UIC John Marshall Journal of Information Technology & Privacy Law

Volume 27
Issue 2 *Journal of Computer & Information Law - Winter 2009*

Article 4

Winter 2009

The Computer Fraud and Abuse Act: Reassessing the Damage Requirement, 27 J. Marshall J. Computer & Info. L. 279 (2009)

Matthew Andris

COMMENT

THE COMPUTER FRAUD AND ABUSE ACT: REASSESSING THE DAMAGE REQUIREMENT

MATTHEW ANDRIS*

I. INTRODUCTION

An elected village commissioner logged on to her official e-mail and discovered that a village employee had been forwarding her correspondence with her constituents to the mayor, her political rival.[1] She surmised that a village information technology employee was responsible.[2] This e-mail forwarding hurt the village commissioner because she had challenged the mayor for his seat in the prior election.[3] As a result of local media coverage, the mayor denied any involvement with the forwarding of the e-mails.[4] The village commissioner brought suit in federal court claiming, among other things, a violation of the Computer Fraud and Abuse Act ("CFAA").[5]

The village commissioner felt she had been damaged by the unauthorized access of her e-mail account. However, no actual physical damage was done to her computer, nor did she suffer any measurable monetary loss as a result of the intrusion. In order to recover, she should not have to prove that she suffered actual measurable damages as a result of the unauthorized access to her computer. This comment will ex-

[*] J.D. Candidate, 2012, The John Marshall Law School. A special thank you to Kate Croteau for her support and patience and thank you to Professor Mary Nagel for her assistance.

[1] Steinbach v. Vill. of Forest Park, No. 06-C-4215, 2009 WL 2605283 at *1 (N.D. Ill. Aug. 25, 2009). These are the facts as alleged by the plaintiff, Theresa Steinbach against the Village of Forest Park, information services employee Craig Lundt, and village mayor Anthony Calderone. *Id.*

[2] *Id.*

[3] *Id.*

[4] *Id.*

[5] *Id.* at *2.

plore whether a civil plaintiff needs to claim actual damage to a protected computer to recover against a defendant under the CFAA.

Several courts have noted that there is little case law regarding damages, and the case law that exists does not help define the reach of damages.[6] Currently, courts are split as to whether a computer system needs to have actual physical damage in order for recovery under the CFAA. Additionally, courts have not adequately addressed how to assess damages, including whether damages may be aggregated across multiple computer systems. The Third, Fifth, and Ninth Circuit Courts of Appeals have held that plaintiffs do not need to show damage to a protected computer in order to recover under the CFAA.[7] However, the Seventh Circuit has stated that a litigant can only state a cause of action if there has been measurable damage to a protected computer.[8] This is a significant issue because, under the CFAA, specific criteria are used to show what constitutes a "protected computer."[9]

If the act requires a showing of actual damages to a protected computer, then civil litigants will be seriously limited in their ability to bring a cause of action. Issues also arise when multiple computers across a network are affected and damage to each individual computer does not reach the statutory minimum proscribed in the CFAA.[10] Litigants should be able to aggregate damages across multiple protected computers within an affected network.

This comment will argue that showing actual damages to a protected computer should not be required for a civil litigant to state a claim under the CFAA. Additionally, this comment will argue that damages should be aggregated across multiple protected computers to reach the jurisdictional damage amount. Furthermore, this comment will discuss how the courts have not sufficiently analyzed the CFAA.

Section II will discuss the background and history of the CFAA, including the present state of the Act, amendments to the Act, and current

[6] *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 584 (1st Cir. 2001).

[7] Fiber Sys. Int'l, Inc. v. Roehrs, 470 F.3d 1150, 1157 (5th Cir. 2006); P.C. Yonkers, Inc. v. Celebrations the Party & Seasonal Superstore, LLC, 428 F.3d 504, 511-12 (3d Cir. 2005); Theofel v. Farey-Jones, 359 F.3d 1066, 1078 n. 3 (9th Cir. 2004).

[8] *See* Kathrein v. McGrath, 166 Fed. Appx. 858, 863 n. 2 (7th Cir. 2006).

[9] 18 U.S.C. § 1030(a)(4) (2008). The term protected computer as defined by section 1030(e)(2) is a computer used:

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

Id. at 1030(e)(2).

[10] *See In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 524 (S.D.N.Y. 2001).

jurisprudence surrounding the Act. Section III will analyze the term "protected computer," the aggregation of damages, and what constitutes damages under the CFAA. Finally, Section IV will propose that the courts should liberally construe the term "protected computer" and find that a plaintiff need not show specific damages in order to recover under the CFAA.

Additionally, this comment will propose an amendment to the CFAA to clarify ambiguous language in the statute. The term, "protected computer," is far too narrow to protect potential victims if their computer systems are damaged. Furthermore, as will be demonstrated, current jurisprudence is varied and contradictory in defining how damages can be aggregated to meet the statutory minimum. Civil litigants need an avenue that provides them with the ability to pursue a cause of action against an alleged violator.

II. BACKGROUND

A. Current State of the Computer Fraud and Abuse Act

The CFAA has two components: a criminal penalty against those who violate it, as well as a civil remedy for those who may have been damaged by the violator.[11] In order to recover civilly, a plaintiff must show that the defendant accessed a protected computer without authorization and caused damages aggregating at least $5,000.[12] Generally, a protected computer is defined as a computer that is "used exclusively for the use of a financial institution of the United States" or "is used in or affecting interstate or foreign commerce or communication."[13] Recovery under the CFAA can be very broad; however, Congress intended that the $5,000 damage threshold must be met, regardless of how a court may construe the terms "damage" and "loss."[14]

The statute defines loss as "any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[15] Additionally, a Senate Report released in 1996 on the CFAA makes clear that Congress intended the term "loss" to account for addi-

[11] Bradley C. Nahrstadt, *Delete at Your Own Risk: Application of the Computer Fraud and Abuse Act, 18 U.S.C. § 1030,* Ill. Bus. L. J. 3 (May 6, 2006), *available at* http://www.iblsjournal.typepad.com/illinois_business_law_soc/2006/05_delete_at_your_1.htmls.

[12] 18 U.S.C. § 1030(a)(4).

[13] *Id.* at § 1030(e)(2)(a)(4).

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

[15] Forge Indus. Staffing, Inc. v. De La Fuente, No. 06 C 3848, 2006 U.S. Dist. LEXIS 75286 at *19 (N.D. Ill. Oct. 16, 2006).

tional lesser damages that could not be counted towards direct damage to an information system.[16] "Loss" is not meant to except certain injuries from the $5,000 damages threshold.[17]

Civil actions can be maintained for some, but not all of the CFAA's provisions.[18] A civil litigant must prove a two-part injury requirement in order to recover: there must be an underlying injury and a violation of one of the five statutory effects.[19] A person can pursue civil remedies if there was a loss to one or more computers aggregating $5,000 in damages, the modification or impairment of medical treatment, physical injury, a threat to public safety, or damage to a United States computer used for national defense or national security.[20] Legislative history states that although a victim may not suffer damage, they can still suffer loss. If the victim's loss meets the monetary minimum in the CFAA, then the victim is entitled to relief.[21] Under the CFAA, damages and losses can only be aggregated across victims for a single act.[22] This can be deduced from the statute from the way that section 1030(e)(8)(A) is phrased.[23] The section states, "any impairment to the integrity or availability of data, a program, a system or information that causes loss."[24] The statute places the damages required in the singular tense, not in the plural.[25] However, a criminal prosecution under the CFAA is not required in order for a successful civil suit. A civil litigant can only use certain portions of the CFAA to recover against a defendant.

