigroup, had access to the company's computer systems and confidential customer information.[100] John used this access to print out information that she shared with her brother, enabling them to incur fraudulent charges on four accounts.[101] This was in violation of Citigroup's official policy, prohibiting the misuse of computer systems and customer information.[102] This company-wide policy was well-known, as it was reiterated at training sessions that John attended.[103] The court held that because the policy was so widely known, and was known or should have been known by John, the company policy dictated the terms under which John was "authorized" to use the computer systems and customer information stored on them.[104] Because John used her access in a way contrary to Citigroup's policies, the court held that John's conduct exceeded authorized access.[105]

The contract-based approach has the benefit of not being as restrictive as the code-based approach. The contract-based approach provides protection even when information is not protected by a password. This is useful when the information needs to be protected from an insider who would have the password, as was the case in United States v. John.[106] Rather than the limited definition of the code-based approach, the contract-based approach gives those with the authority to authorize computer use the ability to tailor the scope of that authorization to their own specific purposes. Under this approach,

---

[97] Field, *supra* note 53, at 828.

[98] *EF Cultural Travel*, 318 F.3d at 64 ("[P]ublic website providers ought to say what non-password protected access they purport to forbid.").

[99] United States v. John, 597 F.3d 263, 272 (5th Cir. 2010).

[100] *Id.* at 269.

[101] *Id.*

[102] *Id.* at 272.

[103] *Id.*

[104] *Id.* at 273.

[105] *Id.* at 272-73.

[106] *See id.* at 269.

employers have the freedom to specify prohibited uses for their machines, to better serve the function of the CFAA. On the other hand, the contract-based approach has also received criticism for being too vague and open to discretion in defining "authorization," to the extent that it may raise due process concerns.[107]

AGENCY-BASED APPROACH

The broadest approach used by the courts to interpret "without authorization" is the agency-based approach.[108] The agency-based approach is derived from the principles of agency law, where the employee owes a duty of loyalty to their employer, acting only in the employer's interest.[109] This duty, along with the agency relationship, terminates the moment the employee serves an interest adverse to their employer's interests.[110] Under the agency-based approach, employees are "authorized" to use a computer in the interest of their employer, however this authorization ends when the employee uses the computer or information stored on it to serve an interest adverse to the employer's.[111]

Like the contract-based approach, courts using the agency-based approach look to the purpose for which a computer is accessed, rather than the way it is accessed.[112] This approach differs from the contract approach in that courts do not look to the existence of a contract to define the limits of authorization.[113] Under the agency-based approach, courts look to the existence of a relationship between the user and the party granting authorization to define the authorization's limits.[114] The user "exceeds authorization" or is "without authorization" when they have acted to serve an interest which is adverse to their duties.[115]

Courts invoking the agency-based approach, such as those in the Seventh Circuit, have held that if the employee breaches a duty of loyalty or fails to disclose adverse interests, the employee has terminated their agency relationship.[116] At this point, the employee no longer has any authority to access the computer which they were granted access to under the terms of that

---

[107] *See* Jensen, *supra* note 75, at 96-97; *infra* text accompanying notes 189-202.

[108] *See* Dresser-Rand Co. v. Jones, 957 F. Supp. 2d 610, 615-16 (E.D. Pa. 2013).

[109] Field, *supra* note 53, at 823.

[110] *Id.*

[111] *Id.*

[112] *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006).

[113] *See* Field, *supra* note 53, at 823.

[114] *Id.*

[115] *See id.*

[116] *Citrin*, 440 F.3d at 420-21; RESTATEMENT (SECOND) OF AGENCY § 112 (1958).

relationship.[117] This is what the court held in *International Airport Centers, L.L.C. v. Citrin*.[118] In this case, Citrin was an employee of a real estate company.[119] The company loaned Citrin a laptop to record and collect data identifying potential properties to acquire.[120] While employed by the company, Citrin breached his duty of loyalty by using the laptop to engage in improper conduct.[121] Upon quitting his job with the company, Citrin loaded a program into the computer that deleted and overwrote both the data he collected and the data that showed his participation in improper conduct during his employment.[122] The court held that the agency relationship ended when Citrin violated his duty of loyalty to his employer.[123] The court further held that because the only basis of his authorization to access the laptop was this agency relationship, this authorization also ended with his breach of duty.[124] The court ultimately held that using the program to erase the data evidencing Citrin's misconduct constituted "knowingly caus[ing] the transmission of a program . . . and as a result of such conduct, intentionally caus[ing] damage to a protected computer," was in violation of 18 U.S.C. § 1030(a)(5)(A)(i).[125]

The broad scope of the agency-based approach favors employers, as it only requires a demonstration that the employee acted adversely to the employer's interests in order to show they were "without authorization."[126] One scholar has even suggested that the number of claims filed by companies under the CFAA has increased since the Seventh Circuit adopted the agency-based approach in Citrin.[127] The agency-based approach gives the authorizing party the benefit of providing protection in the absence of an expressed or implied contract or the existence of coded protections such as a password. It may be difficult for an employer to outline every specific use they wish to prohibit in an employment contract or employee handbook. The agency-based approach

---

[117] *Citrin*, 440 F.3d at 420-21.

