Brooklyn Law Review

Volume 82 | Issue 4 Article 10

1-1-2017

Cannibal Cop Out: The Computer Fraud and Abuse Act, Lenity, Quasi-Strict Liability, Draconian Punishment and a Surgical Solution

Charles S. Wood

Cannibal Cop Out

WHY LENITY IS A NECESSARY, YET UNWORKABLE SOLUTION IN INTERPRETING THE COMPUTER FRAUD AND ABUSE ACT

INTRODUCTION

In a mere handful of decades, computers have facilitated unprecedented access to digital information. As this swell of available data increasingly includes the most sensitive personal information, regulation is needed to shield the public from the opportunistic machinations of bad actors. The Computer Fraud and Abuse Act (CFAA),[1] was Congress's response to criminal activity via computer, criminalizing the illicit access of digital information. As with many pieces of new legislation, the CFAA ushered in a melee of judicial interpretation. In a range of cases tackling the nuances of the CFAA, even the tamest of phrases were subject to varying judicial interpretations, leading to strikingly different results. When such conflicting results concern something as central to contemporary life as computers, it represents potentially nationwide repercussions.

In a two-to-one decision in *United States v. Valle*, the Second Circuit determined the meaning of "exceeds authorized access" as defined in the CFAA to be ambiguous, and therefore, after applying the rule of lenity, adopted the narrow interpretation that the phrase only applies to users who access information outside of the scope of their authorization.[2] This was chosen over the broader view, which would extend the meaning of the phrase to users who access otherwise authorized information for an improper use.[3] Arguably, however, both interpretations are problematic. Under the narrow view's adoption of lenity—excluding an improper, but otherwise authorized access from the "exceeds authorized access" analysis[4]—arguably any use that

---

[1] 18 U.S.C. § 1030(a) (2012).

[2] United States v. Valle, 807 F.3d 508, 523–28 (2d Cir. 2015).

[3] *Id.* at 523–28; *see* 18 U.S.C. § 1030(a).

[4] *See Valle*, 807 F.3d at 527–28 (Second Circuit applying lenity and reversing the district court's verdict that Valle had exceeded his authorized access by

"exceeds authorized access" in essence becomes "unauthorized." This therefore renders the "exceeds" language redundant, thereby leaving a blind spot in the CFAA regarding fraudulent access to information by otherwise authorized users. In contrast, under the broader view, the CFAA would essentially criminalize any violation of a computer use policy—even restrictions imposed by terms of service that users do not know about.[5] In deciding *Valle*, the Second Circuit joined the Fourth and Ninth Circuits in a canyon-like circuit split against the First, Fifth, Eighth, and Eleventh Circuits which hold the broader view that violations of usage restrictions are within the scope of "exceeds authorized access."[6] As the resolution of this split could affect all the nation's computer usage, should we favor more narrow protections at the expense of enforceability, or broader protections that could result in a tidal wave of accidental liability?

Valle represents perhaps the most colorful fact pattern out of the cadre of cases in the split. The defendant in *Valle,* nicknamed "cannibal cop," was a New York Police Department officer who used credentialed access to a government database in order to obtain information about the subjects of his cannibalistic sexual fantasies.[7] He was tried and convicted by a jury for conspiracy to kidnap and for violation of the CFAA by exceeding his authorized access to the databases from which he obtained the information.[8] The district court reversed the conspiracy verdict, but affirmed the charge under the CFAA.[9] On appeal, a two-to-one majority reversed Valle's conviction under the CFAA, holding that the ambiguous language of the statue, and the credibility of both interpretations, required the invocation of the rule of lenity and the statute therefore had to be narrowly tailored in the defendant's favor.[10] Under this narrow

---

improperly using the database he was otherwise authorized to use, therefore eliminating an improper use analysis).

[5] United States v. Nosal, 676 F.3d 854, 858, 860–62 (9th Cir. 2012).

[6] For the cases in the split adopting the narrow interpretation, see *Valle*, 807 F.3d 508; *Nosal*, 676 F.3d 854; and WEC Carolina Energy Sols., LLC. v. Miller, 687 F.3d 199 (4th Cir. 2012). For the cases in the split adopting the broad interpretation, see United States v. Teague, 646 F.3d 1119 (9th Cir. 2011); United States v. John, 597 F.3d 263, (5th Cir. 2010); United States v. Rodriguez, 628 F.3d 1258 (11th Cir. 2010); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418 (7th Cir. 2006); and EF Cultural Travel BV v. Explorica, 274 F.3d 577 (1st Cir. 2001).

[7] *See* Benjamin Weiser, *Prosecutor in "Cannibal Cop" Case Asks Appeals Court to Reinstate Conviction*, N.Y. TIMES (May 12, 2015), https://nyti.ms/2vx1GVO [http://perma.cc/E5M6-DSXX]; *see also* Joseph Goldstein, *Officer Plotted to Abduct, Cook and Eat Women, Authorities Say*, N.Y. TIMES (Oct. 25 2012), https://nyti.ms/2vx9cjC [http://perma.cc/7WMP-K2N8] (describing the facts that led to Valle's arrest).

[8] *Valle*, 807 F.3d at 512–13.

[9] *Id.* at 513, 515 (citing United States v. Valle, 301 F.R.D. 53, 111, 113 (S.D.N.Y. 2014)).

[10] *Id.* at 523–28.

interpretation, since Valle possessed the technical credentials to access the information, the CFAA was inapplicable.[11] An impassioned dissent argued that the text of the CFAA was unambiguous, therefore the rule of lenity was irrelevant, and that Valle's conviction under the CFAA should not have been reversed.[12]

This note first argues that the Second Circuit was correct in applying lenity to the phrase "exceeds authorized access"[13] due to the logical validity of both the narrow and broad interpretations. Second, this note argues that under the narrow view's application of lenity, all use that "exceeds authorized access" essentially becomes "unauthorized," rendering the language superfluous. In contrast, under the broad interpretation, Section (a)(2) opens the door to arbitrary and draconian enforcement. Therefore, the prudent solution to suture the split would be for the legislature to remove liability for a use that "exceeds authorized access" under Section (a)(2) in the event the conduct would only receive the minimum punishment under (c)(2)(A).[14] As this would resolve the narrow view's concern over the potential for arbitrary absurdity, it could then release the improper use analysis from the jaws of lenity, thereby restoring uniformity to the interpretation of the "exceeds" prong.

Part I of this note gives a primer on the birth and evolution of the CFAA in reference to the "exceeds" prong. Part II then details the diverging interpretations of the phrase within the circuits of the split. Narrowing the focus to *United States v. Valle*, Part III discusses the facts of the case, as well as the majority and dissenting opinions. Picking a side, Part IV argues that the Second Circuit was correct in applying lenity in *Valle* due to the inherent ambiguity of the exceeds prong. Finally, Part V contends that in order for Congress to conjure a workable solution to reconcile the fifteen-year-old split, liability should be omitted as a use that "exceeds authorized access" under Section (a)(2) until the conduct reaches the threshold for the second tier of punishment under Section (c)(2)(B). This alteration would remove the section's vast potential for arbitrary and possibly unjust enforcement, thereby allowing for

---

[11] *Id.*

[12] *Id.* at 537–40 (Straub, J., dissenting).

[13] As defined in the CFAA, "the 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." 18 U.S.C. § 1030(e)(6) (2012).

[14] *Id.* § 1030(c)(2)(A) (Under this minimum tier of punishment for section (a)(2), simply the act of accessing a computer in excess of one's authorized access will trigger liability, subjecting the offender to one year in jail, a fine, or both.).

the broad view's improper use analysis under the exceeds prong throughout the rest of the statute.

I. THE INCEPTION AND EVOLUTION OF THE COMPUTER FRAUD AND ABUSE ACT

The CFAA came to be as a response to computer crime, and has been continuously reshaped and reconsidered as computers have evolved from a novel invention to a necessary tool used for navigating the modern world. This part examines the Act from "crib" to present, and how it has continuously been molded by ever-changing policy concerns, as well as the need for the government to wield some form of policing power over the unruly and amorphous connectivity of information in the digital world.

A. History of the Act

Congress has continuously broadened the scope and coverage of the Computer Fraud and Abuse Act since its original enactment. Reflecting on the history of the Act's expansion, the Senate Report on the 1996 amendments noted:

> As intended when the law was originally enacted, the Computer Fraud and Abuse statute facilitates addressing in a single statute the problem of computer crime . . . . As computers continue to proliferate in businesses and homes, and new forms of computer crimes emerge, Congress must remain vigilant to ensure that the Computer Fraud and Abuse statute is up–to–date and provides law enforcement with the necessary legal framework to fight computer crime.[15]

In response to the increasing rate of computer crime, Congress enacted the Counterfeit Access Device and Computer Fraud and Abuse Act, entitling 18 U.S.C. § 1030 "Fraud and related activity in connection with computers."[16] The act originally only protected a narrow category of government computers, or those used in financial institutions, criminalizing "computer misuse to obtain national security secrets, computer misuse to

---

[15] Deborah F. Buckman, Annotation, *Validity, Construction, and Application of Computer Fraud and Abuse Act (18 U.S.C.A. § 1030)*, 174 A.L.R. Fed. 101 (2001) (omission in original) (quoting S. REP. NO. 104-357, at 5 (1996)).

[16] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92 (codified as amended at 18 U.S.C. § 1030 (2012)); *see* H.R. REP. NO. 98-894, at 2 (1984); S. REP. NO. 99-432, at 16 (1986).

obtain personal financial records, and hacking into U.S. government computers."[17]

Access and authorization were defined as: "knowingly accesses a computer without authorization, or having accessed a computer with authorization, uses the opportunity such access provides for purposes to which such authorization does not extend."[18] The conduct was analogized to "breaking and entering," with Congress stating the act "deals with an 'unauthorized access' concept of computer fraud rather than the mere use of a computer."[19] However, "[t]he 1984 Act had a couple of loopholes, or scenarios not accounted for: 1) *authorized persons* causing harm to protected computer systems; and 2) unauthorized persons who gave codes or software to authorized persons who loaded them into their computers."[20] Essentially foreshadowing the current split, these loopholes could have been exploited by users who abused otherwise authorized access for nefarious purposes.

In 1986, Congress enacted the Computer Fraud and Abuse Act to amend the 1984 version.[21] Congress amended the "knowingly" requirement to "intentionally" in order to prevent an accidental violation by someone "who *inadvertently* 'stumble[s] into' someone else's computer file or computer data."[22] Additionally, the reach of the statute was extended to private computers under the addition of the new category "Federal Interest Computer," expanding on the original requirement that the subject computer must have been used by a financial institution or the U.S. Government to include, "one of two or more computers used in committing the offense, not all of which are located in the same State."[23] The proscribed conduct was still analogized to thievery via computer.[24] Therefore, two fundamental differences between the original and the 1986 amendment were a stricter scienter[25] requirement coupled with

---

[17] Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563–64 (2010); *see* Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 § 2102(a), 98 Stat. at 2190–92.

[18] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984 § 2102(a), 98 Stat. at 1290–91. This is the primordial form of the exceeds prong.

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

[20] Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1194 (E.D. Wash. 2003) (emphasis added) (citing Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, § 2012(a), 98 Stat. at 2190).

[21] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99–474, 100 Stat. 1213.

[22] S. REP. NO. 99-432, at 6 (emphasis added).

[23] Computer Fraud and Abuse Act of 1986, § 2, 100 Stat. at 1213–15.

[24] S. REP. NO. 99-432, at 9.

[25] "A degree of knowledge that makes a person legally responsible for the consequences of his or her act or omission; the fact of an act's having been done knowingly, esp. as a ground for civil damages or criminal punishment." *Scienter*, BLACK'S LAW DICTIONARY (10th ed. 2014).

a substantial expansion to the category of computer covered by the CFAA.

Most significantly, the 1986 Act included the current language of "exceeds authorized access," reading: "the 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."[26] In Congress's own words, the exceeds language was used to replace its previous form to remove "one of the *murkier grounds of liability*, under which a Federal employee's access to computerized data might be legitimate in some circumstances, but criminal in other (not clearly distinguishable) circumstances that might be held to exceed [their] authorization."[27] This represents an acknowledgement of ambiguity as to when an authorized, yet illegitimate, use would be considered a crime in the then-fledgling statute.

The CFAA was again amended in 1994 as part of the Violent Crime Control and Law Enforcement Act of 1994, under the smaller subsection titled the Computer Abuse Amendments Act of 1994.[28] Most notably, the amendments extended the scope of the previously criminal-only CFAA to allow for a private cause of action.[29] This not only represented another large expansion of the CFAA but also opened the door for an onslaught of private litigation.