[16] *In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 522 (S.D.N.Y. 2001).

[17] *Id.*

[18] Fiber Sys. Int'l v. Roehrs, 470 F. 3d. 1150, 1157 (5th Cir. 2006). "Civil actions are authorized for some, but not all, violations of Section 1030's substantive provisions." *Id.*

[19] ResDev, LLC v. Lot Builders Ass'n, Inc., No. 6:04-cv-1374-Orl-31DAB, 2005 U.S. Dist. LEXIS 19099 at *9 (M.D. Fla. Aug. 10, 2005). "The CFAA's private cause of action is principally defined by a two-part injury requirement; a plaintiff must suffer a certain type of root injury, which is not sufficient to support a civil action, unless one of the five operatively substantial effects occur." *Id.*

[20] 18 U.S.C. § 1030 (2008).

[21] S. Rep. No. 104-357, at 11 (1996). The report states that intruders often times alter computer log in programs, which allows hackers the ability to access a computer system. *Id.* The hacker then retrieves the stolen password. After he retrieves the password he restores the log in protocol to its original setting. *Id.* The report states that in this scenario no damage has been done to the computer system, yet the owners still suffer loss. *Id.* Loss is suffered because the owner has to spend time re-securing the system. *Id.*

[22] *In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 524 (S.D.N.Y. 2001).

[23] *Id.*

[24] *Id.* at 523.

[25] *Id.* According to the Court in *Doubleclick*, the legislative history supports this contention. *Id.* By using 'one or more others,' the Committee intends to make clear that losses caused by the same act may be aggregated for the purpose of meeting the [then] $1,000 threshold." *Id.* (citing S. Rep. No. 99-132).

B. The Computer Fraud and Abuse Act of 1984

Congress initially passed the Computer Fraud and Abuse Act in 1984.[26] The CFAA was the first comprehensive federal law aimed at computer crime.[27] Prior to the passage of the CFAA, Congress primarily relied on mail and wire fraud statutes in order to regulate crimes committed against computers.[28] As these crimes grew more sophisticated in nature, the wire and mail fraud statutes proved to be inadequate for crimes that did not involve interstate commerce.[29] Initially, the law was a criminal statute meant to protect computers owned by government and financial institutions.[30]

The first incarnation of the bill was meant to protect government computers that contained classified government information, government credit information, and financial sector information.[31] The Act was meant to protect against hackers and people who wished to damage and take advantage of computer systems.[32] The Act was intended to regulate interstate computer crime.[33] However, since the proliferation of the Internet, almost any computer could be considered interstate in character.[34] After the passage of the Act, its scope has been expanded dramatically.[35] With increased frequency, employers are using the CFAA to sue former employees who wrongfully seek information to achieve a competitive edge in the work place.[36]

[26] Reid Skibell, Comment, *Cybercrimes & Misdemeanors: A Reevaluation of the Computer Fraud and Abuse Act*, 18 Berkeley Tech. L.J. 909, 912 (Summer 2003).

[27] Megan M. LaBelle, *Working Together in a Digital World: An Introduction: The "Rootkit Debacle:" The Latest Chapter in the Story of the Recording Industry and the War on Music Piracy*, 84 Denv. U.L. Rev. 79, 102 (2006).

[28] Shaw v. Toshiba Am. Info. Sys., 91 F. Supp. 2d 926, 930 (E.D. Tex. 1999).

[29] *Id.*

[30] Graham M. Liccardi, Comment, *The Computer Fraud and Abuse Act: A Vehicle for Litigating Trade Secrets in Federal Court,* 8 J. Marshall Rev. Intell. Prop. L. 155, 158 (Fall 2008).

[31] Shurgard Storage Centers Inc. v. Safeguard Self Storage, 119 F. Supp. 2d 1121, 1126 (W.D. Wash. 2000). In *Shurgard*, the plaintiff owned self storage facilities. *Id.* As part of their business plan they had sophisticated marketing and computer software that was used to help further their business. *Id.* The defendant was also in the self storage business. *Id.* An employee of the plaintiff was working as an agent for the defendant. *Id.* In this capacity, the agent was funneling confidential information to the defendant via e-mail. *Id.*

[32] S. Rep. No. 101-544, at 3 (1990). "But [national and international computer networks] also provide a window of vulnerability that can be exploited by those who seek to abuse and undermine our computer systems." *Id.*

[33] *Shurgard*, 119 F. Supp. 2d at 1126.

[34] *Id.*

[35] *In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 524 (S.D.N.Y. 2001).

[36] *Id.*

C. The 1986 Amendments

After its passage, the Act was widely criticized as being too vague and too narrow.[37] In fact, Congress itself noted the deficiencies located within the CFAA.[38] In response to criticism, Congress amended the CFAA in 1986.[39] The overarching goal of the 1986 amendments to the CFAA was to draw a distinction between mere trespass and acts that caused more harm.[40] Additionally, the amendments created a hacking offense that was designed to punish those who altered the computer data of others.[41] Subsequent to the 1986 Amendments, Congress has amended the CFAA an additional eight times.[42]

D. The 1990 Amendments

Congress enacted the 1990 amendments to strengthen the CFAA as technology was rapidly progressing.[43] The 1990 CFAA amendments also greatly broadened the jurisdictional reaches of the Act. Under the 1990 amendments, the Act protected against computer abuses that have significant effects on interstate and foreign commerce.[44]

Congress had discussed creating a civil cause of action under the CFAA. A 1990 Senate Report stated that the proposed civil remedies under the Act "would create a civil cause of action for those who suffer violations of the Computer Fraud and Abuse Act."[45] In the 1990 Senate Report, all injuries were considered violations subject to the statutory minimum damage threshold, not just damages as defined by the statute.[46] A different Senate Report stated, "[t]he Committee intends to make clear that losses caused by the same act may be aggregated for the purposes of meeting the [then] $1,000 threshold."[47] There has been much discussion as to what damage is and what amount of damage is needed in order to recover under the CFAA.

[37] Skibell, *supra* note 26, at 912.

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*

[42] *Id.*

[43] S. Rep. No. 101-544, at 2 (1990). Senator Humphrey stated "[t]he national and international computer networks, which allow the rapid exchange of information and ideas provide one of the great benefits of modern computer technology." *Id.* at 3.

[44] S. Rep. No. 101-544, at 56 (1990). "The bill broadens jurisdiction for newly created sections of the Computer Fraud and Abuse Act, to cover all computers used in interstate commerce and communication." *Id.* at 6.

[45] S. Rep. No. 101-544, at 10 (1990).

[46] *In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 522 (S.D.N.Y. 2001).

[47] *Id.*

E. The 1994 Amendments

The 1994 amendments to the CFAA created civil remedies available to litigants.[48] The civil remedies portion was added to the statute as Section 1030(g).[49] Section 1030(g) allows any person who suffers a loss under sub-clauses I-V of subsection (c)(4)(A)(i) to bring an action for injunctive relief and damages.[50] A 1996 Senate report on the CFAA acknowledged the Act's shortcomings. The Senate report stated that gaps still existed because the Act did not cover damage to civilian or state owned computers.[51] Furthermore, damages for unauthorized access of information of non-classified information only extended to computers owned by financial institutions.[52] The CFAA has been amended by Congress in part to correct deficiencies and in part to keep the law current with the advancement of technology.

Some of the CFAA's amendments have dealt directly with the definitions of "damage" and "loss." In 1994, Congress defined damages in two ways: any impairment to the integrity or availability to a system and any way in which the Act prohibited.[53] Damages are limited to those that are economic in scope, unless the defendant intentionally or recklessly damaged a computer.[54] However, some courts struggled with how to accurately define "integrity" within the scope of the Act.[55]

[48] Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d. 667, 675 (E.D. Tex. 2001). "In 1994, Congress amended the CFAA and created a private right of action similar to that in section 1964(c) of the Racketeer Influenced and Corrupt Organization Act," thus, adding a civil remedy to a criminal statute. *Id.* at 675.