[118] *Id.*

[119] *Id.* at 419.

[120] *Id.*

[121] *Id.* at 420.

[122] *Id.* at 419. Typically, just deleting a file only deletes the computer's index for it and frees up the space in which it is written to be used by something else. *Id.* The file remains until new data is written in its place. *Id.* By using this program, Citrin ensured that the company would be unable to retrieve the files. *See id.*

[123] *Id.* at 420.

[124] *Id.* at 420-21.

[125] *Id.* at 419.

[126] Field, *supra* note 53, at 824.

[127] Katherine Field noted that at the time of her writing in 2008, two years after the *Citrin* decision, Shepardizing the case through LexisNexis indicated that the case had been cited in thirty-one cases. Field, *supra* note 53, at 824 n.30. As of December 18, 2013, according to LexisNexis, *Citrin* has been cited in one hundred thirteen cases.

solves this by looking more generally at the interest of the party authorizing the computer's use rather than specific prohibited uses. Under the agency-based approach, when someone such as an employer is authorizing access to their machines containing confidential data, they do not have to worry about this information being used against them. Like the contract-based approach, the agency-based approach has also received criticism for raising potential due process concerns because of it being too vague and open to discretion in defining "authorization."[128]

EXAMINING LEGISLATIVE HISTORY

When the language of a statute leads to different interpretations, it is generally helpful to look at the legislative history to try to glean Congress's intent when it passed the statute.[129] Courts usually construe the legislative history to support whichever stance they ultimately take.[130] In this particular case, the legislative history is also ambiguous and does not provide a clear answer as to how to interpret "authorization."[131] However, looking more generally at the way the statute has evolved since it first passed, the statute's history seems to support a broader approach.

The Senate report accompanying the original 1986 act contains language that strongly supports a narrower code-based approach.[132] Congress was concerned with creating a statute that was overbroad and wanted to make sure that any party prosecuted under the CFAA was deserving of criminal liability.[133]

> The Committee was concerned that a Federal computer crime statute not be so broad as to create a risk that government employees and others who are authorized to use a Federal Government computer would face prosecution for acts of computer access and use that, while technically wrong, should not rise to the level of criminal conduct.[134]

The legislative history further supports this intent: "The Committee wishes to avoid the danger that every time an employee exceeds his authorized access to his department's computers . . . he could be prosecuted under this

---

[128] *See* Jensen, *supra* note 75, at 96-97; *infra* text accompanying notes 189-202.

[129] 73 AM. JUR. 2D *Statutes* § 83 (2015).

[130] Field, *supra* note 53, at 829-30 (citing *Citrin*, 440 F.3d 417; Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 965-66 (D. Ariz. 2008)); Shurgard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121, 1127-29 (W.D. Wash. 2000)).

[131] *See* S. REP. NO. 99-432 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479; S. REP. NO. 104-357 (1996).

[132] *See* S. REP. NO. 99-432.

[133] *Id.* at 7.

[134] *Id.*

subsection."[135] Congress seemed to think cases where an employee accesses a computer without authorization, but where the conduct was undeserving of criminal liability, should be handled by administrative sanctions, rather than criminal punishment.[136] Additionally, the legislative history hints that Congress was considering a narrower view, as it states that they wished to "preclud[e] liability in purely 'insider' cases."[137]

The House report indicates that the House Judiciary Committee considered the CFAA to be "deal[ing] with an 'unauthorized access' concept of computer fraud rather than a mere use of a computer . . . in committing the offense."[138] This shows that the focus may have been on prohibiting electronic trespassing rather than preventing the misuse of information obtained by accessing the computer.[139] The purpose indicated in the House Report and the intent to narrow the CFAA's scope as indicated in the Senate Report are best served by the code-based approach that limits the definition of "without authorization" to cases where the user's access is blocked by a password.

The legislative history also contains hints that Congress may have intended a broader interpretation of the term "authorization."[140] "The Senate Judiciary Committee's concern about these problems has become more pronounced as computers proliferate in business and homes across the nation and as evidence mounted that existing criminal laws are insufficient to address the problem of computer crime."[141] The Judiciary Committee wanted to develop a statute that would be more effective than pre-existing laws at addressing computer crimes.[142] A broader interpretation furthers this intent by enabling the CFAA to better deal with these crimes.