The CFAA was amended yet again by the Economic Espionage Act of 1996, under the subsection the National Information Infrastructure Protection Act of 1996.[30] These amendments represent one of the largest expansions to the CFAA, criminalizing any type of unauthorized (or in excess of authorization) access to information on a computer "if the conduct involved an interstate or foreign communication."[31] These amendments were coupled with a drastic expansion to the definition of computers under the protection of the CFAA, replacing "Federal interest" computer with "protected" computer, covering any computer "which is used in interstate or foreign commerce or communication."[32] This eliminated the previous

---

[26] § 2, 100 Stat. at 1213–15; *accord* 18 U.S.C. § 1030(e)(6) (2012).

[27] S. REP. NO. 99-432, at 21 (emphasis added).

[28] Violent Crime Control and Law Enforcement Act of 1994, Pub. L. No. 103-322, § 290001, 108 Stat. 1796, 2097–99.

[29] *See* 18 U.S.C. § 1030(g) (2012).

[30] Economic Espionage Act of 1996, Pub. L. No. 104-294, § 201, 110 Stat. 3488, 3491–94.

[31] *Id.* at 3492.

[32] *Id.* at 3493.

requirement that the offense be committed on two or more computers in different states.[33]

The Identity Theft Enforcement and Restitution Act of 2008, as found within the Former Vice President Act of 2008,[34] brought the CFAA to its current form and showcased yet another hefty expansion—although one would need a magnifying glass to see the change in language.[35] The act removed the requirement that the illegal access of a "protected computer" include some form of an interstate communication under 18 U.S.C. § 1030(a)(2), thereby allowing for purely intrastate liability.[36] Secondly, the definition of "protected computer" was subtlety expanded to include computers "used in . . . [or] *affect[ing]* interstate or foreign . . . communication."[37] In layman's terms, the statute would now include basically any computer with Internet access regardless of whether it was actually used in interstate communication due to the total lack of borders in digital communication.[38]

The CFAA has evolved from a statute prohibiting the unauthorized access of information from a government computer, to criminalizing, as well as providing a private cause of action for, the access of information from any computer with Internet access, that is unauthorized, or in excess of authorization.

B. The Current CFAA

As noted above, the CFAA has continuously expanded the group of computers that fall under its protection, with the current definitions being the most expansive to date.[39] The current CFAA defines a computer as "an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device."[40] This definition has includes cellular telephones,[41] as well as computer-based radio systems.[42] It does, however,

---

[33] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99–474, 100 Stat. 1213, 1215.

[34] Former Vice President Act of 2008, Pub. L. No. 110-326, §§ 203-09, 122 Stat. 3560, 3560–65 (2008).

[35] *See* Kerr, *supra* note 17, at 1569–70.

[36] § 203, 122 Stat. at 3561.

[37] 18 U.S.C. § 1030(e)(2)(B) (2012); *see* § 207, 122 Stat. at 3563 (emphasis added).

[38] *See* discussion *infra* Section I.B.2.

[39] *See* discussion *supra* Section I.A.

[40] 18 U.S.C. § 1030(e)(1).

[41] *See* United States v. Kramer, 631 F.3d 900 (8th Cir. 2011).

[42] *See* United States v. Mitra, 405 F.3d 492, 496 (7th Cir. 2005).

expressly exclude "automated typewriter[s] . . . portable hand held calculator[s], or [any] other similar device[s]."[43]

The CFAA defines a protected computer as either one used by a "financial institution or the United States Government" or, by drawing on the full power vested to Congress through the Commerce Clause of the Constitution,[44] one "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."[45] Under this second definition, a protected computer becomes any computer (as defined under the CFAA) with access to the Internet.[46]

Now that the term "computer" has been explained in the context of the CFAA, how does one access it in excess of authority? As defined in the text of the CFAA—and as noted in this note's introduction—"the 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."[47] In the sections of the CFAA enumerating criminal conduct, "exceeds authorized access," is always found directly following the term "without authorization."[48] For the purposes of the analysis to follow, the first half of this clause will be referred to as the "unauthorized prong," and the other as the "exceeds prong." "Unauthorized" is not a defined term in the CFAA, but the term "authorization" has consistently been given its plain, everyday meaning when interpreting the unauthorized prong.[49] It is important to note that the exceeds prong only applies to certain offenses under the statute, with several provisions only applying exclusively to users with a total lack of authorization.[50] Congress's motive behind this

---

[43] 18 U.S.C. § 1030(e)(1).

[44] "The Congress shall have Power To . . . regulate commerce with foreign nations, and among the several States." U.S. CONST. art. 1, § 8, cl. 3.

[45] 18 U.S.C. § 1030(e)(2).

[46] *See* United States. v. Nosal, 676 F.3d 854 (9th Cir. 2012); United States. v. Yücel, 97 F. Supp. 3d 413 (S.D.N.Y. 2015). This could possibly also include smartwatches, modern cars, modern videogame systems, cable boxes, etc.

[47] 18 U.S.C. § 1030(e)(6).

[48] *Id.* § 1030 (a)(1) ("without authorization or exceeding authorized access"); *id.* (a)(2) ("without authorization or exceeds authorized access"); *id.* (a)(4) ("without authorization, or exceeds authorized access"), *id.* (a)(7)(B) ("without authorization or by exceeding authorized access").

[49] *See* United States v. Morris, 928 F.2d 504, 511 (2d Cir. 1991). The plain, everyday meaning of authorize is defined as to "approve, consent to[,] . . . permit, allow, license, entitle, [or] empower." *Authorize*, THE OXFORD DESK DICTIONARY AND THESAURUS 47 (Frank R. Abate ed., American ed. 1997).

[50] 18 U.S.C. § 1030(a)(3), (5)(A).

was to differentiate "insiders, who are authorized to access a computer," and "outside hackers who break into a computer."[51]

The exceeds prong appears in Sections (a)(1), (2), (4), and (7)(B).[52] Section (a)(1) prohibits the access of confidential government information.[53] Section (a)(2) prohibits the access of information on, among other things, a protected computer.[54] Section (a)(4) prohibits the access of a protected computer in furtherance of a fraud, resulting in the obtainment of anything under $5000.[55] Section (a)(7)(B) prohibits extortion involving a threat to a protected computer.[56] Sections (a)(1), (4), and (7)(B) all require that the offender specifically access the information in conjunction with a malicious purpose,[57] while in (a)(2), the mere intent to access is enough to trigger liability.[58] Simply put, every instance of "exceeds authorized access," aside from (a)(2), is contained in a section enumerating a specific offense—i.e., theft of national secrets, fraud, or extortion—whereas (a)(2) only involves the access of a computer.[59] Looking specifically at Section (a)(2) of the statute, the CFAA attaches liability to:

> (a) Whoever—
>
> . . . .
>
> (2) intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains—
>
> (A) information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act;

---

[51] S. REP. NO. 104–357, at 11 (1996); *see also* S. REP. NO. 99–432, at 7 (1986) (discussing choice not to use exceeds prong in certain violation, stating "[a]t the same time, the Committee was required to balance its concern for Federal employees and other authorized users against the legitimate need to protect Government computers against abuse by 'outsiders.'").

[52] 18 U.S.C. § 1030(a)(1), (2), (4), (7)(B) (These sections detail the conduct criminalized by the CFAA.). The phrase also appears in Sections (e)(6) and (e)(10). *Id.* § 1030(e)(6), (10) (These sections detail the definition of the phrase, as well as the statute's definition of conviction.).

[53] *Id.* § 1030(a)(1).

[54] *Id.* § 1030(a)(2).

[55] *Id.* § 1030(a)(4).

[56] *Id.* § 1030(a)(7).

[57] *Id.* § 1030(a)(1) (intentional procurement of confidential government information); *id.* § 1030(a)(4) (in furtherance of intended fraud, assisting in the obtainment of an object of over $5000 in value); *id.* § 1030(a)(7)(B) (intent to commit extortion).

[58] *Id.* § 1030(a)(2) (mere intent to access in order to obtain information).

[59] *Id.* § 1030(a)(1), (a)(4), (a)(7); *compare* 18 U.S.C. § 1030(a)(2).

> (B) information from any department or agency of the United States; or
>
> (C) information from any protected computer.[60]

After a violation of the CFAA, what kind of punishments can be expected? Under the current form of the CFAA, violations of Section (a)(2) are subject to a three-tiered sentencing system.[61] The lowest tiered offense, yet the most problematic in the eyes of those crying lenity, is Section (c)(2)(A), which calls for a fine, a year in prison, or both, for a violation or attempted violation of Section (a)(2).[62] Second in the batting order, and in this author's opinion, the most logical approach to liability due to the requirement of motive or minimum value to the information obtained, is Section (c)(2)(B), which calls for a fine, five years in prison, or both, for a completed or attempted violation of Section (a)(2), if "committed for purposes of commercial advantage or private financial gain[,] . . . committed in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State," or "the value of the information obtained exceeds $5,000."[63] Finally, under Section (c)(2)(C), one who commits, or attempts to commit a violation of Section (a)(2) after a previous conviction under (c)(2)(A) or (B), will face a fine, ten years in prison, or both.[64]

As Section (a)(2) and its lowest tier of punishment only require the intent to "access[] a computer without authorization or [in excess of] authorized access," instead of requiring a malicious purpose, or even an intent to obtain information, it could therefore be viewed as a type of quasi-strict liability.[65] The word "quasi" is used as there is still the hurdle of intending to access the computer, therefore precluding cases of purely accidental access (which in this author's opinion, could push the section into strict liability territory). This type of quasi-strict liability, when paired with the immensely broad

---

[60] *Id.* § 1030(a)(2) (internal citation omitted).

[61] *Id.* § 1030(c)(2).

[62] *Id.* § 1030(c)(2)(A). Also included are violations of Sections (a)(3) and (6). *Id.* § 1030(c)(2)(A).

[63] *Id.* § 1030(c)(2)(B).

[64] *Id.* § 1030(c)(2)(C). Again, violations of Sections (a)(3) and (6) are also included. *Id.* at § 1030(c)(2)(C).

[65] *Id.* § 1030(a)(2), (c)(2)(A). *Black's Law Dictionary* defines strict liability as "[l]iability that does not depend on proof of negligence or intent to do harm but that is based instead on a duty to compensate the harms proximately caused by the activity or behavior subject to the liability rule." *Strict Liability*, BLACK'S LAW DICTIONARY (10th ed. 2014). For a hypothetical example of this alleged quasi-strict liability, see *infra* Part II.

definition of "protected computer," appears to be the lynchpin in several circuits' application of lenity to the statute.[66]

II. CIRCUIT SPLIT SCORECARD: THE NARROW, THE BROAD, AND THE UGLY

Steve Strawman, an engineer at Hypothetical Inc., lives in a jurisdiction that follows the narrow view of the exceeds prong. Steve, using his unique password and username to access the company server (to be used for work purposes only), accesses and downloads client contact information to sell to Hypothetical Inc.'s main competitor. As Steve had access to the company server, his improper use would not exceed his authorized access under the narrow view. Steve would only have exceeded his authorized access under the narrow view if some form of internal circumvention was required to access the client list to which his current credentials did not pass muster.[67]

On the other hand, say Steve Strawman instead lives in a jurisdiction that follows the broad view. This time he accesses and downloads the client list merely to send out invitations to a dinner party. As per his employee agreement, however, Steve was only allowed to access this list in the course of his professional duties. As this action was in clear violation of the usage restrictions set by Hypothetical Inc., Steve has exceeded his authorized access under the broad view's interpretation of the exceeds prong. He would therefore be in violation of the CFAA.[68] These two hypotheticals showcase the key difference between the competing interpretations of the circuit split.

A. The Narrow View—Internal Virtual Trespass

The Fourth and Ninth Circuits have embraced the narrow view of the exceeds prong, requiring the potential offender to circumvent a system and access material he is generally not cleared to view in order to violate the CFAA. In the familiar case of an ex-employee utilizing proprietary information, the Fourth Circuit veered toward the narrow view in *WEC Energy Solutions LLC v. Miller*.[69] The defendant downloaded and emailed to himself proprietary information from databases, to which he had authorized access, in order to make a presentation on behalf of a competitor, in clear violation of the plaintiff's prohibition on

---

[66] *See* discussion *infra* Section I.B.3.
[67] *See* discussion *infra* Section II.A.
[68] *See* discussion *infra* Section II.B.
[69] WEC Energy Sols. LLC v. Miller, 687 F.3d 199, 201 (4th Cir. 2012).

such usage.[70] The defendant was alleged to have, among other things, exceeded his authorized access to a protected computer under Section (a)(2)(C) of the CFAA.[71]

In its opinion, the court acknowledged that "two schools of thought exist," (referencing the narrow and broad view) and chose to apply lenity even though it was civil case.[72] The court noted that because the CFAA involves "both civil and criminal application," their reasoning would have to "appl[y] uniformly in both contexts," therefore recognizing that in a criminal context, the exceeds prong was ambiguous enough to mandate lenity.[73] Therefore, under the Fourth Circuit's interpretation, a violation of usage restrictions would fail to trigger the exceeds authorized access prong under the CFAA, instead a violation would only occur "when [one] has approval to access a computer, but uses [their] access to obtain or alter information that falls outside the bounds of [their] approved access."[74] The defendant therefore had no liability under the CFAA for his improper use, as the court noted, to the "disappoint[ment] [of] employers hoping for a means to rein in rogue employees."[75]

In yet another case of employers attempting to use the CFAA as a weapon against a former employee's access of proprietary information through credentialed access for an improper use, the Ninth Circuit determined Section (a)(2) to not be the appropriate vehicle for relief.[76] Among other things, the plaintiff's complaint alleged the defendant's violation of Section (a)(2) of the CFAA.[77] The plaintiff, an addiction treatment center, hired the defendant (who owned several companies performing referrals for businesses similar to plaintiff's) to help oversee certain operations, one of which included interacting with a third party who provided computer services to plaintiff.[78] In the course of his duties, the defendant received administrative access to plaintiff's website.[79] During his employment, the defendant emailed documents from the plaintiff's website to his own and his wife's personal email accounts, and allegedly accessed plaintiff's information remotely

---

[70] *Id.* at 202.