[49] Lockheed Martin Corp. v. Speed, No. 6:05-cv-1580-Orl-31KRS, 2006 U.S. Dist. LEXIS 53108, at *7 (M.D. Fla. Aug. 1, 2006). "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator." *Id.* at *7.

[50] 18 U.S.C. § 1030(g). A cause of action for civil damages can be brought if:

> (I) loss to 1 or more persons during any 1-year period (and for purposes of an investigation, prosecution, or other proceeding brought by the United States only, loss resulting for a related course of conduct affecting 1 or more other protected computers), (II) the modification or impairment, or potential modification or impairment, of medical examination, diagnosis, treatment, or care of 1 or more individuals; (III) physical injury to any person; (IV) a threat to public health or safety; (V) damage affecting computer used by or for an entity of the United States Government in furtherance of the administration of justice, national defense, or national security. *Id.* at (c)(4)(A)(i)(I-V).

[51] S. Rep. No. 104-357, at 4 (1996).

[52] *Id.*

[53] Skibell, *supra* note 26, at 915. Skibell states, "Congress intentionally refrained from making a list of prohibited actions to avoid being under-inclusive." *Id.* at 915.

[54] S. Rep. No. 104-357, at 12 (1996). "Damages are limited to economic damages, unless the defendant. . .intentionally caused damage, or recklessly caused damage while trespassing in a computer." *Id.* at 12.

[55] World Span L.P. v. Orbitz L.L.C., No. 05 C 5386, 2006 U.S. Dist. LEXIS 26153, at *14 (N.D. Ill. Apr. 19, 2006). "The CFAA does not define 'integrity,' but the dictionary

F. The 1996 Amendments

From the time of the CFAA's inception, Congress has consistently broadened the reach and terms of the Act. Congress was aware that the CFAA would have to be expanded as technology evolved, because at its beginnings the Act dealt with computer crime generally.[56] The 1996 amendments to the CFAA added the term "protected computer," which replaced the term "federal interest computer."[57] As technology progresses, the circumstances under which a computer will suffer actual physical damage will likely be less than the amount of money companies will spend in order to recover from an attack, as well as the cost of securing computers against continued attempted virtual assaults by hackers.[58] A Senate report on the CFAA stated that the Act needed to be sufficiently broad in order to anticipate developments in computers and technology.[59]

G. The 2001 Amendments

The CFAA was amended again in 2001 to include, among other changes, the term "loss" in the discussion of damages.[60] In the 2001 version of the CFAA, "loss" includes costs to the victim associated with the violation by the offender.[61] More broadly, loss is defined as any reasona-

definition is 'an unimpaired or unmarred condition: entire correspondence with an original condition: soundness.'" *Id.* at *14.

[56] United States v. Middleton, 231 F.3d 1207, 1212 (9th Cir. 2000). This case cited a Senate report on the CFAA stating: "[a]s computers continue to proliferate in businesses and homes, and new forms of computer crime 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." *Id.* at 1212.

[57] Shurgard Storage Centers Inc. v. Safeguard Self Storage, 119 F. Supp. 2d 1121, 1128 (W.D. Wash. 2000).

[58] *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001).

[59] S. Rep. No. 104-357, at 11 (1996). "As the NII system. . .continues to grow, computers will increasingly be used for access to critical services. . .and will be critical to other systems which we cannot yet anticipate. Thus, the definition of "damage" is amended to be sufficiently broad to encompass the types of harm against which people should be protected." *Id.* at 11.

[60] Creative Computing v. Getloaded L.L.C., 386 F.3d 930, 934 (9th Cir. 2004). In *Creative Computing*, Getloaded attempted through several avenues, including hacking, the creation of fake profiles, and the hiring of Creative Computing employees to gain unauthorized access to Creative Computing's website. *Id.* The case was before the Ninth Circuit Court of Appeals because Getloaded was appealing the entry of a permanent injunction against its access to Creative Computing's website. *Id.*

[61] *Id.* "'Loss' is defined in the new version as 'any reasonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data. . .and any revenue lost, cost incurred, or other consequential damages incurred because of the interruption of service.'" *Id.*

ble cost associated with the damage done by the defendant.[62] Losses and damages must meet the statutory minimum of $5,000, but need not be shown for each intrusion into the protected computer but can be aggregated over the course of one year.[63] The legislative history clearly states that Congress intended the term "loss" to target expenses undertaken by the victim to correct indirect damage incurred as a result of a hacker.[64] Although a victim's systems may not be physically damaged, the fact that outside consultants had to be hired to fix the intrusions by hackers does not mean that the victim did not suffer loss as defined by the statute.[65] However, both loss and damage are required in order to recover under the CFAA.[66]

H. Court Interpretation of the CFAA

Courts have struggled to determine what is considered loss and what accounts for damages under the CFAA. The Ninth Circuit has included damages under the CFAA to mean a measurable loss of data, steps taken to restore that data, or costs associated with re-securing the data.[67] Additionally, a plaintiff can determine the amount of loss for damages to include costs incurred to restore programs, systems, and data that the defendant may have damaged.[68]

Judge Thad Heartfield, a federal judge sitting in the United States District Court for the Eastern District of Texas, has held that, absent a substantive violation, plaintiffs are barred from recovery.[69] In this case, the court accepted the Department of Justice's ("DOJ") interpretation of the CFAA and included it in determining what constitutes damage under the CFAA, holding that $5,000 in damage must be done to an individual

[62] ResDev, LLC v. Lot Builders Ass'n, Inc., No. 6:04-cv-1374-Orl-31DAB, 2005 U.S. Dist. LEXIS 19099 at *16 (M.D. Fla. Aug. 10, 2005).

[63] *See* Fiber Sys. Int'l v. Roehrs, 470 F.3d 1150, 1157 (5th Cir. 2006).

[64] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 585 (1st Cir. 2001). "Congress intended the term 'loss' to target remedial expenses borne by the victims that could not properly be considered direct damages caused by a computer hacker." *Id.* (citing *In re Doubleclick Inc. Privacy Litig.*, 154 F. Supp. 2d 497, 521 (S.D.N.Y. 2001)).

[65] *See Explorica*, 274 F.3d at 584-85.

[66] Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667, 678 (E.D. Tex. 2001). "Nowhere in the plain language of 18 U.S.C. Section 1030(g) is 'loss' defined as an alternative to showing a substantive violation of the CFAA. The statute expressly mandates 'loss by reason of a violation.'" *Id.*

[67] United States v. Middleton, 231 F.3d 1207, 1213 (9th Cir. 2000). The criminal defendant was convicted of illegally accessing e-mail accounts of Slip.net's employees after he was let go as an employee. *Id.* at 1208. He deleted accounts and created new accounts. *Id.* at 1209. He unsuccessfully argued on appeal that the trial court incorrectly instructed the jury on the definition of damage under the CFAA. *Id.* at 1213.

[68] *Id.* at 1213.