The Senate Judiciary Committee stated its purpose in drafting the 1996 amendments as "closing gaps in the law to protect better the confidentiality, integrity, and security of computer data and networks."[143] One way it did this was by broadening the CFAA's scope by changing the phrase "federal interest computer" to "protected computer."[144] This simple change expanded the CFAA's jurisdiction to every computer that participated in interstate commerce.[145] The Senate Judiciary Committee not only expressed concern with the way a computer is accessed, but also with the reasons for which it as

135 *Id.*

136 *Id.*

137 *Id.* at 8.

138 H.R. REP. NO. 98-894, at 20 (1984).

139 Shamrock Foods Co. v. Gast, 535 F. Supp. 2d 962, 966 (D. Ariz. 2008).

140 *See* S. REP. NO. 104-357 (1996); S. REP. NO. 99-432.

141 S. REP. NO. 99-432, at 2.

142 *See id.*

143 S. REP. NO. 104-357, at 3.

144 *See id.*

145 *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030 (2012).

accessed.[146] The Committee wanted to impose a stricter penalty in cases where the wrongdoer used his or her access to obtain private information for commercial gain or to commit further crimes.[147] The 1996 amendment was passed to allow the CFAA to apply to insiders who already had access to the computer, rather than limiting its power only to outsiders.[148] These new areas of focus are more suitably addressed by the broader approaches.

Because some of the language used in the committee reports can be taken to support any of the three approaches, they are not particularly helpful in identifying which meaning of "authorization" Congress intended. Looking more generally at the way the CFAA has evolved through its various amendments, however, shows a general trend that supports a broader approach.[149] Since the CFAA first passed in 1986, its subsequent amendments have helped to mold it into a comprehensive computer crime act.[150] The amendments have increased the CFAA's scope by broadening its jurisdiction to cover all "protected computers," as well as improving its ability to address issues where the wrongdoer is an insider who has been granted access to the computer.[151] Although the initial act focused on the way a computer was accessed, the subsequent amendments focused on the purpose of access as well as who accessed the computer.[152] The general trend towards empowering rather than restricting the CFAA shows that a broader approach may align better with the statute's purpose.

---

[146] "This subsection would ensure that the theft of intangible information by the unauthorized use of a computer is prohibited in the same way theft of physical items are protected . . . The crux of the offense . . . is the abuse of a computer to obtain the information." S. REP. NO. 104-357, at 7-8.

[147] "Those who improperly use computers to obtain other types of information . . . face only misdemeanor penalties, unless the information is used for commercial advantage, private financial gain or to commit any criminal or tortious act." *Id.* at 8.

[148] "[T]he prohibition only applies to outsiders who gain unauthorized access to Federal Government computers, and not to Government employees who abuse their computer access privileges to obtain Government information that may be sensitive and confidential." *Id*. at 4 (describing a gap in the existing version of the statute that this amendment was developed to fix). Congress added 18 U.S.C. § 1030(a)(5)(A) which criminalized "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." This provision criminalizes causing damage rather than accessing the computer in order to eliminate the distinction between insiders and outsiders. *See id.* at 11.

[149] *See* S. REP. NO. 104-357; S. REP. NO. 99-432 (1986), *reprinted in* 1986 U.S.C.C.A.N. 2479; H.R. REP. NO. 98-894 (1984), *reprinted in* 1984 U.S.C.C.A.N. 3689.

[150] *See* S. REP. NO. 104-357; S. REP. NO. 99-432; H.R. REP. NO. 98-894.

[151] *See supra* note 146 and accompanying text.

[152] *See* S. REP. NO. 104-357; S. REP. NO. 99-432; H.R. REP. NO. 98-894.

ALTERNATIVE REMEDIES

Another factor we might consider in determining how to interpret "authorization" under the CFAA is whether there are alternative remedies available. Alternative remedies would lessen the need for a broader approach by providing other means of protection should the CFAA fail to cover a specific instance. The potential sources of alternative remedies are other federal criminal and civil statutes, as well as state criminal and civil statutes.

When the CFAA was first passed in 1986, Congress intentionally created it as a separate provision of the Comprehensive Crime Control Act of 1984 instead of adding provisions involving computers to existing criminal statutes.[153] By doing this, Congress was able to create a better fit between the law and the rapidly growing computer crime problem than they would have been able to achieve by amending pre-existing criminal statutes to incorporate computers.[154] Also, computer crimes were all brought together under one statute in order to clearly inform both law enforcement and those who use computers as to which acts were prohibited.[155] Because Congress chose to use the CFAA as the only federal statute governing computer crimes, there are no alternative federal criminal statutes available to provide remedies.

By 1994, the number of computer crime claims had risen so high that the government was unable to prosecute them.[156] As a result, Congress amended the CFAA to allow parties who had suffered harm as a result of a computer crime to bring private suits against the perpetrator and recover civil, legal, or equitable remedies.[157] By allowing private parties to bring suits, Congress ensured that a greater number of CFAA claims were brought to the courts.[158] In passing this amendment, Congress made a conscious decision to broaden the CFAA to cover civil suits involving the victims of computer crimes as well.[159] As with criminal suits, the CFAA has now combined all civil claims by victims of computer crimes under one statute.[160] Therefore, there are no alternative federal civil remedies available to those harmed by violators of the CFAA.