[71] *Id.* at 203.

[72] *Id.* at 203–04.

[73] *Id.* at 204.

[74] *Id.* at 204–06. The court also rejected the "cessation-of-agency theory" that a breach of the duty of loyalty automatically made usage unauthorized. *Id.* at 206.

[75] *Id.* at 207.

[76] LVRC Holdings LLC v. Brekka, 581 F.3d 1127, 1128–29 (9th Cir. 2009).

[77] *Id.* at 1131.

[78] *Id.* at 1129.

[79] *Id.*

after he had ceased plaintiff's employ.[80] While plaintiff unsuccessfully pursued its claim under the unauthorized prong, the Ninth Circuit determined that the claim would also fail under the exceeds prong as the defendant was "entitled to obtain the documents at issue."[81]

Several years later the Ninth Circuit was afforded the opportunity to officially adopt the narrow view in *United States v. Nosal*.[82] The defendant in *Nosal*, a former employee of the plaintiff, persuaded his former colleagues to procure confidential information from plaintiff, with the intention of using it to his advantage as he planned to start a competing company.[83] The defendant was convicted for aiding and abetting the employees in exceeding their authorized access under Section (a)(4) of the CFAA (which also contains the exceeds prong), by convincing them to access a protected computer to fraudulently procure the valuable information.[84] In a thoughtful opinion affirming the dismissal of the defendant's charge under the CFAA, the court thought it dispositive that the broad interpretation would turn the statute "into a sweeping Internet-policing mandate," creating liability for even the most microscopic digital misstep on "all computers with Internet access."[85]

While the court stated that the narrow interpretation is the more valid of the two, in its conclusion it announced that it was applying the rule of lenity, and therefore would construe the statue narrowly in favor of the defendant.[86] The dissent urged that the plain meaning of the statute was clear, and that the correct method of intervening upon the hypothetically vast reach of the statute would be an as-applied constitutional challenge.[87] In a separate appeal, where Nosal tried to contest the charges under the unauthorized prong, the Ninth Circuit chose to use the plain meaning of the word in its analysis.[88] Therefore,

---

[80] *Id.* at 1129–30.

[81] *Id.* at 1135 n.7.

[82] United States v. Nosal, 676 F.3d 854, 863–64 (9th Cir. 2012).

[83] *Id.* at 856.

[84] 18 U.S.C. § 1030(a)(4) (2012); *Nosal*, 676 F.3d at 856.

[85] *Nosal*, 676 F.3d at 858–59. To illuminate the sheer potential for liability, the court used examples such as: the usage of "work computers for personal purposes," the former prohibition against minors using Google's services, dating websites forbidding the use of inaccurate information, posting items in the wrong category on eBay or Craigslist, and finally noting that "website owners retain the right to changes the terms [of service] at any time." *Id.* at 858, 860–62.

[86] *Id.* at 863–64.

[87] *Id.* at 864–67 (Silverman, J., dissenting). "This is not an esoteric concept. . . . A new car buyer may be entitled to take a vehicle around the block for a test drive. But the buyer would . . . 'exceed [their] authority' . . . to take the vehicle to Mexico on a drug run." *Id.* at 865.

[88] *Nosal*, 828 F.3d at 868.

under the strictest application of the narrow view, an abuse of authorized access is not enough to exceed one's authority; instead one must act as an inside hacker—an authorized user circumventing an internal technological barrier.

B. The Broad View—Access Based on Usage Permissions

The First, Seventh, Eighth, and Eleventh Circuits have adopted the broad view of the exceeds prong. In the civil case of *EF Cultural Travel BV v. Explorica, Inc.*, the First Circuit endorsed the broad approach by affirming a preliminary injunction against the defendant under the exceeds prong of 18 U.S.C. § 1030(a)(4).[89] Here, while the offense may have been under Section (a)(4) as opposed to Section (a)(2), the interpretation of the exceeds prong remained static. Defendant Explorica and plaintiff EF Cultural Travel were both competitors in the business of offering student tours, with several of defendant's employees having previously worked for plaintiff.[90] In an effort to undercut plaintiff, defendant developed a computer program called a "scraper" to capture plaintiff's tour prices from its website.[91] To do this, the defendant used proprietary knowledge about the structure of the plaintiff's site and "tour codes whose significance [were] not readily understandable to the public."[92] Tantamount to the First Circuit's finding that the use was in excess of authorization was the overarching confidentiality agreement between plaintiff and its former employees, including the strict prohibition on the release of any information that would be adverse to plaintiff's interests.[93] This analysis appeared to be in large part based upon contract law, holding that when defendant was in breach of the confidentiality agreement, the use of proprietary information in contradiction to plaintiff's interests exceeded the defendant's otherwise authorized access to the public website.[94]

In the companion case, also titled *EF Cultural Travel BV v. Explorica, Inc.*, the First Circuit faced the question of whether the preliminary injunction against Explorica also applied as to defendant Zefer Corp., the company responsible for creating the "scraper" tool.[95] The court rejected the district

---

[89] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585, 582 n.10 (1st Cir. 2001).

[90] *Id.* at 579.

[91] *Id.*

[92] *Id.* at 579, 583.

[93] *Id.* at 583.

[94] *Id.* at 582–84.

[95] EF Cultural Travel BV v. Zefer Corp., 318 F.3d 58, 60 (1st Cir. 2003).

court's usage of a "reasonable expectations test" in determining a lack of authorization under the CFAA.[96] Interestingly, the court acknowledged in dicta that a "lack of authorization may be implicit, rather than explicit" in determining liability.[97]

The Seventh Circuit addressed the "paper thin" difference between "'without authorization' and 'exceeding authorized access'" in *International Airport Centers, L.L.C. v. Citrin*.[98] While it was alleged the defendant had violated an older version of the statute, which dealt with unauthorized damage to a protected computer under Section (a)(5)(A),[99] the provisions are functionally identical to ones still currently in the CFAA.[100] The defendant in this case had been an employee of plaintiff who "decided to quit . . . in breach of his employment contract."[101] He then ran a program to delete all the files on his work laptop, including data collected for plaintiff and evidence of his improper conduct, and permanently prevent their recovery.[102] Using agency theory, the court determined that the defendant lost all authorization to use the laptop in question when he breached a duty of loyalty to plaintiff.[103] While the defendant's ultimate liability in this case was decided upon the use being unauthorized, in their discussion of the difference between an authorized use versus a use that exceeds authorized access, the Seventh Circuit cited to a First Circuit case upholding the broad view.[104] The court's decision therefore indicates that if liability had hinged upon the exceeds prong, the Seventh Circuit may have officially adopted the broad view.

In 2011, the Eighth Circuit implicitly adopted the broad interpretation of the exceeds prong in *United States v. Teague*.[105] In affirming the district court's opinion, the Eighth Circuit held that the defendant had violated Section (a)(2)(B) of the CFAA (obtaining "information from [any] department or agency of the United States") by exceeding her authorized access

---

[96] *Id.* at 62–63. The test focused on what would be reasonably expected of an ordinary user. *Id.* at 60.

[97] *Id.* at 63.

[98] Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420 (7th Cir. 2006) (quoting 18 U.S.C § 1030(a)(1), (2), (4) (2006)).

[99] *See* 18 U.S.C. § 1030(a)(5)(A); *Int'l Airport Ctrs., L.L.C.*, 440 F.3d at 419.

[100] *See* 18 U.S.C. § 1030(a)(5)(A), (B) (2012).

[101] *Int'l Airport Ctrs., L.L.C.*, 440 F.3d at 419.

[102] *Id.*

[103] *Id.* at 420–21.

[104] *Id.* at 420 (citing EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583–84 (1st Cir. 2001); Pac. Aerospace & Elecs., Inc. v. Taylor, 295 F. Supp. 2d 1188, 1196–97 (E.D. Wash. 2003)).

[105] United States v. Teague, 646 F.3d 1119, 1120 (8th Cir. 2011).

when she violated her employer's computer usage policy.[106] The violation in question occurred when the defendant—the employee of a "contractor that assists with student loan inquiries" for the Department of Education—accessed the student loan information of former President Barack Obama to satiate her curiosity.[107] She was sentenced to two years of probation for the offense.[108] While there was no actual discussion as to the scope of "exceeds authorized access" in the opinion, the Eight Circuit's decision to hold a violation of a usage policy sufficient to satisfy the exceeds prong comports with the broad view's analysis.[109]

In *United States v. Rodriguez*, the Eleventh Circuit chose to establish a strict and broad approach in affirming the defendant's conviction of a twelve-month sentence under Section 1030(c)(2)(A), for a violation of Section (a)(2)(B) of the CFAA.[110] The defendant, "a TeleService representative for the Social Security Administration," utilized credentialed access to databases in order to acquire the sensitive personal information of women with whom he was infatuated.[111] In rejecting the narrow interpretation, the court stated that as applied to the facts of this case, "the plain language of the [CFAA] forecloses any argument that [the defendant] did not exceed his authorized access"; that is, by accessing the information for an improper purpose, the defendant was no longer entitled to obtain the information, and the conduct was clearly within the purview of the exceeds prong.[112] Finally, the court rejected the defendant's argument that he would only be liable had the violation occurred in conjunction with a crime, tort, or for monetary gain as it "would eviscerate the distinction between [the] misdemeanor and felony provisions."[113] The United States Supreme Court subsequently declined to hear the case on appeal.[114] Therefore, to summarize the broad view, if an individual violates a usage restriction, that individual forfeits his or her entitlement to obtain the information. As such, a use in violation of the usage restriction represents a use that exceeds otherwise authorized access.

---

[106] *Id.* at 1120–21.

[107] *Id.* at 1121.

[108] *Id.* at 1120.

[109] *Id.* at 1120–22. In this author's opinion, in viewing the similarities, yet opposite outcomes, between this case and *Valle*, allows one to truly put their "finger on the pulse" of the split.

[110] United States v. Rodriguez, 628 F.3d 1258, 1260–62 (11th Cir. 2010).

[111] *Id.*

[112] *Id.* at 1263.

[113] *Id.* at 1264; *see* 18 U.S.C. § 1030(c)(2)(A) (2006); *cf. id.* § 1030 (c)(2)(B)(i), (ii).

[114] Rodriguez v. United States, 563 U.S. 966 (2011).

III. THE CANNIBAL COP COURT COURTS AMBIGUITY: THE SECOND CIRCUIT ENTERS THE FRAY

In a case of dark fantasy and thought crime, Gilberto Valle successfully reversed two jury convictions after two rounds of appeals, and in doing so, prompted the Second Circuit to join the narrow side of the split in the interpretation of "exceeds authorized access."[115] The Court's adoption of lenity, and therefore the narrow interpretation of the statute, was fueled by trepidation at the thought of the severe implications the broad interpretation of the phrase would bring—the possibility of making the entire country criminals for violations of unread or unknown terms of service, thereby resulting in arbitrary and absurd enforcement.[116] In doing so, the Second Circuit further illuminated an aged fissure in the judicial interpretation of these three simple words in the CFAA, and how perhaps in its current form it poses an irreconcilable clash of logic—a logical reading giving illogical results.

A. Background and Procedural History

Prior to his jury conviction, Gilberto Valle was an NYPD officer married to Kathleen Mangan, and had no prior criminal record or history of violence.[117] In his free time he frequented a macabre sexual Internet group called "Dark Fetish Network" where he would discuss kidnapping, torturing, and cannibalizing women he knew with other individuals, including three users charged as his co-conspirators.[118]

Due to his status as an NYPD officer, Valle was permitted access to Omnixx Force Mobile, "a computer program that allows officers to search various restricted databases, including the federal National Crime Information Center database, which contain sensitive information about individuals such as home addresses and dates of birth."[119] Valle was well

---

[115] United States v. Valle, 807 F.3d 508, 511 (2d Cir. 2015).