[69] *Thurmond*, 171 F. Supp. 2d at 675.

computer and cannot be spread across a series of computers.[70] Additionally, the Northern District of Illinois explicitly stated that a cause of action can only be brought if damage and loss is affirmatively plead.[71]

Courts seem to be split on whether civil plaintiffs must allege damage in order to state a claim under the Act.[72] The United States Court of Appeals for the First Circuit said that "[f]ew courts have endeavored to resolve the contours of damage and loss under the CFAA."[73] Some courts, like the Seventh Circuit Court of Appeals, have held that damages are required in order to state a claim under the CFAA.[74] For example, the Seventh Circuit stated that installing a program that was intended to delete files is a sufficient showing of damages under the CFAA.[75] The court implied that no actual physical damage needed to be done to the computer, but the simple act of deleting programs and software was enough to constitute damages under the CFAA.[76] Judge Terrence F. McVerry, sitting in the Western District of Pennsylvania, ruled that a plaintiff could maintain a cause of action under the CFAA because the hiring of an outside consultant to analyze the company's computer systems exceeded the jurisdictional amount of $5,000.[77] The implication under this scenario is that loss could be further defined as hiring a specialist to determine what sensitive data could have been

[70] *Id.* at 680-81 (citing *Cybercrime*: *Hearing Before the Subcomm. on Commerce, Justice and State; Judiciary and Related Agencies of the S. Comm. on Appropriations*, 106th Cong. 13 (2000) (Statement of Janet Reno Attorney General of the United States)).

[71] Garelli Wong & Assoc., Inc. v. Nichols, 551 F. Supp. 2d 704, 708 (N.D. Ill. 2008). "A thorough reading of the [act] shows that it is necessary for a plaintiff to plead both damage and loss in order to properly allege a civil CFAA violation." *Id.*

[72] *See, e.g.,* Kathrein v. McGrath, 166 Fed. Appx. 858, 863 n. 2 (7th Cir. 2006) (stating "[a] violation can occur, however, only where there is damage to a 'protected computer'"); Int'l Airport Centers L.L.C. v. Citrin, 440 F.3d 418, 419 (7th Cir. 2006) (stating "damage" includes "any impairment to the integrity or availability of data, a program, a system or information").

[73] EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 584 (1st Cir. 2001) (noting only two district courts have directly addressed the issue of damages under the CFAA).

[74] *See Kathrein*, 166 Fed. Appx. at 863. In *Kathrien*, Michael Kathrien created a website about his ex-wife's new husband, Michael Monor that depicted him in various sexual and pornographic situations. *Id.* at 859. In its decision on other various unrelated claims, the Court stated in a footnote that a violation of the CFAA can only occur where there is damage to a protected computer. *See Id.* at 863 n.2.

[75] *Citrin*, 440 F.3d at 419. The court stated:

> we don't see what the difference the precise mode of transmission can make. In either the Internet download or the disk insertion, a program intended to cause damage, not to the physical computer, of course, but to its files—but "damage" includes "any impairment to the integrity or availability of data, a program, a system or information." *Id.*

[76] *Id.*

[77] Hudson Global Res. Holdings, Inc. v. Hill, No. 02:07cv 132, 2007 U.S. Dist. LEXIS 14840, at *5-6 (W.D. Pa. Mar. 2, 2007).

damaged, as well as the costs associated with upgrading security features.

In contrast, some courts have taken a narrower approach to loss and damages under the CFAA.[78] In a case from the Second Circuit Court of Appeals, a company claimed that the defendant's violation of the CFAA caused $10 million in damage.[79] Under the Act, the Second Circuit explained that lost revenue is different from costs incurred from an "interruption of service."[80] Additionally, the Second Circuit held, citing to a Southern District of New York case, that a loss of good will and business could not be used to calculate loss and damages unless it resulted directly from the impairment of a computer system.[81] On appeal the Second Circuit upheld the district court's ruling that travel expenses incurred as a result of traveling to respond to a computer offense cannot be used to calculate loss under the CFAA.[82]

When calculating compensatory damages under the CFAA, a plaintiff is not entitled to investigator's fees simply because they are a natural and foreseeable result of damage done by a defendant.[83] Any loss not associated with computer impairment or computer damage is barred from monetary recovery.[84] A civil litigant can include costs of investigating the amount of damage done to a computer system in the loss analysis, but cannot include investigating costs that are incurred in a search for who might have actually hacked the computer system.[85]

I. THURMOND ET AL V. COMPAQ COMPUTER CORP.

In *Thurmond v. Compaq Computer Corp.*, the court ruled that damages could not be aggregated among prospective class members to meet the $5,000 threshold.[86] Damages could not be aggregated because the

[78] *See*, *e.g.*, Nexan Wires S.A. v. Sark-USA, Inc., 166 Fed. Appx. 559, 561 (2d Cir. 2006).

[79] *Id.*

[80] *Id.* at 562.

[81] *Id.* (citing *Register.com Inc. v. Verio*, *Inc*, 126 F. Supp. 2d 238, 252 n.12 (S.D.N.Y. 2000)).

[82] Nexan Wires S.A. v. Sark-USA, Inc., 319, F. Supp. 2d 468, 473 (S.D.N.Y. 2004), *aff'd,* 166 Fed. Appx. 559 (2d Cir. 2006).

[83] Tyco Int'l (U.S.) Inc. v. John Does 1-3, No. 01 Civ. 3856, 2003 U.S. Dist. LEXIS 11800, at *3 (S.D.N.Y. July 11, 2003).

[84] Civic Ctr. Motors, L.T.D. v. Mason St. Imp. Cars, L.T.D., 387 F. Supp. 2d 278, 382 (S.D.N.Y. 2005).

[85] *Tyco Int'l*, 2003 U.S. Dist. LEXIS 11800 at *5. "Although the court in *Middleton,* uses the word 'investigating,' it is clear from both the court's language ('investigating. . .the *damage*') and the facts of the case that this investigation involved only assessing the damage to the system-not locating and collecting information about the hacker." *Id.*

[86] Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d. 667, 680 (E.D. Tex. 2001); *see also* LaBelle, *supra* note 27, at 103.

statute requires that the damage must be done to a "protected computer" meaning one computer, not many.[87] The *Thurmond* court cited the congressional testimony given by Justice Department officials, including the then Attorney General Janet Reno and Deputy Attorney General Eric Holder.[88] Both testified before various committees that were considering amendments to the CFAA. Relying heavily on the testimony offered by Justice Department officials, the *Thurmond* court reached the conclusion that if Congress had wanted to allow for an aggregation of damages across multiple computers, it would have specifically written language into the statute that would have permitted it.[89]

J. In Re Doubleclick Inc. Privacy Litigation

In *Doubleclick,* the Court reached the conclusion that damages could only be aggregated across victims for a single act by the defendant.[90] However, the court reached its decision on a different analysis of the statute.[91] The *Doubleclick* court looked to the legislative history to conclude that Congress only used the singular form of certain words in the statute and that this decision meant only a single act could be used to determine that "losses caused by the same act may be aggregated for the purposes of meeting the . . threshold."[92] Thus, the court ruled that the accessing of data on millions of computers, in potential violation of the CFAA, could not constitute a single act under the statute.[93]

K. In Re America Online, Inc. Version 5.0 Software Litigation

In *America Online,* the court was highly critical of the results reached in both *Thurmond* and *Doubleclick* pertaining to the analysis

[87] *Thurmond*, 171 F. Supp. 2d. at 680; *see also* LaBelle, *supra* note 27, at 104.

[88] *Thurmond*, 171 F. Supp. 2d. at 680-81. "The Justice Department's understanding of the statute suggests "damage" must be to an individual computer." *Id*. (interpreting *Cybercrime*: *Hearing Before the Subcomm. on Commerce, Justice and State; Judiciary and Related Agencies of the S. Comm. on Appropriations*, 106th Cong. 13 (2000) (Statement of Janet Reno Attorney General of the United States) and *Internet Denial of Service Attacks and the Federal Response: Joint Hearing Before the Subcomm. on Crime of the H. Comm. on the Judiciary and the Subcomm. on Criminal Justice Oversight of the S. Comm. on the Judiciary,* 106th Cong. 95 (2000) (Testimony of Eric Holder, Esq., United States Deputy Attorney General, Dept. of Justice)).