With no available alternative federal statutes, the only other possible remedies for victims of computer crimes are state law statutes. Since Congress

---

[153] *See* Comprehensive Crime Control Act of 1984, Pub. L. No. 98-473, § 1762, 98 Stat. 1976 (1984); *supra* text accompanying notes 6-9.

[154] S. REP. NO. 99-432, at 14; *supra* notes 6-7 and accompanying text.

[155] H.R. REP. NO. 98-894, at 6, 3692; *supra* text accompanying note 9.

[156] *See* 146 CONG. REC. S10, 916 (daily ed. Oct. 24, 2000) (statement of Sen. Patrick Leahy); Jensen, *supra* note 75, at 92.

[157] Computer Fraud and Abuse Act, 18 U.S.C. § 1030(g) (2012); Jensen, *supra* note 75, at 92.

[158] *See* Jensen, *supra* note 75, at 92.

[159] *See* Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 290001, 108 Stat. 1796, 2097-98 (codified as amended at 18 U.S.C. § 1030).

[160] *See* 18 U.S.C. § 1030.

first passed the CFAA in 1986, Congress has repeatedly amended the statute to broaden its scope.[161] One such change occurred in Congress's 1996 amendment that broadened the CFAA's scope from "federal interest computers" to "protected computers," defined as "a computer which is used in or affecting interstate or foreign commerce or communication."[162] Congress understood that the Internet was interstate in nature and that the potential for computer crimes across state lines was great.[163] Congress purposely chose to expand the CFAA's scope using the commerce clause.[164] Because almost every computer today connects to the Internet, the CFAA's scope expands to virtually every computer. As a result, the CFAA preempts state criminal and civil statutes that deal with computer crimes.[165]

Although the CFAA preempts state computer crime statutes, private parties may still bring state tort or contract claims. These claims are not within the same area of law as the CFAA and cover claims distinct enough that they may not be preempted. In one case, the Fourth Circuit, using the narrow approach, dismissed an employer's claim, noting that a broader approach was unnecessary as there were nine possible alternative state law remedies.[166]

Although the existence of alternative remedies lessens the need for a broader approach, the outcome here is inconclusive. In many cases, alternative state law claims may be available; however, this will not always be true and will be specific to each case. There will also be cases where no state law alternative exists. In that case, the victim's only opportunity for a remedy is through the CFAA.

ARGUMENT

All three of the established approaches have merit. However, they also have their shortcomings, preventing any of them from producing a completely

---

[161] *See supra* text accompanying notes 7-27.

[162] *See* 18 U.S.C. § 1030(e)(2)(B); S. REP. NO. 104-357, at 9.

[163] S. REP. NO. 101-544, at 9 (1990).

[164] *Id.* at 6 ("It is the intent of the legislation to exercise the full extent to the powers of Congress under the commerce clause of the United States Constitution . . . to prohibit forms of computer abuse which arise in connection with, and have a significant effect upon, interstate or foreign commerce.").

[165] The Supremacy Clause of the Constitution states "[t]his Constitution, and the laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be made, under the Authority of the United States, shall be the supreme Law of the Land; and the Judges in every State shall be bound thereby, any Thing in the Constitution or Laws of any State to the Contrary notwithstanding." U.S. CONST. art. VI, cl. 2. Preemption, stemming from the Supremacy Clause, is the invalidation of state law when it conflicts with federal law.

[166] WEC Carolina Energy Solutions LLC v. Miller, 687 F.3d 199, 207 n.4 (4th Cir. 2012).

satisfactory result. Courts that are proponents of each of the approaches have made compelling arguments based on the legislative history to indicate that theirs is the interpretation that Congress intended.[167] While each of these approaches does provide us with a satisfactory rule as to when one does not have "authorization," the converse is not true. No single approach gives us a satisfactory rule as to when one *does* have "authorization."

Considering the Code-Based Approach

The code-based approach makes it clear that one is acting "without authorization" when a user circumvents a password or other coded security measure in order to gain access to a computer or the files on it.[168] The purpose of a password is to secure a computer or the data stored on it so that it can only be accessed by those who possess the password. Therefore, it can be inferred that if a person does not know the password, the individual has not received authorization.