[116] *Id.* at 527. For example: an innocent and unknowing violation of a website's terms of services—which may be changed without notice—could be considered a felony under the broad interpretation.

[117] *Id.* at 512.

[118] United States v. Valle, 301 F.R.D. 53, 59 (S.D.N.Y. 2014), *aff'd in part, rev'd in part*, 807 F.3d 508 (2d Cir. 2015). The three were "Michael VanHise, a man from New Jersey who was known to Valle as 'mikevanhise81@aol.com' and 'michael19902135@yahoo.com'; an un-identified individual apparently located in Pakistan who used the screen name 'Aly-Khan'; and Dale Bolinger, a man in England who was known to Valle only by his screen name, 'Moody Blues.'" United States v. Valle, 807 F.3d 508, 512 (2d Cir. 2015).

[119] *Valle*, 807 F.3d at 512–13.

aware that the NYPD had a strict policy restricting the program's use to only the course of his duties as an officer.[120] Heedless of the known prohibition, in the period from 2011 to 2012, Valle accessed the database to query the names of several women.[121] All of the women were subjects of the sexual fantasies discussed between himself and his alleged co-conspirators.[122] "There [was] no evidence, however, that Valle used any information obtained from these searches in furtherance of the alleged kidnapping conspiracy, or that he told his alleged co-conspirators that he had conducted these searches or had access to such information."[123]

After his arrest, Valle was convicted by a jury for conspiracy to kidnap,[124] and for exceeding his authorized access to the government database under 18 U.S.C. § 1030(a)(2)(B), to which he subsequently moved for either a judgment of acquittal or for a new trial.[125] The district court granted Valle's motion with regard to the conspiracy to kidnap charge and reversed the conviction, holding that the government had failed to satisfy its burden of establishing "proof beyond a reasonable doubt"[126] that Valle's actions truly crossed the threshold from fantasy to conspiracy.[127] The court did, however, affirm the conviction under the CFAA as it found that Valle's "conduct [fell] squarely within the plain language of Section 1030(a)(2)(B)."[128] As Valle was only permitted to use the database in the course of his duties as an NYPD officer,[129] the court felt he had clearly exceeded his authorized access by "access[ing the] computer with authorization and . . . us[ing] such access to obtain . . . information . . . [he was] not entitled so to obtain or alter."[130] The court acknowledged that the Second Circuit had not yet weighed in on the reach of the exceeds prong, as well as the differing methods of interpreting

---

120 *Id.* at 513.

121 *Id.* at 512–13; *Valle*, 301 F.R.D. at 76–77.

122 *Valle*, 807 F.3d at 512–13; *Valle*, 301 F.R.D. at 76–77.

123 *Valle*, 301 F.R.D. at 77.

124 "If two or more persons conspire to violate [18 U.S.C. § 1201(a)—kidnapping] and one or more of such persons do any overt act to effect the object of the conspiracy, each shall be punished by imprisonment for any term of years or for life." 18 U.S.C. § 1201(c) (2012).

125 *Valle*, 301 F.R.D. at 59; *see also* FED. R. CRIM. P. 29 (motion for a judgment of acquittal); *id.* R. 33 (motion for a new trial).

126 *Valle*, 301 F.R.D. at 83.

127 *Id.* at 59, 60, 90.

128 *Id.* at 115.

129 *Id.*

130 18 U.S.C. § 1030(e)(6) (2012).

its scope in the other circuits, yet still held that such a blatant disregard for usage restrictions triggered liability.[131]

B. The Majority Opinion and the Dissent

By a two-to-one majority opinion, the Second Circuit affirmed the acquittal of the conspiracy to kidnap charge, yet reversed the district court's judgment on the CFAA charge.[132] As the majority found merit in both the broad and narrow interpretations of the phrase "exceeds authorized access," they therefore found that lenity,[133] the judicial doctrine of construing ambiguous criminal statutes narrowly in favor of defendants, forced them to adopt the narrow view of the exceeds prong in Valle's favor.[134] In reaching their ultimate conclusion, the court looked to the legislative history of the exceeds prong, considering first, the government's contention that before the "exceeds authorized access" prong was added to the CFAA in 1986, the statute contained an improper purpose analysis, and that the current language was only meant to be a linguistic simplification; and second, that Valle's opposing contention that the 1986 amendment was intended to "abrogate any purpose-based inquiry"[135] and therefore should only apply to internal virtual trespass. Upon arrival at their decision to apply lenity, and thus the move to adopt the more acute interpretation of the exceeds prong, the majority admitted to the logical validity of both arguments based on the legislative history of the CFAA.[136]

In the court's opinion, Valle was authorized to use the database, so using it for an improper purpose did not fall under the scope of the CFAA. In its analysis, the majority also acknowledged the great divide of judicial interpretation in the circuit split,[137] stating that if the "sharp division means anything, it is that the statute is readily susceptible to different interpretations."[138] Additionally, the majority expressed a shared trepidation with the Ninth Circuit that if the broad view were adopted, it could possibly criminalize the conduct of

---

131 *Valle*, 301 F.R.D. at 111–15.

132 United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015).

133 For a more in-depth look at the inner workings of the doctrine of lenity, see discussion *infra* Part IV.

134 *Valle*, 807 F.3d at 526.

135 *Id.* at 525–26.

136 *See id.* at 526.

137 *Id.* at 511.

138 *Id.* at 524.

countless unsuspecting people for the violation of *any* computer usage policy.[139]

The main thrust of the dissenting opinion in *Valle* was that "[i]n reaching [the] result, the majority discover[ed] ambiguity in the statutory language where there is none. Under the plain language of the statute, Valle exceeded his authorized access to a federal database in violation of the CFAA."[140] Further contending that "[b]ecause the majority opinion [sought] to enshrine all the conduct in this case in an academic protective halo, [the dissent found] it necessary to offer the realistic context of this controversy."[141] Acknowledging and dismissing the majority's policy concerns, the dissent surmised that even if the current workings of the exceeds prong were frighteningly broad, the legislature had the exclusive power to remedy such a statute ripe for abuse, not the judiciary.[142] The dissent urged that as lenity is a "rule of last resort," the high threshold for its invocation had not been reached in *Valle,* and its application was grossly inappropriate where the proscribed conduct is unambiguous as applied to the facts of this case.[143] Finally, the dissent pushed back on the majority's consideration of the legislative history of the CFAA, contending that even if the legislative history could possibly support the narrow interpretation, that it is wholly irrelevant when the statutory text is unambiguous on its face.[144] The striking polarity of the majority and dissenting opinions, while not dispositive as to whether the narrow or broad view is correct, is illustrative of how widely interpretation of the exceeds prong varies—a fact that weighs in favor of the majority's finding of ambiguity.

IV. LEAN ON LENITY WHEN FACED WITH A LIEN ON LOGIC

The facts of *Valle* have served to further illuminate a gorge of ambiguity in the CFAA, and regardless of whether

---

[139] *Id.* at 527–28.

[140] *Id.* at 537 (Straub, J., dissenting). In the dissent it was first argued that the jury verdict as to the conspiracy to kidnap charge was based off of sufficient evidence, and that it was not the court's place to overturn it ad hoc. *Id.* at 529–37. However, as this note is focused on the charge under the CFAA, the dissent's reasoning as to the sufficiency of evidence and the lines of "fantasy" and "reality" will be omitted.

[141] *Id.* at 528–29.

[142] *Id.* at 539 (citing Dep't of Hous. & Urban Dev. v. Rucker, 535 U.S. 125 (2002)).

[143] *Valle*, 807 F.3d at 539 (Straub, J., dissenting) (citing Oppedisano v. Holder, 769 F.3d 147, 153 (2d Cir. 2014), *cert. denied sub nom.,* Oppedisano v. Lynch, 136 S. Ct. 211 (2015); United States v. Ron Pair Enters, Inc., 489 U.S. 235, 241 (1989)).

[144] *Id.* at 540 (citing United States v. Woods, 134 S. Ct. 557, 567 (2013); Puello v. Bureau of Citizenship & Immigration Servs., 511 F.3d 324, 331 (2d Cir. 2007)).

Valle's perverse computer searches were a breach of his employment contract, in this author's opinion, lenity was the only proper judicial tool to resolve this case of "thought crime." This section will discuss lenity and statutory interpretation as it applies to the facts of *Valle*, arguing that the Second Circuit was correct to invoke the rule and thus come down in Valle's favor in its legal analysis.

"The rule of lenity springs from the fair warning requirement."[145] A fair warning challenge is defined as "[a] defense that no one should be held criminally liable for conduct that he or she could not reasonably understand to be prohibited."[146] The rule of lenity mandates that upon a judicial finding that a criminal statute is ambiguous, it must be narrowly interpreted in a defendant's favor.[147] In upholding this rule, the courts "interpret ambiguous criminal statutes in favor of defendants, not prosecutors."[148]

"In . . . circumstances . . . where *text*, *structure*, and *history* fail to establish that the Government's position is unambiguously correct[,] [courts] apply the rule of lenity and resolve the ambiguity in [the defendant's] favor."[149] The Supreme Court has "always reserved lenity for those situations in which a reasonable doubt persists about a statute's intended scope even *after* resort to 'the *language* and *structure*, *legislative history*, and *motivating policies'* of the statute."[150] However, the mere possibility of a divergence of interpretation, even "a division of judicial authority" is not in itself enough to activate the rule.[151]

Therefore, to argue that this is more than a mere judicial disagreement, and that the Second Circuit was in fact correct to apply lenity to the exceeds prong, this section will argue that even after reviewing the plain meaning of the words "exceeds authorized access," the wording as contained in the CFAA, the legislative history, and chronology of the statute, as well

---

[145] United States v. Dauray, 215 F.3d 257, 264 (2d Cir. 2000). Interestingly enough, at least one court has held that the CFAA is not unconstitutionally vague. United States v. Fernandez, No. 92 CR. 563 (RO), 1993 WL 88197, at *1 (S.D.N.Y. Mar. 25, 1993).

[146] *Fair-Warning Challenge*, BLACK'S LAW DICTIONARY (10th ed. 2014).

[147] *Rule of Lenity*, BLACK'S LAW DICTIONARY (10th ed. 2014).

[148] United States v. Santos, 553 U.S. 507, 519 (2008) (emphasis added).

[149] United States v. Granderson, 511 U.S. 39, 54 (1994) (emphasis added).

[150] Moskal v. United States, 498 U.S. 103, 108 (1990) (emphasis added) (quoting Bifulco v. United States, 447 U.S. 381, 387 (1980)).

[151] *Id.* at 107–08. A fissure in judicial interpretation, even as large as the one presented here, where more than half of the circuit court judges are aggressively bifurcated in their analysis, is not sufficient in itself to trigger lenity. *See* discussion *supra* Part II.

as reviewing "access" as contained in other similar statutes, both interpretations are plausible, and therefore the statute is ambiguous.

A. Plain Meaning of the Words

To demystify the words "exceeds authorized access" as some esoteric concept, one must examine the plain meaning of the words. The approach will be as follows: first, the terms will be examined using their dictionary definitions, and second, the analysis used by the majority and dissent in *Valle* will be scrutinized. The goal is to showcase that the phrase "exceeds authorized access" on its face is easily susceptible to both a narrow and broad interpretation.

> It is elementary that the meaning of a statute must, in the first instance, be sought in the language in which the act is framed, and if that is plain, and if the law is within the constitutional authority of the law-making body which passed it, the sole function of the courts is to enforce it according to its terms . . . .
>
> Where the language is plain and admits of no more than one meaning, the duty of interpretation does not arise and the rules which are to aid doubtful meanings need no discussion.[152]

"Our starting point for statutory interpretation is the statute's plain meaning, if it has one."[153] To discern the plain meaning of the phrase "exceeds authorized access"—a phrase so innocuous on its face, yet so capable of creating a tributary of interpretations—the proceeding analysis will observe the definitions in isolation, and then in conjunction with one another.[154] "Exceed" is defined as to "go beyond or do more than is warranted . . . ."[155] "Authorize" is defined as to "give authority."[156] "Authorization" is defined as to "approve, consent to[,] permit, . . . allow, license, entitle, [or] empower."[157] "Authority" is defined as a "delegated power."[158] Finally, "access" is defined as "a right or opportunity to reach or use or visit; admittance."[159] Thus when assembling the dictionary definitions of the terms, "exceeds authorized access" will mean,

---

[152] Caminetti v. United States, 242 U.S. 470, 485 (1917) (internal citations omitted).

[153] United States v. Dauray, 215 F.3d 257, 260 (2d Cir. 2000).

[154] As each word has several definitions, only the definitions which are in this author's opinion on point to the discussion have been utilized in this note.

[155] *Exceed*, *supra* note 49, at 263.