[89] *Thurmond*, 171 F. Supp. 2d. at 681. "If Congress intended otherwise, it would have provided for either transmission 'to a protected computers;' or the transmission to all "protected computers.'" *Id.*

[90] *See In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 523 (S.D.N.Y. 2001).

[91] LaBelle, *supra* note 27, at 105.

[92] *Doubleclick*, 154 F. Supp. 2d at 524 (citing S. R. No. 99-432, at 2483 (1986)). The court went on to explain that "[t]he prohibition is phrased in the singular: "[whoever] intentionally accesses a computer without authorization. . .and thereby obtains. . .information from any protected computer." *Id.*

[93] *Id.*

regarding damages.[94] Judge Alan Gold stated that the courts in *Thurmond* and *Doubleclick* did not properly analyze the term "protected computer" in regard to the CFAA.[95] Additionally, Judge Gold reasoned that the *Thurmond* court did not properly apply legislative history.[96] Judge Gold stated that instead of looking to the legislative history as the *Thurmond* court purported to do, the court instead cited a comment by then Attorney General Janet Reno.[97] Judge Gold argued that the analysis offered by the attorney general was not a strong indication of what Congress intended when it adopted the CFAA.[98] In sum, Judge Gold stated that the conclusions reached by the *Thurmond* and *Doubleclick* courts would lead to absurd results when a litigant was pursuing a civil action under the CFAA.[99]

III. ANALYSIS

A. Statutory analysis

Key to this comment are principles of statutory analysis. How courts analyze a statute becomes particularly important when certain provisions are ambiguous. The cases discussed suggest that the first step in a statutory analysis is to determine whether the language at issue has a "plain and unambiguous meaning" within the terms of the dis-

[94] *See In re* Am. Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1373 (S.D. Fla. 2001) (refusing to adopt the reasoning of *Thurmond* and *Doubleclick* courts).

[95] *Id.* "Most importantly, in *Thurmond* and *Doubleclick*, the courts found the statutory language to be clear, ignored the comma that precedes "to a protected computer," and overlooked the fact that the phrase was a dangling participle." *Id.*

[96] *Id.*

[97] *Id.* The court stated that Attorney General Janet Reno's statements "are not a reliable indication of what both Houses of Congress intended when they adopted the [CFAA]). *Id.* Attorney General Janet Reno stated, "we may need to strengthen the Computer Fraud and Abuse Act by closing a loophole that allows computer hacker who have cause a large amount of damage to a network of computers to escape punishment if no individual computer sustained over $5,000 worth of damage." *Id.*

[98] *Id.*

[99] *Id.* at 1374. The court held:

> [the *Thurmond* and *Doubleclick* courts' interpretation] of the [CFAA] would lead to the absurd result that a party who accesses one computer without authorization, and thereby causes $5,000 worth of damage to that one computer, would be guilty of violating the CFAA and, therefore, civilly liable. On the other band, a party who accesses millions of computers and causes only $100 worth of damage to each computer would not be guilty of violating the CFAA. *Id.*
>
> *See also* LaBelle, *supra* note 27, at 104. The result would be absurd because if a party accessed a computer without authorization and caused $5,000 worth of damage to one computer they would be civilly liable. *Id.* However, if a party access millions of computers and does only $100 worth of damage no violation of the CFAA would be present. *Id.*

pute.[100] If the statute is ambiguous, the courts will proceed to the next step of statutory analysis.[101] Generally, if a court finds that a term is ambiguous, it will look outside the four corners of the statute to other sources, such as the legislative history and other outside materials to determine what Congress intended.[102] Despite similar facts and the same principles of statutory construction, several courts have reached vastly different results when interpreting the CFAA.[103]

B. Ambiguities are present in the CFAA

The damage requirement section of the CFAA contains ambiguous statutory language.[104] The court in *America Online* pointed out an issue with a dangling participle in the language and how it has caused confusion.[105] The Supreme Court has noted that a dangling participle can be particularly troubling in statutory language.[106] The court in *America Online* notes how this deficiency creates uncertainty under the CFAA.[107] The language in the CFAA is unclear as to whether a defendant must knowingly cause a transmission of a program or whether a defendant must intentionally cause damage.[108] Ambiguity is present in the damages language of the CFAA as to what a plaintiff is required to show in order to establish that a computer has been damaged.

The Supreme Court has ruled that when a statute is ambiguous, a court may turn to the legislative history to determine the legislature's

[100] *See* ResDev, LLC v. Lot Builders Ass'n, Inc., No. 6:04-cv-1374-Orl-3 1DAB, 2005 U.S. Dist. LEXIS 19099 at *3 (M.D. Fla. Aug. 10, 2005); *see also In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 520 (S.D.N.Y. 2001); *see also In re* Am. Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1369 (S.D. Fla. 2001) (stating "[a] court must assume that Congress used the words in the a statute as they are commonly and ordinarily understood, and if the statutory language is clear, no further inquiry is necessary."); *see also* Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d. 667, 677 (E.D. Tex. 2001) (stating "[t]o interpret statutory terms, the Court looks first looks to the plain language of the statute, examining, 'the statute as a whole, including its design, object, and policy'") (citing *New York Life Ins. Co. v. Deshotel*, 142 F.3d 873, 885 (5th Cir.1998)).

[101] Robinson v. Shell Oil Co., 519 U.S. 337, 340-41 (1997).

[102] *Am. Online*, 168 F. Supp. 2d at 1369. "If the statutory language is ambiguous, a court may examine extrinsic materials, including legislative history, to determine Congressional intent." *Id.*; *see also Doubleclick*, 154 F. Supp. 2d at 520; *see also ResDev*, 2005 U.S. Dist. LEXIS 19099 at *3.

[103] *Compare Am. Online*, 168 F. Supp. 2d 1359 *with Doubleclick*, 154 F. Supp. 2d 497.

[104] *Am. Online*, 168 F. Supp. 2d at 1372 (discussing 18 U.S.C. § 1030(a)(5(A) (2008)).

[105] *Id.* (explaining that the language of the § 1030(a)(5) is particularly troubling because it leaves open for interpretation that damages could or could not be aggregated across multiple computers).

[106] Young v. Cmty. Nutrition Inst., 476 U.S. 974, 980-81 (1986) (stating "[a]s enemies of the dangling participle well know, the English language does not always force a writer to specify which of two possible objects is the one to which a modifying phrase relates").

[107] *Am. Online*, 168 F. Supp. 2d at 1372.

[108] *Id.*

intent.[109] However, relying solely on the testimony of justice department officials is not the best approach to ascertain Congressional intent in the CFAA.[110] The court in *Thurmond* incorrectly relied on the Attorney General's statements to conclude that damages cannot be aggregated across multiple computers.[111] Conversely, the court in *America Online* correctly relied on a Senate report that was released in conjunction with the original CFAA in 1986.[112] Senate Report 99-474 stated that certain malicious acts may cause less than the statutory threshold, but according to the specific language in the statute, the committee made clear that the same actions that caused the losses resulting from the same act may be aggregated to reach the damage minimum.[113]

C. Legislative history of the CFAA

Several key Senate reports have addressed the legislative intent of the CFAA's provisions. From the legislative history, it is evident that Congress has been concerned with keeping the CFAA up to date with advancements in technology. As computer criminals have become more sophisticated in their deviant actions, the legislature must constantly change the law to stay in line with technological advancements.[114] Congress has been cognizant that ambiguities have existed in the CFAA, which is why the amendments have attempted to clarify some of those ambiguities.[115]

With the advent and development of the Internet, Congress likely would intend for the statute to allow for the aggregation of damages across multiple computers and computer systems. Senator Humphrey

[109] *Young*, 106 S. Ct. at 979-81 (1986). The use of a dangling participle does create ambiguity in the CFAA. Thus, court should use legislative history to interpret the CFAA.