The code-based approach breaks down when used as the sole indicator that one has authorization. The facts of *LVRC Holdings LLC v. Brekka* provide a perfect example of why the code-based approach cannot, on its own, define authorization.[169] In this case, LVRC ran a rehabilitation clinic and hired Brekka to oversee several operations.[170] Brekka, who owned and operated two consulting businesses that provided referrals to patients for rehabilitation facilities, used his position with LVRC to gain administrative access to the company's private statistical data.[171] Brekka emailed some of these private files to his personal email account and used the data for his consulting businesses.[172]

Under the code-based approach's interpretation of "authorization," because Brekka had an administrative login and password, he is considered authorized and can continue to access any files on LVRC's website until they change the password.[173] It is an absurd result that an employee may use a company's private files in competition against it and that the company would have no remedy, just because the employee has acquired a password in the course of his employment.[174] While not having a password seems like a good indicator that somebody is not authorized, having one seems like a minimum

[167] Field, *supra* note 53, at 829-30.

[168] *Id.* at 825.

[169] *See supra* notes 64-65 and accompanying text.

[170] LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1129 (9th Cir. 2009).

[171] *Id.*

[172] *Id.* at 1129-30.

[173] *Id.* at 1133, 1135.

[174] *See* Griffin v. Oceanic Contractors, Inc., 458 U.S. 564, 575 (1982) ("[I]nterpretations of a statute which would produce absurd results are to be avoided if alternative interpretations consistent with the legislative purpose are available.").

requirement in determining whether that person actually has authorization.

Considering the Contract-Based Approach

The contract-based approach considers whether an expressed or implied contract dictates the terms of use, and considers the user to be "without authorization" or "exceeding authorization" if they breach the contract.[175] The contract-based approach gives an employer a greater amount of freedom than the code-based approach by allowing them to create specific policies and contracts that define the limits of how its employees are "authorized" to use its computers.

It would be difficult to rely on the contract-based approach exclusively, however. At least one court has affirmed that employers should explicitly state in their contracts which uses they want to forbid.[176] An interpretation that requires the employer to explicitly state which access it wants to prevent may leave it vulnerable. It would be difficult for the employer to determine every specific act it wishes to prohibit in order to include that in its contract.

As a result, employers often fill their contracts with vague language in order to create a broad sense of what types of access are not permitted.[177] The CFAA is a criminal statute that assigns criminal penalties.[178] Therefore, enforcing this vague language through the CFAA may give rise to constitutional concerns involving the notice requirement of due process.[179] Further, an employee may unintentionally breach the terms of a contract if they are not aware that a specific act is prohibited. Breach of contract exposes the defendant to civil liability. Interpreting a criminal statute under the principles of contract law may deprive potential defendants of their freedom through imprisonment, where they would expect the most severe punishment to only be civil liability.[180]

A contract-based approach is only applicable to settings where there are contracts that outline specific and clear rules governing computer use. Situations where a contract is unlikely to be found, such as more personal settings, are unlikely to have enforceable contracts.[181] In personal settings, when one gives permission to use his or her computer, it is unlikely that the

[175] *See* EF Cultural Travel BV v. Explorica, 274 F.3d 577, 581-82 (1st Cir. 2001).

[176] EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 64 (1st Cir. 2003).

[177] *See* Jensen, *supra* note 75, at 117 ("[G]eneric terms prohibiting 'non-business purposes,' or limiting computer use to 'legitimate company business,' provide insufficient notice to employees of what computer use is prohibited.").

[178] Computer Fraud and Abuse Act, 18 U.S.C. § 1030(c) (2012).

[179] *See* Jensen, *supra* note 75, at 117-18.

[180] *Id.*

[181] In order for a contract to be enforceable, it requires an offer, acceptance, consideration, and intent of the parties to be bound. *See* SAMUEL WILLISTON, A TREATISE ON THE LAW OF CONTRACTS (Richard E. Lord ed., 4th ed. 2007).

parties would have valid consideration to form a contract. It is much more likely to be the case that access is granted as a favor, and nothing is given in return. In addition, it is unlikely that any terms of the arrangement would be stated with sufficient specificity to indicate how the person is permitted to use the computer. Furthermore, in a personal setting, it is unlikely that the parties are considering a binding legal relationship, much less intending to be legally bound. In a case such as this, where no contract exists to restrict use, the mere permission to access would give the borrower free reign to use any private files he can acquire.

In practice, the contract approach falls short if used on its own to define "authorization." In order to define "authorization" and "without authorization" through contract, the authorizer would need to list every specific act that is or is not authorized. This is both impractical and, more than likely, impossible. The contract-based approach does, however, provide the authorizer with the opportunity to designate specific acts it wishes to deem "unauthorized" or "exceeding authorization." For this reason, it creates an excellent supplement to defining "without authorization," although it does not succeed on its own.