[156] *Authorize*, *supra* note 49, at 47.

[157] *Authorization*, *supra* note 49.

[158] *Authority*, *supra* note 49, at 47.

[159] *Access*, *supra* note 49, at 5.

to "go beyond or do more than is warranted" the "delegated power" of "a right . . . to reach[,] . . . use or visit."[160]

Unfortunately, these terms linked as defined can be seen to support either side of the circuits' divide. For the proponents of the broad interpretation, the pairing of the idea that exceed can mean "more than is warranted,"[161] with the word "use" as contained in the definition of access,[162] appears to be directly on point with the interpretation that one can exceed his authorized access by violating usage restrictions—i.e., a nonwarranted use. Conversely, in support of the narrow interpretation, is the idea that to exceed one's authorized access, one must "go beyond"[163] his right to "reach" or "visit."[164] This notion agrees with the proposition that there must be some form of internal trespass wherein the offender treads past the boundaries of her "delegated power."[165] In the event of this type of stalemate, lenity dictates the win go to the interpretation favoring the defendant.[166]

In *Valle* the majority focused on how the term "authorization" could be read in two ways, with each way supporting either side of the argument.[167] The majority also reaffirmed that as an undefined term in the CFAA, the word would be given its plain, everyday meaning.[168] The court reasoned that "authorization" could either support the government's contention that it refers to a specific mandate of proper usage (the broad view), or that "it could . . . refer to the particular files or databases in the computer to which one's authorization extends" (the narrow view).[169] Delving deeper, the court then rationalized that the true bone of contention rested rather on how one interprets the term "access."[170] The majority found that while not dispositive, when viewed in conjunction with the phrase "without authorization," the narrow view was a sensible interpretation

> because "without authorization" most naturally refers to a scenario where a user lacks permission to access the computer at all, one

---

160 *Id.*; *Authorize*, *supra* note 49, at 47; *Exceed*, *supra* note 49, at 263.

161 *Exceed*, *supra* note 49, at 263.

162 *Access*, *supra* note 49, at 5.

163 *Exceed*, *supra* note 49, at 263.

164 *Access*, *supra* note 49, at 5.

165 *Authority*, *supra* note 49, at 47.

166 *See* United States v. Santos, 553 U.S. 507, 511, 513–14 (2008). In *Santos*, the Supreme Court applied lenity when faced with the question whether "proceeds" meant "receipts" or just "profits," as both meanings held merit. *Id.* at 511, 513–14.

167 United States v. Valle, 807 F.3d 508, 524 (2d Cir. 2015).

168 *Id.*

169 *Id.*

170 *Id.*

> sensible reading of the statute is that "exceeds authorized access" is complementary, referring to a scenario where a user has permission to access *the computer* but proceeds to "exceed" the parameters of authorized access by entering an area of the computer to which his authorization does not extend.[171]

Finally, by quoting the majority opinion in *Nosal*, the Second Circuit agreed with the Ninth Circuit's analysis that as read together, both the unauthorized prong and exceeds prong could logically be read to apply only to hackers: "'[w]ithout authorization' would apply to *outside* hackers (individuals who have no authorized access to the computer at all) and 'exceeds authorized access' would apply to *inside* hackers (individuals whose initial access to a computer is authorized but who access unauthorized information or files)."[172] The majority did not officially come down and pick a side of the fence at this stage of the analysis.[173]

The dissent in *Valle* accused the majority of purposely ignoring how unambiguous the exceeds prong is on its face due to their policy concerns.[174] According to the dissent, Valle was well aware that he could only access the database for work purposes, and by breaching that agreement had exceeded his authorized access plain and simple.[175] The core of the dissent's argument was that if the statute reads broadly as defined, then it is broad, and therefore wholly the responsibility of the legislature to fix.[176] In this author's opinion, while the majority may have been partially swayed by policy concerns, the dissent's opinion on the plain meaning of the words is dangerously black and white, in that it wholly fails to consider whether the narrow view of the statute is plausible. Therefore, the plain meaning of the words fails to name a clear victor. However, this is merely the first step in the analysis, for

> [w]hether a statutory term is unambiguous, . . . does not turn solely on dictionary definitions of its component words. Rather, "[t]he plainness or ambiguity of statutory language is determined [not only] by reference to the language itself, [but as well by] the specific context in which that language is used, and the broader context of the statute as a whole."[177]

---

171 *Id.*

172 *Id.* (quoting United States v. Nosal, 676 F.3d 854, 858 (9th Cir.2012)).

173 *Id.* at 524–25.

174 *Id.* at 537–39 (Straub, J., dissenting).

175 *Id.*

176 *Id.*

177 Yates v. United States, 135 S. Ct. 1074, 1081–82 (2015) (second and third alterations in original) (quoting Robinson v. Shell Oil Co., 519 U.S. 337, 341 (1997)).

B. "Exceeds Authorized Access" as Defined and Within the Context of the Statue

In the effort to combat statutory ambiguity, context is key. This crucial component in determining whether a statutory term is ambiguous enough to invoke lenity,

> "is determined [not only] by reference to the language itself, [but also by] the specific context in which that language is used, and the broader context of the statute as a whole." Identical language may convey varying content when used in different statutes, sometimes even in different provisions of the same statute.[178]

Therefore, an essential element in attempting to ferret out ambiguity is to view the phrase "exceeds authorized access" as defined in the CFAA, and the context with which it is placed within the statute in its entirety.[179]

As defined, "'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."[180] Existing in a vacuum, the phrase by itself does not shed light on whether some form of improper circumvention is required, or if a mere misuse of granted access will create liability. However, in the sections of the CFAA detailing prohibited conduct, it is always in conjunction with and immediately following "without authorization,"[181] and therefore must fall into a grey zone wherein the individual is not simply an outsider cracking a virtual safe, but someone who was entrusted access to a digital realm and abused said access in an unwarranted manner. Yet this still does not ring dispositive to whether Valle "exceeded his authorized access" by executing a handful of searches outside of the scope of his duties, or if some form of further unwarranted intrusion into the database was required.[182]

---

[178] *Yates*, 135 S. Ct. at 1077 (alterations in original) (internal citations omitted) (quoting *Robinson,* 519 U.S. at 341); *see id.* at 1078 (a protected fish was not a "tangible object" under the Sarbanes-Oxley Act as the statute due to the context and purpose of the statute); *cf.* Muscarello v. United States, 524 U.S. 125, 126–27, 138–39 (1998) (having a gun within a car during a drug crime does constitute a valid use/carry as it creates the potential for the harm the statute was designed to protect against).

[179] *See Robinson*, 519 U.S. at 341; Deal v. United States, 508 U.S. 129, 132 (1993). "In law as in life, however, the same words, placed in different contexts, sometimes mean different things." *Yates*, 135 S. Ct. at 1082.

[180] 18 U.S.C. § 1030(e)(6) (2012).

[181] *Id.* § 1030(a)(2), (4).

[182] For example: say one is given a key to a home with the express instructions to not drink any of the vintage wines in the cellar. Would one need to simply drink the wine, or would there need to be a lock on the cellar door to which the potential committer of grand theft vino must pick?

The exceeds prong is found within Sections (a)(1), (2), (4), and (7)(B) of the statute criminalizing conduct.[183] Section (a)(1) deals with the intentional theft of confidential government information.[184] Section (a)(2) deals with the unlawful procurement of data, either "contained in a financial record of a financial institution, or of a card . . . , or contained in a file of a consumer reporting agency on a consumer,"[185] "from any department or agency of the United States,"[186] or "from any protected computer."[187] Section (a)(4) criminalizes conduct when a perpetrator "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."[188] Finally, Section (a)(7)(B) requires the wrongdoer have the intent to commit extortion, through an interstate or foreign transmission, and threaten to "obtain information from a protected computer."[189]

Therefore, unlike the other sections, Section (a)(2) fails to indicate criminal conduct with the specificity of the other sections.[190] Yet again, this breathes life into both interpretations of the statute. The broad view could plausibly contend that due to the specific and malicious behavior proscribed in the other subsections of the CFAA containing the exceeds prong, that its exclusion was intentional for Section (a)(2), as it was intended to be a catch-all provision, otherwise many internal offenders (like Valle), committing offenses the statute was arguably designed to protect against, would get off scot free.[191] Yet in a deft riposte (using eerily similar logic), the proponents for the narrow view could make the argument that as Section (a)(2)'s "sister-sections" all expressly provide a clearly defined proscribed usage *subsequent* to the appearance of "exceeds authorized access," then improper usage was not intended to be enshrined in the exceeds prong, only the concept of digital trespass or internal hackers. Additionally, it could be argued that if the legislature sought to criminalize even accidental or innocuous violations,

---

183 18 U.S.C. § 1030(a)(1), (2), (4), (7)(B).

184 *Id.* § 1030(a)(2)(A).

185 *Id.* § 1030(a)(2)(A).

186 *Id.* § 1030(a)(2)(B).

187 *Id.* § 1030(a)(2)(C). Protected computer being the term that threatens to give the CFAA its near omnipotent reach as it refers to a wide array of devices with internet access. *See* discussion *supra* Section I.B.1.

188 18 U.S.C. § 1030(a)(4).

189 *Id.* § 1030(a)(7)(B).

190 *Id.* § 1030(a)(2); *cf. id.* § 1030(a)(1), (4), (7)(B).

191 For example: it would be ludicrous for a government employee to escape liability under § 1030(a)(1) for disseminating confidential government information simply because she had been granted access. *See id.* § 1030(a)(1).

then Congress would have been far more succinct in its definition of the infamous three-word phrase.[192] This deadlocked split does not seem to give when looking at the defined term, or its context in the CFAA as a whole. The logical next step would be to attempt to read the tea leaves of legislative intent through the CFAA's history.

C. A Contradictory Legislative History

In examining any potential ammunition the legislative history of the CFAA may provide to either side of the split, the bulk of this cache will come from the Act's original formation and its 1986 amendment. In discovering an abundance of artillery for either viewpoint, this section will urge that the majority's adoption of lenity in *Valle* was the correct choice, for "[w]hen Congress leaves to the judiciary the task of imputing to Congress an undeclared will, the ambiguity should be resolved in favor of lenity."[193]

1. Support for the Narrow View

The CFAA was originally enacted to criminalize and deter the growing crime of computer hacking, analogizing it to trespass and thievery.[194] This original scope is far more on point with the narrow view's internal hacker analysis as opposed to the broad view's contention that any contravention of usage restrictions violates the exceeds prong. As trespass deals with "wrongful entry," its analogy to the CFAA recalls someone treading where she does not belong, as opposed to someone doing something improper in an area where she does.[195] This is also compounded with the legislature's intention for Section (a)(2) specifically to be about privacy protection.[196] Privacy is defined as "[t]he quality, state, or condition of being free from public attention to intrusion into or interference with one's acts or decisions."[197] Viewing this definition in reference to Section (a)(2), as well as the overarching theme of trespass in the CFAA, it could imply that a violation thereof entails individuals going

---

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

[193] United States v. Santos, 533 U.S. 507, 515 (2008) (quoting Bell v. United States, 349 U.S. 81, 83 (1955)).

[194] Counterfeit Access Device and Computer Fraud and Abuse Act of 1984, Pub. L. No. 98-473, § 2102(a), 98 Stat. 2190, 2190–92 (codified as amended at 18 U.S.C. § 1030 (2012));.H.R. REP. NO. 98-894, at 20 (1984); S. REP. NO. 99-432, at 9–10 (1986).

[195] *See Trespass*, BLACK'S LAW DICTIONARY (10th ed. 2014).

[196] S. REP. NO. 99-432, at 6.

[197] *Privacy*, BLACK'S LAW DICTIONARY (10th ed. 2014).

beyond the limits of their access in order to view something they are not authorized to, not viewing something they are entitled to in an impermissible way.[198]

The 1986 version of the Act altered the original wording of the exceeds prong ("having accessed a computer with authorization, uses the opportunity such access provides for *purposes* to which such authorization does not extend"[199]) by most notably removing the word "purposes."[200] This was replaced with the current definition of "exceeds authorized access" where a user with authorization uses that access "to obtain or alter information in the computer the accesser is not entitled so to obtain or alter."[201] This change was made in order to resolve "one of the murkier grounds of liability," to distinguish a legitimate use from a criminal one.[202] Is this recognition of ambiguity, and an attempt to resolve the internal trespass versus improper use divide? If so, the narrow view would appear to emerge the winner. These changes, viewed as an island, push toward the understanding that by removing the word "purposes" and adding the word "entitled," that the analysis under the exceeds prong is intended to be based off a spatial analysis as opposed to a behavioral one, e.g., an internal trespass as opposed to an improper use.