[110] *See In re* Am. Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1373 (S.D. Fla. 2001) (explaining the Attorney General's statements "are not a reliable indication of what both Houses of Congress intended when they adopted the statutory language in question").

[111] Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d. 667, 680-681 (E.D. Tex. 2001).

[112] *Am. Online*, 168 F. Supp. 2d at 1373. "In fact, the predecessor versions of the CFAA make it clear that damage is to be measured as it stems from one act, not a single computer, and thereby affects several individuals." *Id.* (discussing S. Rep. No. 99-474, at 2483 (1986)).

[113] S. Rep. No. 99-474, at 2483 (1986).

> Certain types of malicious mischief may cause smaller amounts of damage to numerous individuals, and thereby collectively create a loss of more than $1,000 [original damage amount]. By using "one or more others," the Committee intends to make clear that losses caused by the same act may be aggregated for the purposes of meeting the. . .threshold. *Id.*

[114] S. Rep. No. 101-544, at 4 (1990). "A primary focus of the legislation is to avoid the complications and ambiguities created by certain language in the current CFAA." *Id.*

[115] *Id.* at 5.

noted, "[i]t is important that we update our computer crime laws to stay abreast of the rapid changes in computer abuse technologies."[116] As technology has progressed, Congress has attempted to keep up with the advancements through the various amendments to the CFAA.[117] Amendments have specifically addressed issues pertaining to newly discovered forms of malicious computer use.[118] Some forms of malicious computer use that the amendments to the CFAA have addressed include destructive worms and viruses that could be released and cause damage to a computer network.[119] Congress has consistently intended for the CFAA to be a pertinent tool for law enforcement and civil litigants in prosecuting malicious computer use.

From the legislative history attached to the CFAA, it is clear that Congress has used the CFAA to properly protect computers users from those who wish to exploit technology. For instance, included in a discussion of the 1996 amendments to the CFAA, Congress broadened "damages" to include damage to computer systems both from insiders and outsiders who intentionally damage a computer system.[120]

D. Court reliance on legislative history

The *Shurgard* court properly applied the legislative history of the CFAA when it denied the defendant's motion to dismiss, based in part, on the claim that the CFAA was intended only to apply to industry computers that, if damaged, could affect the public's privacy interests.[121] The court noted that the defendant's analysis of the legislative history was incorrect.[122] The court stated that, although sections of the act supported both the plaintiff and the defendant, the history supporting the plaintiff's analysis was far more convincing.[123] The *Shurgard* court, in reading the legislative history, broadly applied the CFAA. In doing so, the Court understood that Congress intended for the CFAA to adapt to the changes in computer technology and infrastructure. The *Shurgard* court explained that the scope of the CFAA extends to suits involving alleged wrongful conduct between two individual companies where the

[116] *Id*. at 4.

[117] *Id.* "In response to changes in computer technology and the threat posed by new techniques for creating and transmitting malicious programs and codes," amendments, to the CFAA were proposed in 1990. *Id.*

[118] *Id.* at 2. "The legislation amends the Computer Fraud and Abuse Act of 1986, 18 U.S.C. 1030, to strengthen and clarify the application of Federal law to newly discovered forms of computer abuse." *Id.*

[119] *See Id.* at 2.

[120] S. Rep. No. 104-357, at 9 (1996).

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

[122] *Id.*

[123] *Id.* at 1128.

information wrongfully obtained may not extend to the public at large.[124] This court's analysis takes a broad view of the CFAA, and in doing so, correctly construes Congress's intent for the statute as an effective means to fight damage to computer systems.

In *ResDev v. Lot Builders*, the court was highly critical of the conclusion that was reached in *Shurgard*.[125] The *ResDev* court argued that the *Shurgard* court's application of legislative history was incorrect and stretched the meaning of the statute too far.[126] As stated earlier, the CFAA is ambiguous in regards to damages and the types of computers and computer systems that the CFAA protects.[127] The court in *ResDev* was highly critical of legislative history, but legislative history shows Congress' intent clearer than the sources on which the court relied.[128] The *ResDev* court turned to, among other sources, Black's Law Dictionary and Eleventh Circuit Pattern Jury Instructions, to help it determine the meaning of words within the CFAA.[129] While both of these are reputable sources, they do not reflect the intent of Congress.

ResDev court's criticism is unfounded because a court should examine the legislative history if the language of the statute is not clear. The court in *ResDev* should have turned to the legislative history instead of other sources to determine the intended meaning of the CFAA. The *ResDev* court would have benefited from looking at the legislative history of the CFAA to help it determine Congress's intent for the CFAA. The *ResDev* court was highly critical of the use of legislative history in general.[130] The *ResDev* court stated that legislative history should be only used if the language of the statute produces a ridiculous result.[131]

[124] *Id.* The court noted that the legislative history suggests a "broad reading" of the terms "protected computer" and "without authorization." *Id.* 1129. The court determined that someone who violates the CFAA could be liable if intellectual property rights are involved as well as someone who wrongfully accessed a computer for commercial gain. *Id.*

[125] ResDev, LLC v. Lot Builders Ass'n, Inc., No. 6:04-cv-1374-Orl-3 1DAB, 2005 U.S. Dist. LEXIS 19099 at *13 (M.D. Fla. Aug. 10, 2005).

[126] *Id.* (stating "[a]nother thing that detracts from *Shurgard* is its heavy reliance on legislative history").

[127] *See In re* Am. Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1372 (S.D. Fla. 2001).

[128] *ResDev*, 2005 U.S. Dist. LEXIS 19099 at *8.

[129] *Id.* The court used Black's Law Dictionary in an attempt to help the court define "loss" and "damages." *Id.* at 10-11. Then the Court turned to the Eleventh Circuit Pattern Jury instructions in an attempt to help define "economic damages." *Id.* at *9-10.

[130] *Id.* at *3.

[131] *Id.* "[A] court should resort to extrinsic materials, such as legislative history, only if the statutory language produces a clearly absurd result or presents substantial ambiguity." *Id.* at *6.

E. Aggregation of damages

There is a split among the federal courts as to whether a litigant may aggregate damages and to what extent a litigant can aggregate damages in a potential lawsuit under the CFAA.[132] This split leads to a lack of clarity as to whether a plaintiff can aggregate damages. Few courts have attempted to resolve the ambiguous language in the CFAA regarding whether damages can be aggregated, as well as what actually constitutes damage under the statute.[133] Adding to the ambiguity are the Justice Department's analysis and interpretation of portions of the Act.[134]

In *America Online*, the court noted that the analysis offered by the attorney general and the deputy attorney general may contradict the language of the statute.[135] Additionally, Congress' legislative history is more convincing about its intent than the interpretation of the statute offered by DOJ officials. Like nearly every stakeholder involved within the legislation, the DOJ has an agenda when it offers its comments and opinions on legislation. While the DOJ's analysis could be persuasive, it should not be mistaken as Congress' intent in regards to a certain statute, like the CFAA. Litigants should be allowed to aggregate damages because Congress has clearly intended that the CFAA should be able to adapt along with fast growing computer technology.[136] As a result of these analyses, it is clear that plaintiffs who bring suit under the CFAA should be allowed to aggregate the $5,000 damage threshold across multiple computers. Additionally, litigants should be able to rely on a liberal construction of the term "damage" because Congress has intended the CFAA to be an effective tool in fighting malicious computer activity.