Considering the Agency-Based Approach

The agency-based approach considers the existence of a legal relationship between the user and the party granting authorization and assesses whether there exists a duty of loyalty that the user has breached.[182] This approach finds the user to be "without authorization" or "exceeding authorization" when they have breached a duty of loyalty owed to the authorizer by serving an adverse interest.[183] The agency-based approach grants the largest amount of protection to employers against the misuse of their devices and confidential information by their employees.[184]

Congress amended the CFAA in 1996 to strengthen it and broaden its scope to better protect confidential information stored on computers by filling gaps left open by the then-existing version of the statute.[185] One of the gaps Congress intended to fill was the CFAA's inability to protect computers from insiders who would already have access to the computer through the course of their employment or other means.[186] The agency-based approach is best suited to meeting this objective as it provides the greatest level of protection against insiders by ending their authorization the moment they use their access to serve an interest adverse to the authorizer.[187] By having a lower requirement to

[182] *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420-21 (7th Cir. 2006).

[183] *Id.* at 421.

[184] Field, *supra* note 53, at 824.

[185] S. REP. NO. 104-357, at 3.

[186] *Id.* at 4.

[187] *See Citrin*, 440 F.3d. at 420-21.

show lack of "authorization" than an explicit term of a contract or circumvention of coded security measures, the agency-based approach is able to carry out the intent of the act more effectively than the other approaches.

The agency-based approach conceptually makes the most sense and is best suited to carry out the purpose of the CFAA. Additionally, it is more logical to focus on the reason a computer is accessed rather than the way it was accessed. It does not make sense that the absence of a computer password or the absence of a contract from the authorizer should make the difference as to whether a wrongdoer's act should be criminalized. The focus for a criminal act should be on the perpetrator and not the victim.

Although the agency-based approach appears to be the ideal solution, it is too broad and may raise due process concerns because the CFAA is a criminal statute.[188]

Constitutional Concerns

The agency and contract-based approaches have received some criticism for evoking potential due process concerns, centering on the void for vagueness doctrine.[189] Under the void for vagueness doctrine as laid out by Justice Sutherland,

[T]he terms of a penal statute creating a new offense must be sufficiently explicit to inform those who are subject to it what conduct on their part will render them liable to its penalties is a well-recognized requirement, consonant alike with ordinary notions of fair play and the settled rules of law. And a statute which either forbids or requires the doing of an act in terms so vague that men of common intelligence must necessarily guess at its meaning and differ as to its application violates the first essential of due process of law.[190]

The void for vagueness doctrine is a two-prong test: a criminal statute should give the public fair notice of which acts are prohibited so that they may act in compliance, and the statute should contain meaningful standards in order to limit the government's use of discretion in applying the statute.[191] A criminal statute that does not meet these two prongs is considered unconstitutionally vague and violates a citizen's due process rights.[192] According to the Supreme Court, "[t]he constitutional requirement of definiteness is violated by a criminal statute that fails to give a person of ordinary intelligence fair notice that his contemplated conduct is forbidden by the statute."[193]

---

188 *See* Jensen, *supra* note 75, at 96-97.

189 *See id.*

190 Connally v. Gen. Const. Co., 269 U.S. 385, 391 (1926).

191 Jensen, *supra* note 75, at 96-97.

192 *Id.*

193 United States v. Harriss, 347 U.S. 612, 617 (1954).

The void for vagueness doctrine raises some constitutional concerns for the agency and contract-based approaches.[194] Neither approach provides a bright line rule by which a citizen could know with certainty which uses they are not "authorized" for. The agency-based approach says that the user's authorization ends when they serve an interest that is adverse to the authorizer's.[195] The determination as to which acts are against the authorizer's interest, however, may be open to judicial discretion.[196]

Although there may be some discretion involved by the user and the court in determining which actions are adverse to the authorizer's interests, the discretion is likely to be minimal as the motive in most cases is clear. Most CFAA cases where the existence of authorization is at issue involve employees who have either misappropriated data for their own use or to serve a new employer, or have destroyed their former employer's data in order to cause them harm.[197] In cases such as this, any person of reasonable intelligence would be aware that they are acting adversely to their employer's interest. One example of this is in *Shugard Storage Ctrs. v. Safeguard Self Storage, Inc.*[198] In this case, an employee of a company that developed storage centers was induced to send competitors secrets while still under the company's employment.[199] The employee knew or should have known that he was no longer serving his employer's interest, thus, little discretion was involved.[200] As another example, in *International Airport Centers, L.L.C. v. Citrin*, Citrin loaded software onto his borrowed computer in order to delete the evidence of improper conduct he had engaged in during the course of his employment.[201] Citrin must have known his conduct was adverse to the company's interests, otherwise he would not have attempted to delete these files.[202]

Additionally, the contract-based approach may raise due process concerns when the governing contract provides language which only vaguely suggests the types of acts which are prohibited; for example, a confidentiality agreement that only suggests that employees should not share trade secrets. These concerns may be mitigated by strictly requiring the author to outline specifically which acts it wishes to prohibit.

---

194 *See* Jensen, *supra* note 75, at 96-97.

195 *See* Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 421 (7th Cir. 2006).

196 *See* Jensen, *supra* note 75, at 116-17.