Finally, the 1986 amendment altered the scienter requirement from "knowingly" to "intentionally."[203] This was primarily done as in Congress's opinion the word knowingly might be inappropriate in the context of computers, as one could "knowingly," yet "inadvertently 'stumble into' someone else's computer file or computer data."[204] To elaborate on this point, Congress also mentioned how one might exceed this authorized access, giving the example: "where an individual is authorized to sign onto and use a particular computer, but subsequently *exceeds his authorized access* by mistakenly *entering* another computer file or data *that happens* to be accessible from the same terminal."[205] Two interesting things might be gleaned from this example: (1) this was a use that

---

[198] Of course, the possible pushback would be that if one abuses access to view confidential information not as intended, then that could also be a violation of privacy. The unique character of this inquiry as to the appropriateness of lenity however, is not that there is one right answer, but that both answers *could* be right.

[199] § 2102(a), 98 Stat. at 2190–92.

[200] Computer Fraud and Abuse Act of 1986, Pub. L. No. 99–474, 100 Stat. 1213.

[201] 18 U.S.C. § 1030(e)(6) (2012).

[202] S. REP. NO. 99-432, at 21 (1986).

[203] *Id.* at 5.

[204] *Id.* at 6.

[205] *Id.* (emphasis added).

Congress did not want to criminalize;[206] and (2) at the time their idea of "exceeds" was, in fact, spatial.[207] Under the given example, the user, while authorized to use one computer, exceeded that authorization when entering *"another* computer file or data *that happen*[*ed*] to be accessible."[208] If Congress meant in this example the user, while authorized to use one computer, exceeds that authorization by accessing files on a different computer or network, this type of usage would be right on point with the theory of digital trespass.[209]

2. Support for the Broad View

A compelling argument for the broad view is that the CFAA has shown continuous expansion since its inception.[210] Throughout this rapid expansion, Congress has not once sought to amend the "exceeds authorized access" language since it was enshrined within the CFAA in 1986.[211] The legislature has chosen not to alter the language in order to clarify a very public circuit split with a vintage of over fifteen years.[212] One could plausibly infer that Congress has deemed the statute to be working as intended, and in accordance with the trend of the CFAA's reach growing exponentially bigger, that its intent was for the exceeds prong to include the improper use analysis. Additionally, and as the government argued in *Valle*, another possible interpretation of Congress's choice to remove the "purposes" language from the original statute was not to alter any culpability requirement, but merely to simplify the wording of the statute.[213]

Fuel can be found for the broad view's contention by looking to the reasoning employed by Congress in deciding not to include the exceeds prong in Section (a)(3) of the CFAA.[214] It

---

[206] If mistaken violations were intended to be left out of Section (a)(2), that certainly does not support the broad view, which technically would criminalize such actions.

[207] This is inferred from the usage of the phrase "entering another computer file or data that happens to be accessible from the same terminal," invoking the idea that authorization refers to the right to use a computer and the data located therein, as opposed to the terms of its use. S. REP. NO. 99-432, at 6.

[208] *Id.*

[209] Of course, the counter argument could be that this example was meant to mean accessing files located on the *same* computer, which would indicate a violation of use restrictions.

[210] *See* Buckman, *supra* note 15.

[211] *See* discussion *supra* Section I.A.

[212] *See* discussion *supra* Part II.

[213] S. REP. NO. 99-432, at 9; United States v. Valle, 807 F.3d 508, 525 (2d Cir. 2015).

[214] Section (a)(3) deals with the access of government computers. 18 U.S.C. § 1030(a)(3) (2012) The wording is still nearly identical to when it was originally drafted. *Compare id.* § 1030(a)(3), *with* 18 U.S.C. § 1030(a)(3) (1986) (the original

chose to omit the exceeds prong, finding it "not difficult to envision an employee or other individual who, while authorized to use a particular computer in one department, briefly exceeds his authorized access and peruses data belonging to the department that he is not supposed to look at."[215] Did Congress imply that an employee with full access to multiple departmental databases, but under the mandate of a usage restriction, would exceed her authorized access by violating that restriction? If so, is this a violation of a usage restriction, or a trespass?

Finally for the broad interpretation, is language nestled in a 1984 House Report,[216] the year of the CFAA's enactment. The report discusses an example violation under Section (a)(3), which contained the original form of the exceeds prong, stating that "[t]he provision also would make it a criminal offense for anyone who has been authorized to use a computer [and accesses] it knowing that the access is for a *purpose* not contemplated by the authorization."[217] Going further, the House explained that

> [t]he provision therefore does not extend to any type or form of computer access that is for a *legitimate business purpose*. Thus, any access for a legitimate purpose that is pursuant to an express or implied authorization would not be affected. The provision does not extend to normal and customary business procedures and information usage and so these legitimate practices will not be interrupted or otherwise affected.[218]

In other words, the exceeds prong would not extend to a permissible use with regard to the scope of one's employment.[219] There was also discussion that an employee's abuse of authorization to commit "time stealing"—wasting time on a computer at work—was not intended to be under the purview of the exceeds prong, and the problem should be handled administratively.[220] This appears to provide support for the broad view, as well as assuage anxiety from the narrow view. The discussion of a legitimate business purpose is strikingly on point with the improper purpose analysis toted by the broad view. Yet by discussing the desire that minor infractions be

---

referring to any government computer, with the current version referring to nonpublic government computers).

[215] S. REP. NO. 99-432, at 7.

[216] H.R. REP. NO 98-894, at 20–23 (1984).

[217] *Id.* at 21 (emphasis added).

[218] *Id.* (emphasis added).

[219] *Id.*

[220] *Id.* at 21–22. This does seem to solve the problem of the narrow view's worry of criminalizing an employee checking social media at work.

handled administratively, the narrow view's worry of draconian enforcement would seem to dissipate. To quote the Second Circuit in *Valle*, "[a]t the end of the day, . . . [there is] support in the legislative history for both [the narrow view's] and the [broad view's] construction of the statute. But because [the] review involves a criminal statute, some support is not enough."[221]

D. Can Other Similar Statutes Tip the Scales of Interpretation?

Can trends in the Congressional pen provide persuasion as to whether the narrow or broad view should hold the crown? Examining how Congress has tackled the complex topic of digital access could either prove an invaluable source of information, or be a fool's errand in this final avenue of analysis.

1. Stored Communications Act: Access of Electronic Communications

The Stored Communications Act (SCA) is a strikingly similar statute to the CFAA. It "was enacted to 'protect against the unauthorized interception of electronic communications.'"[222] The SCA makes it a criminal act whenever an individual

> intentionally accesses *without authorization* a facility through which an electronic communication service is provided; or . . . intentionally *exceeds an authorization* to access that facility; and thereby *obtains, alters,* or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system.[223]

Clearly, this is another statute with both an unauthorized and exceeds prong, dealing with the obtainment or alteration of information.[224] Again in accord with the CFAA, the SCA doles out harsher punishments of five years imprisonment, a fine, or both, or ten years imprisonment, a fine, or both for a repeat offense, if the action in question was done for "commercial advantage," "private financial gain," or "in furtherance of any criminal or tortious act."[225] Again similarly, there is a "catch-all" that dictates one year imprisonment, a fine, or both if the violation was not done in furtherance of the enumerated

---

[221] United States v. Valle, 807 F.3d 508, 526 (2d Cir. 2015).

[222] Organizacion Jd Ltda. v. U.S. Dept. of Justice, 124 F.3d 354, 359 (2d Cir. 1997) (quoting S. REP. NO. 99-541, at 1 (1986)) (The SCA is part of the Electronic Communications Privacy Act).

[223] 18 U.S.C. § 2701(a)(1)–(2) (2012) (emphasis added).

[224] *Compare id.* § 2701(a) *with id.* § 1030(a)(2).

[225] *Compare id.* § 2701(b)(1) *with id.* § 1030(c)(2)(B).

intent.[226] The SCA even directs its definition of "protected computer" to the definition as contained in the CFAA.[227]

The term "exceeds an authorization" is not defined in the SCA,[228] yet some courts have chosen to understand the phrase as it appears in the CFAA and the SCA analogous.[229] Yet with so many similarities, one must look for the differences to further this quest for certainty. A substantial difference between the two manifests in the SCA's definition of "computer trespasser," which is defined as:

> a person who accesses a protected computer without authorization and thus has no reasonable expectation of privacy in any communication transmitted to, through, or from the protected computer . . . [but] *does not include a person known by the owner or operator of the protected computer to have an existing contractual relationship with the owner or operator of the protected computer for access to all or part of the protected computer*.[230]

If the SCA borrows the definition of "exceeds authorized access" does that mean that the CFAA should borrow the definition of "computer trespasser" from the SCA? Clearly the argument for the narrow view would hammer this argument into the ground, as the language obviously excludes those with some form of a relationship entitling them access. While fuel for the opposing side could possibly be that as this definition was not included in the CFAA, the legislature did not intend for any "cross-talk" between the statutes. An even stronger argument is that the legislature purposely excluded this definition from the CFAA, as their intent *was* for there to be an improper use analysis. It would appear that for every one step forward, there are two steps back in this exodus of understanding the exceeds prong.

---

[226] *Compare id.* § 2701(b)(2) *with id.* § 1030(c)(2)(A).

[227] *See id.* § 2711(1) (directing the reader to § 2510); *id.* § 2510(20) (directing the reader to § 1030); *id.* § 1030(e)(2) (definition of protected computer).

[228] *See id.* § 2711 (not defined therein); *id.* § 2510 (not defined therein).

[229] *See* Cloudpath Networks, Inc. v. SecureW2 B.V., 157 F. Supp. 3d 961, 986–87 (D. Colo. 2016); Cheng v. Romo, No. 11-10007-DJC, 2012 WL 6021369, at *3 (D. Mass. Nov. 28, 2012); Penrose Computer Marketgroup, Inc. v. Camin, 682 F. Supp. 2d 202, 211 (N.D.N.Y. 2010); Int'l Ass'n of Machinists & Aerospace Workers v. Werner-Masuda, 390 F. Supp. 2d 479, 498 (D. Md. 2005).

[230] 18 U.S.C. § 2510(21)(A)–(B) (emphasis added).

2. Digital Millennium Copyright Act: Access and Circumvention

While the Digital Millennium Copyright Act (DMCA) does not cover uses that exceed authorized access,[231] it is worth exploring whether, as applied, the interpretation of access is more in line with either side of the circuit split regarding the exceeds prong of the CFAA. The DMCA proscribes the "circumvent[ion of] a technological measure that effectively controls access to a work protected under" the Copyright Act.[232] Essential to finding a conviction under the DMCA, there must have been a circumvention of an effective access control resulting in an unauthorized access of the digital contents therein.[233] A circumvention "means to descramble a scrambled work, to decrypt an encrypted work, or otherwise to avoid, bypass, remove, deactivate, or impair a technological measure, without the authority of the copyright owner."[234] An access control is effective "if the measure, in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work."[235] In other words, the access protection is effective only if it can be ordinarily bypassed through a device, such as a code, granted by the authority of the copyright holder.[236]

It has been held that just because a defendant may have an alternate "back door" to access the material is irrelevant, what matters is how the access protection functions in its ordinary operation.[237] In *Pearl Investments, LLC v. Standard I/O, Inc.,* the defendant's argument that it had programmed the access restriction in question and kept a backup file that allowed it continued access through a "tunnel," was found to be without merit.[238] But in this case, summary judgment was denied as to plaintiff's claim because it was unclear whether

---

[231] 17 U.S.C. § 1201(a)(1)(A) (2012) (no language similar to exceeds authorized access appearing in the statute, instead dealing with circumvention of access restrictions).

[232] *Id.*

[233] Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1203 (Fed. Cir. 2004).

[234] 17 U.S.C. § 1201(a)(3)(A).

[235] *Id.* § 1201(a)(3)(B).

[236] *See id.*

[237] Pearl Invs., LLC v. Standard I/O, Inc., 257 F. Supp. 2d 326, 350 (D. Me. 2003).

[238] *Id.* at 349–50. Interestingly enough, there was also a civil charge under the CFAA against defendant for a violation of Section (a)(5), but summary judgment was granted for the defendant due to insufficient evidence of the mandatory $5000 damage to the computer system. *Id.* at 348–49. As Section (a)(5) does not deal with the exceeds prong, it is not discussed here.

the defendant or the plaintiff's employees had constructed the virtual "tunnel" that allowed access.[239] Yet on the other side of the coin, those with undisputed access, who use said access in an authorized manner, are deemed to act as they please.[240] Therefore in *Chamberlain Group, Inc. v. Skylink Technologies, Inc.*, the defendant, a third party manufacturer of garage door openers for the secondary market, had not violated the DMCA by selling devices that interacted with the plaintiff's copyrighted garage door software, as the customers were authorized to access the code in question to open their garage doors.[241]

It appears as if this interpretation of "access" under the DMCA tilts more toward the narrow interpretation of the exceeds prong under the CFAA, but both interpretations can arguably fit. For the narrow view, as long as one is an authorized user, absent any forced entry or illegal conduct, the user is entitled free reign even outside of the intended scope as provided.[242] Reconciling this with the narrow view, there must be some internal circumvention, as opposed to a use that falls outside of restriction. To parry that argument, as access restrictions under the DMCA are viewed as to the "ordinary course of its operation,"[243]—one who abuses said access can still be liable, thus attaching a similar meaning of access to the CFAA would make it immaterial if one is fully authorized. Yet again, arrival at the crossroads of interpretation appears inevitable, and as ambiguity muddies the water, lenity's mandate becomes clear.