In *Creative Computing v. Getloaded.com*, the Ninth Circuit Court of Appeals initially looked to the legislative history of the CFAA, but then ultimately dismissed the suit, instead, turning on what it deemed to be the clear language of the statute.[137] However, in its decision, the court analyzed a portion of the legislative history pertaining to the aggregation

[132] LaBelle, *supra* note 27, at 104.

[133] *See* EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577 (1st Cir. 2001).

[134] *See In re* Am. Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359 (S.D. Fla. 2001). Certain Justice Department officials offered Congressional testimony that may contradict the language of the CFAA.

[135] *See Id.* at 1373.

[136] *See generally* S. Rep. No. 104-357 (1996); S. Rep. No. 101-544 (1990).

[137] Creative Computing v. Getloaded L.L.C., 386 F. 3d 930, 934 (9th Cir. 2004). "It makes no sense to parse the ambiguous legislative history as though it were law. The preferable way to resolve linguistic ambiguity is to evaluate the alternative readings in light of the purpose of the statute." *Id.*

of damages under the Act.[138] The Court noted that the language in the legislative history pertaining to the aggregation of damages was permissive, not restrictive.[139] Here, the *Creative Computing* court correctly turned to the legislative history. In doing so, the court broadly construed the statute by determining that the aggregation of damages was permissive. The court was taking into account Congress's intent that the statute be flexible to handle changes in technology and computer systems. Thus, according to the Ninth Circuit in its interpretation of the legislative history, the aggregation of damages across a one year period is allowed.

F. Restrictive interpretations of the CFAA

In *Nexan Wires S.A. et al v. Sark-USA, Inc.*, the Southern District of New York court adopted a much narrower reading of the term "loss" as pertaining to the damage analysis under the CFAA.[140] In granting the defendant's summary judgment motion, the court noted that lost revenue not related to the interruption of a computer service could not be used by a plaintiff to determine the $5,000 damage threshold.[141] The court held that the loss must be tied directly to the interruption or impairment of a computer system.[142] In affirming the decision, the Second Circuit Court of Appeals noted that because there was no interruption of services, the plaintiff could not assert their losses under the CFAA.[143]

The statutory definition of loss should be expanded slightly from the *Nexan Wires* court's interpretation. If a hacker is able to steal business documents and use them for profit, it could be reasoned that the victim has lost revenue as a result of the hacker's malicious activity. Simply because there is no interruption of service, does not automatically mean that the victim has not suffered a loss. The terms "damage" and "loss" under the CFAA should be construed liberally, so that when a hacker designs a new way to damage a computer, a potential victim will have the ability to fight back effectively. Additionally, Congress has consistently stated that it wants the CFAA to stay abreast of the technology so that the Act remains an effective tool to for victims.

In *Tyco International v. John Does 1-3,* the Southern District of New

[138] *Id.* The portion analyzed by the court was "the Committee intends to make clear that losses caused by the same act may be aggregated for the purposes of meeting the. . .threshold." *Id.*

[139] *Id.* "The obvious purpose of this remark was permissive, to allow aggregation to meet the $5,000 floor, as when one intrusion causes one expense after another for months." *Id.*

[140] *See* Nexan Wires S.A. v. Sark-USA, Inc., 319, F. Supp. 2d 468, 473 (S.D.N.Y. 2004).

[141] *See Id.*

[142] *See Id.* at 477.

[143] Nexan Wires S.A. v. Sark-USA, Inc., 166 Fed. Appx. 559, 561 (2d Cir. 2006).

York took a restrictive view of damages.[144] The court did not turn to principles of statutory analysis and relied solely on the plain language of the statute.[145] The court noted that while the CFAA allows for recovery of losses beyond physical damage, that damages above and beyond physical damages have been restricted by other courts.[146] The *Tyco* court reached the conclusion that a plaintiff could not include in its damage claim money spent attempting to locate who hacked its system.[147] The *Tyco* court did not turn to the legislative history because the court found that the language was clear. Even though the *Tyco* court did not turn to legislative history to reach its decision, the court did rely on another court's decision that incorrectly applied the legislative history of the CFAA, which led to a decision that took a restrictive view of damages under the statute.[148]

The *Tyco* court analysis is a far too restrictive interpretation of the CFAA. Damages need to be construed liberally in order for the statute to be effective. Furthermore, it is not too difficult to reason that money spent on attempting to locate a hacker could be used in the damage assessment, because the hacker could repeatedly access a computer system, which could lead to continued and repeated loss and damage to a system. If the hacker is found, the unauthorized access would be halted.

G. Same history, different outcomes

In *Register.com Inc. v. Verio*, Second Circuit Court Judge Fred Parker, in a published draft opinion, held that the plaintiff would not be able to reach the $5,000 damage threshold.[149] The plaintiff alleged that the defendant's actions consistently slowed its response time to its customers.[150] Circuit Judge Parker relied on the reasoning reached by the *Shurgard* court.[151] In using the statutory and legislative analysis found in *Shurgard*, Judge Parker reached the conclusion that merely because the plaintiff's system was slowed, this did not show enough damage to prove that the plaintiff could meet the $5,000 damage threshold that the

[144] *See* Tyco Int'l (US) Inc. v. John Does 1-3, 2003 U.S. Dist. LEXIS 11800 (S.D.N.Y. July 11, 2003). In *Tyco*, the plaintiff was looking to recover damages for attempting to track down the person responsible for hacking their computer system. *Id.* at *2.

[145] *See Id.*

[146] *Id.* at *4 (stating, "[d]amages awarded by courts under the Act have generally been limited to those costs necessary to assess the damage caused to the plaintiff's computer system or to resecure the system in the wake of a hacking").

[147] *See Id.*

[148] *In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 521 (S.D. N.Y. 2001).

[149] *See* Register.com, Inc. v. Verio, Inc., 356 F.3d 393, 438 (2d Cir. 2004).

[150] *See Id.*

[151] *See Id.* Circuit Judge Parker relied heavily on the reasoning found in *Shurgard*. *Id.* at 439-40. He said of *Shurgard,* the statutory analysis is "excellent" and the opinion conducts a "thorough search" of the legislative history. *Id.*

CFAA requires.[152] The draft opinion in *Register.com* is an excellent example of how two different courts can use the same legislative history and the same general ideas of statutory construction to reach two differing views. Further, it illustrates why Congress needs to amend the CFAA to eliminate the ambiguities and to continue to keep the statute relevant as technology progresses.

In *EF Cultural Travel v. Explorica*, the First Circuit Court of Appeals, after conducting a statutory analysis, reached the conclusion that the plaintiffs would most likely succeed on the merits of their CFAA claim and thus were entitled a preliminary injunction.[153] In doing so, the court adopted a broad reading of the term "damage."[154] The court concluded that the absence of actual physical damage did not mean that the plaintiff did not suffer damages under the meaning of the CFAA.[155] The court noted that to read the CFAA differently would impair the scope beyond what Congress intended.[156] The court in *EF Cultural Travel* relied on language in Senate Report 104-357 to reach the conclusion that damages could extend to expenses that the plaintiff incurred that could not be considered direct damage that occurred as a result of the violation.[157] The *EF Cultural Travel* court understands that a broad reading of the CFAA is needed in order to properly protect networks and computer systems. In using legislative history, the *EF Cultural Travel* court read a broad view of the CFAA that will allow for its adaptation as technology develops.