197 *See* Shugard Storage Ctrs., Inc. v. Safeguard Self Storage, Inc., 119 F. Supp. 2d 1121 (W.D. Wash. 2000).

198 *Id.*

199 *Id.* at 1123.

200 *See id.*

201 Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006); *supra* text accompanying notes 118-25.

202 *See Citrin*, 440 F.3d. at 419.

A Hybrid Approach

Each of the approaches described above does an excellent job of defining when someone is "without authorization," however, none of these approaches does a satisfactory job of defining "authorization" when used on its own. The best approach to analyzing "authorization" would be one that takes all of the benefits from each of the established approaches, while minimizing any potential drawbacks.

A suitable test encompassing all three approaches can be inferred using a simple syllogism.[203] Any person who accesses a computer is either authorized or without authorization. To be without authorization, one must either have bypassed coded protections, violated the terms of an explicit contract, or acted contrary to the interest of his employer. Therefore, if one is not bypassing a coded protection, violating the terms of an explicit contract, or acting contrary to the interests of his employer, then that person is "authorized."

This approach would consist of a tripartite test, whereby if the defendant is found to be "unauthorized" under any of the three factors, then he is without authorization. On the other hand, if the defendant is not found to be "unauthorized" under any of the factors, then he will be considered "authorized." This gives a plaintiff who is suing under the CFAA three chances to show that the defendant is "unauthorized." Each of the three established approaches makes up one factor of the test. Using this tripartite test, a court would first apply the code factor, where a defendant is found to be unauthorized if he bypassed coded security in order to gain access. If the defendant did not have to bypass security, then the court should look at the second factor: the contract factor. Under this factor, the court will examine any existing contracts dictating the terms of use. A defendant is unauthorized if he breaches the terms of the contract stating what is or is not permitted. If the defendant has not breached any terms of an explicit contract, the court will then examine the agency factor. The court will determine whether the relationship between the authorizer and the user imposes a duty of loyalty on the user, and whether the user has breached that duty by using the computer for a purpose that is adverse to the interests of the authorizer. If he has not, he will be considered authorized. If, however, the defendant is found to have violated any of these three factors, then he will be considered "without authorization."

This new test is able to combine the benefits of the existing approaches, while minimizing the drawbacks. Similar to the code-based approach, the first factor of this test provides a clear rule for a minimum barrier to authorization. This clear rule gives proper notice to any potential defendant who bypasses

[203] A syllogism is a logical argument where a conclusion is inferred from two or more premises. Aristotle created the famous example: All mortals die, all men are mortals, therefore all men die. MERRIAM-WEBSTER, http://www.merriam-webster.com/dictionary/syllogism (last visited June 14, 2015) (archived at http://perma.cc/Z9RD-D46D).

coded security in order to gain access. At the same time, this test does not contain the same limitation that the code-based approach would have on its own. In a case where there is no coded security, the authorizer is not left vulnerable. The authorizer may still show the user was without authorization or exceeding their authorization under the second or third prong of the test. The authorizer may have a contract with the user that specifies limits on authorization, or the user's actions may be found to be hostile to the interests of the authorizer.

By using the code-based approach as only a single factor in a tripartite test, the limitations of the code-based approach seen in *Brekka* are eliminated.[204] In *Brekka*, the employer was left without remedy when Brekka used the password he acquired as an employee to access and misappropriate confidential data for his own business.[205] Under this new test, although Brekka had a password, and therefore passed the first part of the test, it would be easy to find him to be "unauthorized" under a different part, such as the agency or contract prongs of the test.[206] It would be easy for an employer to include a clause in its employment contract restricting the way in which its employees may use the information on the computers to which they are given the passwords. Even if the employer does not include a clause in its employment contract, the employee may still be found to be unauthorized under the agency prong. In a case such as *Brekka*, the agency prong would easily find the employee to be unauthorized under this type of act because it is clearly adverse to the authorizer's interest, as it allowed Brekka to go into competition against his former employer.[207]

The second factor in the test has all of the benefits of the contract-based approach. This factor gives the authorizer the opportunity to specifically designate the ways in which they do not want their computers or the confidential information stored on them to be used. By including the contract-based approach as just one factor, the authorizer can choose specific restrictions without limiting the extent of their protection to those restrictions. As a result, the authorizer is less likely to include broad language that fails to give the defendant notice of when they are breaching the terms of the contract.

In applying the test, it would make the most sense, in light of the other prongs, to construe the contract factor narrowly. Only prohibitions that are written in an explicit contract should be considered for this prong. Courts should not consider any vague language when applying the contract factor, although this vague language may be useful when considering the agency factor. Considering only explicit prohibitions written into a contract or widely

---

[204] *See* LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1133 (9th Cir. 2009); *supra* text accompanying notes 173-74.

[205] *See Brekka*, 581 F.3d at 1129.