As the journey through the plain meaning of the words "exceeds authorized access," their context within the statute, the legislative history of the statute, as well as other similar statutes has failed to provide a beacon of clarity, it would appear a victor emerges due to a lack thereof. For the foregoing reasons discussed above, the Second Circuit was correct in applying lenity, as lenity is a rule that "applies only if, 'after seizing everything from which aid can be derived,' . . . [one] can make 'no more than a guess as to what Congress intended.'"[244]

---

[239] *Id.* at 350.

[240] *See, e.g.*, Chamberlain Grp., Inc. v. Skylink Techs., Inc., 381 F.3d 1178, 1204 (Fed. Cir. 2004).

[241] *Id.* at 1183, 1204.

[242] *See id.*

[243] *Pearl Invs., LLC*, 257 F. Supp. 2d at 350.

[244] Muscarello v. United States, 524 U.S. 125, 138–39 (1998) (quoting United States v. Wells, 519 U.S. 482, 499 (1997)).

V. HAS THE CURRENT INCARNATION OF SECTION (a)(2) EXCEEDED ITS WELCOME?

Due to the inherent flaws in both the narrow and broad interpretations of the exceeds prong, a prudent solution to the split would be to limit liability to a use that "exceeds authorized access" under Section (a)(2) only if it reaches a level of conduct implicating the second tier of punishment under Section (c)(2)(B). This alteration would eliminate ambiguity, as well as the policy concerns of the CFAA becoming over-expansive, thus de-shackling the phrase from the mandate of lenity, and thereby allowing for the improper use analysis. First, the "quasi-strict liability" of Section (a)(2)[245] and the massive reach of the "protected computer" analysis in Section (a)(2)(C)[246] pose grave potential for draconian punishment and arbitrary enforcement, the driving force for the narrow view's adoption of lenity. Second, under the narrow view as many believe to be required by lenity, all conduct that "exceeds authorized access" is in fact "unauthorized," and the phrase is therefore superfluous.[247] Finally, an ideal solution would be to amend the first tier of punishment, (c)(2)(A), to remove Section (a)(2) liability from under its purview. Thus, liability under (a)(2) would only trigger once the act crosses the threshold into eligibility for the second tier of punishment under Section (c)(2)(B), therefore extinguishing the policy concerns of the narrow view while allowing for the improper use analysis.

A. Exceeding the Limits of Logic: A Prosecutor's Poison Weapon

In a showcase of the CFAA's potential for inordinate punishment, take the case of Aaron Swartz, a computer prodigy with a passion for freedom of information.[248]

---

[245] Section (a)(2) merely requires to the intent to access and obtain information outside the purview of authorization. 18 U.S.C. § 1030(a)(2) (2012); *see* discussion *supra* Section I.B.

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

[247] The fact that this argument could be used to argue that Congress intended the exceeds prong to be interpreted under the broad view is not lost upon this author, however the goal of this section is to illustrate the flaws in both interpretations, not argue that one side is correct and the other wrong.

[248] *See* Anne Cai, *Aaron Swartz Commits Suicide*, THE TECH (Jan. 12, 2013), http://tech.mit.edu/V132/N61/swartz.html [https://perma.cc/5JDZ-XD8V]; Larissa MacFarquhar, *Requiem for a Dream: Aaron Swartz Was brilliant and Beloved. But the People Who Knew Him Best Saw a Darker Side*, NEW YORKER (Mar. 11, 2013), http://www.newyorker.com/magazine/2013/03/11/requiem-for-a-dream [https://perma.cc/A4ME-GYT9]; John Schwartz, *Internet Activist, a Creator of RSS, Is Dead at 26, Apparently a Suicide*, N.Y. TIMES (Jan. 12, 2013), https://nyti.ms/2jD79Y6 [http://perma.cc/HHT2-

Unfortunately, his life was cut short after committing suicide in his Brooklyn apartment on January 11, 2013, at the age of twenty-six.[249] He had been "indicted in July 2011 by a federal grand jury for allegedly downloading millions of documents from JSTOR through the MIT network—using a laptop hidden in a basement network closet in MIT's Building 16—with the intent to distribute them."[250] He was facing a potential maximum sentence of thirty-five years in prison and a one million dollar fine.[251] While this case may have been decided on the unauthorized prong, it is a prime example of the troubling potential for the CFAA to be used as the ultimate scare tactic in a prosecutor's arsenal—drumming up charges on disproportionate transgressions to increase the pressure on defendants to settle.[252]

United States v. Drew illustrates how a prosecutor hungry for a conviction may attempt to stretch 18 U.S.C. § 1030(a)(2) when nothing else will stick.[253] The defendant in *Drew* set up a fake MySpace account[254] in order to harass her daughter's thirteen-year-old classmate by pretending to be a sixteen year old through a dummy profile.[255] After fictitiously flirting with her daughter's classmate for several days, the defendant-mother then messaged the classmate saying "the world would be a better place without [the classmate] in it."[256] The classmate committed suicide that same day.[257] The

---

TVWA]. Swartz's impressive bragging rights included: the development of RSS software at the mere age of 14, involvement in drafting the codes for Lawrence Lessig's Creative Commons, creating a company to merge with Reddit at 19, as well as co-founding Demand Progress.

[249] Cai, *supra* note 248; MacFarquhar, *supra* note 248.

[250] Cai, *supra* note 248. "JSTOR is a shared digital library created in 1995 to help university and college libraries free up space on their shelves, save costs, and provide greater levels of access to more content than ever before." *New to JSTOR? Learn More About Us*, JSTOR, http://about.jstor.org/10things [https://perma.cc/LGT8-2H5W].

[251] Schwartz, *supra* note 248.

[252] *See* Cindy Cohn, *Aaron's Law Reintroduced: CFAA Didn't Fix Itself*, ELEC. FRONTIER FOUND. (Apr. 29, 2015), https://www.eff.org/deeplinks/2015/04/aarons-law-reintroduced-cfaa-didnt-fix-itself [https://perma.cc/7YKC-UTKJ].

[253] The court in this case appeared to group unauthorized and exceeds authorized access as one prong, as opposed to two separate forms of usage. United States v. Drew, 259 F.R.D. 449, 460–61 (C.D. Cal. 2009). The type of usage displayed in *Drew* however, seems to be predominantly considered to exceed authorized access by the Circuit Courts championing the broad view. *See* discussion *supra* Section II.B. This type of commonplace judicial inconsistency adds yet another stone to the pile in favor of lenity, as well as evidence of the exceeds prong's problematic placement in such a far-reaching provision of the statute.

[254] MySpace is a social networking site that allows users to build a profile by uploading media in order to connect with others. *See generally* MYSPACE.COM, https://myspace.com (last visited July 4, 2017).

[255] *Drew*, 259 F.R.D. at 452.

[256] *Id.*

[257] *Id.*

prosecution based its theory on the fact that the pertinent MySpace terms of service covering access rights expressly prohibited harassment of other members and the knowing use of false information.[258]

The judge in *Drew* granted the defendant's motion for acquittal[259] "primarily because of the absence of minimal guidelines to govern law enforcement, but also because of actual notice deficiencies."[260] While there was outrage at the fact that the prosecution did not win the case, it is important to consider the ramifications had the decision been in the government's favor. Most importantly, MySpace was entitled to alter its terms of service at any time, therefore, if the court had gone the other way, its holding could have effectively criminalized anyone in violation of a website's forever malleable terms.[261] To illustrate this point further, the decedent in *Drew*—under the prosecution's interpretation of the CFAA—was a criminal herself, due to the fact she was a thirteen year old using MySpace in clear contradiction of the minimum age requirement of fourteen.[262] Thus applying the prosecutor's interpretation of the CFAA, that a violation of a website's terms of service is enough to create criminal liability, nearly anyone could be dragged into court.

Now, must one at least access the computer in question themselves? In *Auernheimer*, another case illustrating how far prosecutors may attempt to push Section (a)(2), the defendant was charged even though he never personally accessed the computer in question himself.[263] David Spitler, a co-conspirator, had discovered a security breach wherein he could manually discover email addresses through an oversight in AT&T's attempt to streamline login services for iPad owners.[264] In an effort to publicize this lapse in AT&T security, Auernheimer assisted Spitler in creating a program to automate the email discovery process and subsequently shared the findings with

---

[258] *Id.* at 454.

[259] *Id.* at 468.

[260] *Id.* at 464.

[261] *Id.* at 454.

[262] *See id.* ("By using the Services, you represent and warrant that (a) all registration information you submit is truthful and accurate; (b) you will maintain the accuracy of such information; (c) you are 14 years of age or older; and (d) your use of the Services does not violate any applicable law or regulation.").

[263] United States v. Auernheimer, 748 F.3d 525, 529–31 (3d Cir. 2014).

[264] *Id.* At the relevant time, AT&T was the exclusive service provider for all iPad owners. *Id.* at 529.

the media.[265] Luckily for the defendant, the conviction was vacated due to the Third Circuit's finding of improper venue.[266]

Yet had the court found Auernheimer guilty, how far could the holding have been stretched? It would have raised the issue as to how far removed one must be until they are exempt from prosecution under the CFAA. While here Auernheimer's connection to the alleged violation was fairly close, could this holding be extended to *any* software developer whose program is used by a hacker?

Coming full circle, it is important to remember the defendant in *Teague*, convicted for looking up President Obama's student loan records in a moment of idle curiosity.[267] Here, the defendant's conduct is a far cry from that in *Valle*, which was undeniably cringe-inducing.[268] No one was harmed, in contrast to *Drew* where a minor committed suicide allegedly due to the defendant's violation of terms of service.[269] Finally, the defendant was no malicious opportunist, unlike the defendants in the many employee/employer wrongful misappropriation cases.[270] Teague was a woman at work, who typed a name into a database for no reason other than what appeared to be curiosity.[271] How far can this extremely strict reasoning go? Under the broad interpretation, will any miniscule infraction of a usage agreement be criminal? For example, if an employer prohibited its employee from checking personal emails at work, would the employee become a criminal even if he were to accidently see one such email pop up on his computer screen?

If the cases above are any indicator, then under the broad view's interpretation of the CFAA, nearly anyone could be subjected to criminal or civil liability, or at the very least be harassed with charges. Without a clearly defined path to liability, the broad interpretation can be used to force people into "making deals" or as an employer's trump card against an unruly employee. While obviously there must be penalties in place to deter computer crime, under the current workings of the broad interpretation, the ends simply do not justify the means—

---

[265] *Id.* at 531; *see also* Ryan Tate, *Apple's Worst Security Breach: 114,000 iPad Owners Exposed*, GAWKER (June 9, 2010), http://gawker.com/5559346/apples-worst-security-breach-114000-ipad-owners-exposed [https://perma.cc/2AGJ-XUFC].

[266] *Auernheimer*, 748 F.3d at 529.

[267] *See* United States v. Teague, 646 F.3d 1119, 1121 (8th Cir. 2011).

[268] *See* United States v. Valle, 807 F.3d 508, 512–13 (2d Cir. 2015).

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

[270] *See* discussion *supra* Section II.B.

[271] *See Teague*, 646 F.3d at 1121.

how many will blindly stumble into liability and face incommensurate punishment in order to catch tomorrow's Valle?

B. When the Distinction Disappears: Is the Exceeds Prong Redundant Under the Narrow View?

At what point does the narrow interpretation of a use that "exceeds authorized access" in fact become simply "unauthorized"? When does a paper-thin distinction disappear altogether, creating superfluous language that only serves to muddy the waters? Under the narrow interpretation as made mandatory by lenity, as well as some scholarly opinions and proposed legislation, it could be argued that there is simply no need for an exceeds prong—whether or not it is ultimately a net positive.

Under the narrow interpretation of the exceeds prong, there must be some further, internal circumvention as opposed to a simple breach of trust. Yet wouldn't any circumvention of a barrier to which one is not authorized just become an unauthorized access—whether done externally or internally? As an example: would a student picking the lock to a professor's office be any more authorized than a burglar doing the same, simply because the student is allowed in the building?