[206] *See id.*

[207] *See id.*

known and well-advertised company-wide policies ensures that the notice requirement of due process is satisfied.

By including the contract-based approach as a single factor, situations such as personal interactions, where there are no enforceable contracts, are not left without protection. These cases can still be protected by the code and agency factors. In personal interactions, where one person allows another to borrow a computer as a favor, for example, any personal and private files that are stored on the computer can still be protected from misappropriation by password protecting them. Under this test, the non-existence of an enforceable contract does not eliminate protection.

The test's third factor is applicable when the first two prongs of the test have not found the user to be without authorization. Under the agency factor, the authorizers do not need to worry about the lack of protection against the misuse of their machines due to the technicalities of the code factor and the contract factor. The agency factor acts as a catchall and protects against any use that is adverse to the authorizer's interests. Because of this, the agency prong acts as the backbone of this hybrid approach.

As with the contract factor, the agency factor will focus on the purpose, rather than the means of access. Under this factor, the court will ask whether the user has accessed the computer for a purpose that is adverse to the interests of the authorizer. If the purpose of access is adverse to the authorizer's interests, the court will find the user to be without authorization.

The hybrid approach recognizes the agency-based approach as the best individual method for interpreting "authorization." The agency factor is the third factor in the test and will always be used if the first two factors do not find the user to be unauthorized. The hybrid approach differs from the agency-based approach in that it recognizes that a narrower interpretation, which is easier to follow and provides clearer rules, is better to use when possible. The hybrid approach uses the code-based and contract-based approaches to give courts guidance in interpreting "authorization" and only leaves interpretation to the court's discretion as a last resort, when these rules fail.

The tripartite test helps to mitigate due process concerns when a defendant is found to be unauthorized under the code or contract prongs. The code and contract factors provide means of giving fair notice and limiting discretion before the agency factor is even considered. In cases where the agency factor is applied, although due process concerns cannot be completely eliminated, they should be minimal as it is usually clear when the user is serving an interest that is adverse to the employer's. The very acts of destroying or misappropriating the employer's confidential data are inherently adverse to the employer's interest. Thus, there is little danger of lack of fair notice or overuse of discretion involved in the use of this factor.

The agency factor of the hybrid approach brings this approach into alignment with Congress's intent, indicated by the general trends in the

CFAA's various amendments.[208] Congress has continued to amend the CFAA with the purpose of strengthening it, and the hybrid approach fits with this purpose.[209] One of the biggest changes in the 1996 amendment was adding the ability to protect computers and the data stored on them from insiders.[210] A hybrid approach that contains the strength of the agency approach is the best equipped to protect against misuse by insiders, and is consistent with the purpose of the 1996 amendment.[211] Using this approach, holdings such as the one in *Brekka* would be avoided, and the CFAA would be more effective in granting companies such as LVRC Holdings a remedy against their treacherous employees.[212]

The hybrid approach also reflects Congress's focus in its later amendments on the purpose for which a computer is accessed, rather than the way in which it is accessed.[213] By using the agency factor as its backbone, the hybrid approach also focuses on the purpose for which the computer is accessed. The hybrid approach uses the code factor and the contract factor to help determine what the employer's interests are, and then uses the agency factor to determine whether the employee has intentionally acted adversely. If the user accessed the computer for a purpose adverse to the authorizer's interests, they can be found liable under the Act. Under this approach, the way in which a computer is accessed, such as whether the user needed to circumvent a password, is secondary and serves primarily as an indication as to whether the user was acting contrary to the authorizer's interests. The hybrid approach's focus on purpose, rather than means of access, aligns it with the amended CFAA's purpose, while continuing to consider means of access as an indication of that purpose.

CONCLUSION

Because of the nature of language, it is impossible to draft a statute that is completely free from ambiguity. The word "authorization" as used in the CFAA is no different. Without a clear definition of the word, everyone who reads the statute will interpret it differently. It is for this reason that courts have adopted different approaches to interpreting the CFAA. In order to apply the law equally to all, a common approach to interpreting the statute must be found. The issue becomes which interpretation is correct.

The hybrid approach proposed in this note is more effective than any of the

---

[208] *See supra* text accompanying notes 149-52.

[209] *Id.*

[210] *See* Computer Fraud and Abuse Act, 18 U.S.C. § 1030(a)(5)(A) (2012); S. REP. NO. 104-357, at 6.

[211] *See* S. REP. NO. 104-357, at 3.

[212] *See Brekka*, 581 F.3d 1127; *supra* text accompanying notes 63-67.

[213] *See* S. REP. NO. 104-357, at 8; *supra* text accompanying notes 149-52.

three main approaches the courts have used because it combines the benefits of each approach, while counterbalancing each of their drawbacks. The hybrid approach focuses on the purpose for which a computer is accessed, rather than how it is accessed. This not only aligns with Congress's intent for the CFAA but also makes a more effective statute at addressing computer crimes.