Professor Orin S. Kerr has proposed a code-based approach, where a user must break through a code-based barrier to become unauthorized, and rejects any analysis based on a breach of contract—i.e., improper use.[272] Professor Kerr has also expressed that an exceeds prong based off of this breach of contract approach would "create a remarkably broad criminal prohibition that has no connection to the rationales of criminal punishment," and is better suited to be covered in future legislation "focused directly at the problem of employee database abuse."[273]

After the death of Aaron Swartz, the bona fide computer prodigy who killed himself due to facing decades in jail for downloading academic articles after being charged under the CFAA,[274] there was proposed legislation, in part based on the Fourth and Ninth Circuit opinions previously discussed.[275]

---

[272] *See generally* Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003) (urging for a code-based approach in interpreting the exceeds prong).

[273] *Id.* at 1663.

[274] For more information on Aaron Swartz, see *supra* Section V.A.

[275] *Wyden, Lofgren, Paul Introduce Bipartisan, Bicameral Aaron's Law to Reform Abused Computer Fraud and Abuse Act*, RON WYDEN: SENATOR FOR OR., (Apr. 21, 2015), https://www.wyden.senate.gov/news/press-releases/wyden-lofgren-paul-introduce-

Namely, the proposed law (Aaron's Law), would strike the exceeds prong from the entirety of the CFAA, replacing both the "unauthorized" and exceeds prongs with the language "access without authorization," meaning a circumvention of "one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information."[276] Examples of such circumvention include, but are not limited to "password requirements, cryptography, or locked office doors."[277] Opponents of the law urged that this will force companies to erect unnecessary barriers, limit the sharing of information, as well as weaken a computer crime statute when cybercrime is at an all-time high.[278]

Professor Kerr and the proposed legislation of Aaron's Law seem to realize that an exceeds prong would be superfluous if circumvention was made a requirement for violations. But, it overlooks the rising trend of computer crime committed by insiders, who may not need to breach a single barrier in order to satiate their nefarious purposes.[279] By simply removing the exceeds prong, or needing a circumvention—which in this author's opinion would simply be outside of the scope of authorization—would render a huge hole within the CFAA. A simpler solution, outside of a brand new law, or striking the exceeds prong in its entirety, would be to remove the quasi-strict liability from Section (a)(2), as enforced by the punishment under Section (c)(2)(A), and create culpability only for Section (a)(2) under (c)(2)(B)—a punishment with a clear culpable conduct. Not only would the CFAA lose its potentially astronomical reach, while still retaining the two decades of work that went into the statute, but it could also remain a weapon against insiders who make gross misuse of their authorization, all without cracking a single code.

---

bipartisan-bicameral-aarons-law-to-reform-abused-computer-fraud-and-abuse-act-[https://perma.cc/DDV9-RNYU].

[276] Aaron's Law Act of 2015, S. 1030, 114th Cong. § 2 (2015).

[277] U.S. SENATE, SECTION-BY-SECTION SUMMARY OF AARON'S LAW 1–2, https://www.wyden.senate.gov/download/?id=5E864E80-FC22-4665-9920-27007DF73201&download=1 [https://perma.cc/3GN7-7D5Z].

[278] Press Release, BSA, 'Aaron's Law' Is Flawed, Says BSA (June 20, 2013), http://www.bsa.org/news-and-events/news/2013/june/en06202013aaronslaw/?sc_lang=en-US [https://perma.cc/RZG3-5D73].

[279] *See 4 Facts About Cybercrime (Cyber Security Statistics in 2016)*, EKRAN SYS. BLOG (July 26, 2016), https://www.ekransystem.com/en/blog/cyber-security-statistics-2016 [https://perma.cc/2477-72G9].

C. An Exceedingly Simple Solution

After examining the CFAA, its history, current form, the circuit split in regard to the exceeds prong, and the cannibal cop case that ushered the Second Circuit into this linguistic dispute, the end point appears to be in sight. To fix this dilemma of logic, one does not need a bulldozer, but a scalpel. After an arduous journey through a decades-old statute and a fifteen-year-old split, this author proposes a surgical solution that not only aims to extinguish ambiguity and policy concerns, but to do so without "declawing" the CFAA, or creating a large loophole in the purview of its enforcement.

1. The Solution Defined

Put simply, the solution contends that to stabilize the exceeds prong, Section (a)(2) should only become punishable when behavior crosses the threshold into the second tier of punishment under the CFAA's sentencing system.[280] Unlike the first tier of punishment, which makes (a)(2) punishable for access alone,[281] the second tier requires the access be "committed for purpose of commercial advantage or private financial gain[,] . . . in furtherance of any criminal or tortious act," or "the value of the information obtained exceeds $5,000."[282] By attaching specific malicious purposes as a gateway to liability under (a)(2), it will allow for an improper use analysis, while at the same time sufficiently reining in its breadth. In essence, the change would eliminate any accidental or harmless liability under (a)(2) when using an improper use analysis, while still retaining the ability to punish fully authorized bad actors—something the narrow view cannot do.[283]

Implementation of the change must be clear and concise. First, (a)(2) must be removed from the first tier of punishment, with the language then reading: "in the case of an offense under subsection . . . (a)(3) or (a)(6)."[284] It may also be advantageous to clearly state that the subsection does not apply to (a)(2) to avoid confusion, yet that also comes with the caveat of adding unnecessary bulk to the section. Second, it

---

[280] *See* 18 U.S.C. § 1030(c)(2)(B) (2012) (describing the second tier of punishment under the CFAA).

[281] *Id.* § 1030(c)(2)(A).

[282] *Id.* § 1030(c)(2)(B).

[283] The fact that Valle would still be innocent under this proposed change is not lost upon this author, yet what matters is *had* he been found guilty of conspiracy, then he would have also been guilty of violating Section (a)(2).

[284] *See* 18 U.S.C. § 1030(c)(2)(A).

must be made clear that a violation of (a)(2) requires the malicious conduct contained under the second tier of punishment. This can be done in two ways. The shortest approach would be to reference (c)(2)(B) as a requirement of (a)(2), alerting the reader to reference that punishment. The alteration could read that "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access," in conjunction with the culpable conduct enumerated in subsection (c)(2)(B), "and thereby obtains . . . information" (followed by the rest of (a)(2)).[285] This method comes with the boon of brevity, yet makes the sacrifice of total clarity.

The other, more long-winded alternative would be to repeat the language of (c)(2)(B) in (a)(2). It could read that "[w]hoever . . . intentionally accesses a computer without authorization or exceeds authorized access," "committed for purposes of commercial advantage or private financial gain[,] . . . in furtherance of any criminal or tortious act in violation of the Constitution or laws of the United States or of any State; or . . . the value of the information obtained exceeds $5,000," "and thereby obtains . . . information" (with the remaining text of the statute continuing as normal from there on out).[286] This approach is the clearer of the two, yet comes with the cost of repetition. Both serve their purpose and put the public on notice, yet the latter would be the more advantageous considering the long-standing conflict and confusion surrounding (a)(2) and the exceeds prong. Finally, no other changes would need to be made to the other instances of the exceeds prong. As (a)(1), (a)(4), and (a)(7) already have a level of specificity attached to them (theft of government secrets, fraud, and extortion, respectively).[287] In fact, the proposed alteration of (a)(2) would make it more similar to its "sister sections."

A final alteration, in addition to those mentioned above, would be to alter the definition of "exceeds authorized access" to officially include an improper use analysis. This may be unnecessary, however, as it will be further argued that the change detailed above would remove the need for lenity. Yet due to the deeply entrenched positions of the circuits in conflict with one another, a heavy handed approach may be the wiser choice to help guide the courts. The change in the definition would read that "the term 'exceeds authorized access' means to

---

[285] *See id.* § 1030(a)(2).
[286] *Id.* § 1030(a)(2), (c)(2)(B).
[287] *Id.* § 1030(a)(1), (4), (7).

access a computer with authorization and to use such access," either by circumvention or violation of usage restrictions, "to obtain or alter information in the computer that the accesser is not entitled so to obtain or alter."[288] As these changes would hopefully remove any ambiguity attached to the CFAA, it would move the interpretation of "exceeds" closer to being free of lenity's mandate.

2. Eliminating Policy Concerns: Lenity No Longer Needed

In its decision to apply lenity in *Valle,* the Second Circuit gave substantial weight to the fact that their decision would greatly shape precedent, "govern[ing] many other situations."[289] The court knew that their "construction of the statute [would] impact[] many more people than Valle."[290] Therefore, tantamount to the majority's decision was the idea that the broad view—"a highly problematic interpretation"—could criminalize "checking Facebook at work," and could therefore not uphold the lower court's decision, even if "the Government promise[d] to use [the statute] responsibly."[291] To put it bluntly, no governmental promise to abstain from abusing such a far reaching interpretation of the CFAA could assuage the court's trepidation at the possibility of criminalizing even the most miniscule deviations from *any* computer use policy—including the usage restrictions imposed by an employer against using social media at work.[292]

Similarly, the Ninth Circuit in *Nosal* was chagrin to adopt the broad view as it would turn "the CFAA from an anti-hacking statute into an expansive misappropriation statute," thereby creating "a sweeping Internet-policing mandate."[293] The court also realized that their decision would affect the exceeds prong as it appears throughout the CFAA in its entirety, as "identical words and phrases within the same statute should normally be given the same meaning."[294] Noting that Section (a)(2)(C) lacks "any culpable intent," and the term protected

---

[288] *Id.* § 1030(e)(6).

[289] United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015).

[290] *Id.*

[291] *Id.*

[292] *See id.*

[293] United States v. Nosal, 676 F.3d 854, 857–58 (9th Cir. 2012).

[294] *Id.* at 859 (quoting Powerex Corp. v. Reliant Energy Servs., Inc., 551 U.S. 224, 232 (2007)). This is similar to the Fourth Circuit's discussion of lenity in *Miller*, applying the doctrine even though it was a civil case, as the CFAA involves "both civil and criminal application" and their reasoning would therefore "appl[y] uniformly in both contexts." WEC Energy Sols. LLC v. Miller, 687 F.3d 199, 203–04 (4th Cir. 2012).

computer includes "effectively all computers with Internet access," the court did not want to turn "millions of unsuspecting individuals" into criminals for violating "vague and generally unknown" terms of service, or by "g-chatting with friends, playing games, shopping or watching sports highlights" at work.[295]

If the solution detailed above were to take effect, the policy concerns of the Second and Ninth Circuits would effectively evaporate. With a clearly defined road to criminality, the elimination of strict liability, and an overall higher bar of culpability, the statute would no longer loom over the heads of any individual using a computer. At the same time, by removing these policy concerns and removing the need for lenity, the CFAA could still be used as a tool to punish internal offenders who otherwise have full authorization.

As a final illustration of how this solution could serve to make both sides happy, recall the examples of Steve Strawman, employee of Hypothetical Inc. In the first example given, where Steve used his authorization to obtain a client list to sell to a competitor, he would not have been guilty under the narrow view.[296] Yet under this new approach, as this action was done for private financial gain and possibly fraud, then his improper use would have triggered liability under Section (a)(2) as well, thus preventing Steve from shirking culpability. Conversely, in the second example, where Steve would have been guilty under the broad view merely by accessing the client information to send out invitations to his dinner party,[297] he would not have under this proposed solution, as his conduct did not cross the requisite threshold into criminality. While not perfect, the proposed solution at least better equips the CFAA to filter out the good from the bad.

CONCLUSION

Computers, cannibals, ambiguity, and a grammatical grudge match have found both the narrow view acute, and the broad view obtuse. Yet only through this clashing of polarized interpretations does a median appear. By harvesting wisdom from both sides of the argument, a clearly enumerated improper use analysis could serve to arm the CFAA with a properly restrained, yet necessarily flexible application. But while 20/20 hindsight is an advantage to someone when playing the role of

---

[295] *Nosal*, 676 F.3d at 859–62.

[296] *See* discussion *supra* Part II & Section II.A.

[297] *See* discussion *supra* Part II & Section II.B.

"armchair congressman," we must not lose sight of the challenges faced in the drafting of laws. As shown in this note, three simple words can cause untold conflict, proving that even Murphy was an optimist.[298] As laws creak and struggle with innovation, policy, and change—like the bow of a ship navigating through uncharted water—one must realize that although these laws can be fallible, they are more than simple words on a page. They represent an evolving doctrine, that at its best represents the amalgamated values of an entire nation, and at its worst . . . well, there's always lenity.

Charles S. Wood[†]

[298] "[T]he facetious proposition that if anything can go wrong, it will." *Murphy's Law*, DICTIONARY.COM, http://www.dictionary.com/browse/murphy-s-law (last visited July 13, 2017).

[†] J.D. Candidate, Brooklyn Law School, 2018, B.A., Columbia College Chicago, 2009. I would like to thank my parents, Sophie Mascatello, Dean Wood, Molly Klinghoffer, Keith Kirsch, Leo Suh, Dylan Hans, Ryan Gilinson, Ryan Starstrom Jessica Schneider, Valentina Lumaj, and the entire *Brooklyn Law Review* staff.