Judge Naomi R. Buchwald, sitting in the Southern District of New York, ruled in *Doubleclick* that the plaintiffs could only aggregate damages for a single act by the defendant.[158] In that decision, Judge Buchwald relied on the legislative history of the CFAA to reach her conclusion.[159] The *Doubleclick* court reasoned that the CFAA is ambiguous as to whether "loss" under the CFAA is subject to the $5,000 threshold.[160] The court adopted a restrictive interpretation of Section

[152] *See Id.*

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

[154] *Id.*

[155] *Id.* (stating "[t]hat the physical components were not damaged is fortunate, but it does not lessen the loss represented by consultant fees").

[156] *Id.* (stating, "[i]f we were to restrict the statute. . .we would flout Congress's intent by effectively permitting the CFAA to languish in the twentieth century, as violators of the Act move in to the twenty-first century and beyond").

[157] *Id.* (stating the "legislative history makes clear that Congress intended the term 'loss' to target remedial expenses borne by victims that could not properly be considered direct damage caused by a computer hacker").

[158] *See generally* LaBelle, *supra* note 27; *In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 523 (S.D.N.Y. 2001).

[159] *See Doubleclick*, 154 F. Supp. 2d at 522.

[160] *Id.* at 521.

1030(a)(2)(C), inferring that the singular language used in the statute means that the damage threshold needs to be met in one singular act.[161]

The *America Online* court was highly critical of the *Doubleclick* court's damage analysis.[162] The court in *America Online* noted that the *Doubleclick* court glossed over the deficiencies and ambiguities located in the CFAA.[163] The *America Online* court decided that the legislative history dictates that the damage threshold should be measured from one act, which can affect many different computers.[164]

The *America Online* court correctly understood the legislative intent of the CFAA. The court read the damage provisions broadly to reach the conclusion that a litigant should be able to aggregate damages of a single act across multiple computer systems.[165] Congress intended that the CFAA would be adaptable to change with advances in technology, such as the ability to connect multiple computers together, which would allow for single act to damage multiple machines.[166]

H. Congress should amend the CFAA

In order to remedy the ambiguities present in the CFAA, Congress must amend the Act in order to clarify the provisions relating to what constitutes damage. By stating that the CFAA was meant to further protect "computer systems," it could be reasonably inferred that Congress intended to protect against damage caused by one individual that could occur across multiple computers.[167] After analyzing the legislative history as well as the amendments to the CFAA, it is clear that Congress intended the statute to be flexible in the ever advancing area of computer systems and technology.[168] In today's business world, computers are linked together in networks.[169] Computer networks provide companies with an efficient way to do business. However, because networks link many computers together, it is important that the CFAA be adaptable to the possibility that more than one computer on a network could be af-

[161] *Id.* at 524.

[162] *In re* Am. Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1373 (S.D. Fla. 2001).

[163] *Id.* at 1372. "Most importantly, in. . .*Doubleclick*, the [court] found the statutory language to be clear, ignored the comma that precedes 'to a protected computer,' and overlooked the fact that the phrase was a dangling participle." *Id.* at 1373.

[164] *Id.* at 1372.

[165] *See Id.* at 1373-74.

[166] *See* S. Rep. No. 101-544 (1990); S. Rep. No. 104-357 (1996).

[167] *See* S. Rep. No. 104-357, at 8 (1996).

[168] *See Id.*; S. Rep. No. 101-544 (1990).

[169] *See* 71 Am. Jur. Trials 111 § 24 (2009). "Computer links and local area networks (LANs) are the means by which computers talk to each other. Local area networks are the means by which computers talk to each other." *Id.*

fected by a malicious attack.[170] Based on the analysis of the policy and legislative history of the CFAA, the ability to aggregate damages across multiple computers should be allowed with the advancement of multiple computers linked together in networks. Congress intended that the CFAA would be a powerful tool for civil litigants to protect their expansive and expensive computer systems from those who wish to do them harm.

IV. PROPOSAL

Congress should amend the CFAA to make clear that litigants should be able to aggregate damages across multiple potential victims and across multiple computers. The legislation should read:

> Damage or loss to a protected computer may be aggregated across multiple computer systems or networks. The damage or loss must occur over a one year period and must reach a minimum of $5,000. The language of this section is not meant to limit the number of computer systems or users that can be used to aggregate damages.
>
> The term "loss" can be construed to mean, but is not limited to, reasonable costs associated with discovering a violation or violations of subclasses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i), lost revenue directly associated with a violation of subclasses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i), and any other reasonable cost associated with a violation of subclasses (I), (II), (III), (IV), or (V) of subsection (c)(4)(A)(i).
>
> Section 1030(a)(5) shall be amended to read: knowingly causes the transmission of a program, information, code, or command, and as a result of such conduct, intentionally causes damage without authorization, to a protected computer or protected computers. Nothing in this section should be read to construe a limitation on the number of protected computers that need to be damaged without authorization.

V. CONCLUSION

The Computer Fraud and Abuse Act is a federal statute designed to be a comprehensive statute to fight cybercrime.[171] Congress intended that as technology progresses, the statute would be able to adequately protect computer systems from malicious hackers.[172] In particular, it can be very difficult to assess damages in a CFAA claim because there may be no actual physical damage to a computer or computer system. The Act's legislative history has consistently suggested that Congress in-

[170] *See Id.*

[171] *See* S. REP. NO. 101-544 (1990); S. REP. NO. 104-357 (1996).

[172] *Id.*

tended the Act to adapt to changes in technology.[173] If Congress' intent is what the legislative history suggests, then the CFAA should be amended again to keep up with the ever changing computer crime environment. Litigants need an effective tool to prevent damage and to punish those who cause damage to computer systems.

Congress needs to amend the CFAA by making it clear that damages can be aggregated across multiple computers and computer systems over the one year period currently allowed under the statute.[174] As court cases have indicated, the statute is ambiguous and poorly written in describing how damages may be sought as well as what amount and which type of damages are required to allow civil litigants recovery under the CFAA.[175] Additionally, the case law demonstrates that it is not ideal to have courts attempting to analyze ambiguous statutory language.[176] Although courts use the same general principles of statutory construction, the results of that process can vary widely.[177] The court interpretations change further when courts begin to analyze more than two decades of legislative history.[178] Situations arise where courts rely on testimony and materials that may not truly reflect the intentions of Congress, but reflect how a government agency has interpreted the CFAA.[179] Congress needs to amend the Computer Fraud and Abuse Act to clarify the damages section of the Act. Congress needs to make clear that a litigant should be able to aggregate damages to meet the $5,000 threshold required for a federal court to have jurisdiction over a claim.

[173] *Id.*

[174] 18 U.S.C. § 1030.

[175] *See In re* Am. Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1372-73 (S.D. Fla. 2001).

[176] *See* ResDev, LLC v. Lot Builders Ass'n, Inc., No. 6:04-cv-1374-Orl-31DAB, 2005 U.S. Dist. LEXIS 19099 at *3 (M.D. Fla. Aug. 10, 2005); *see also In re* Doubleclick Inc. Privacy Litig., 154 F. Supp. 2d 497, 520 (S.D.N.Y. 2001); *In re* Am. Online, Inc. Version 5.0 Software Litig., 168 F. Supp. 2d 1359, 1369 (S.D. Fla. 2001).

[177] *See ResDev*, 2005 U.S. Dist. LEXIS 19099 at *3; *see also Doubleclick*, 154 F. Supp. 2d at 520; *Am. Online*, 168 F. Supp. 2d at 1369; Thurmond v. Compaq Computer Corp., 171 F. Supp. 2d 667, 677 (E.D. Tex. 2001).

[178] *See e.g.*, *Doubleclick*, 154 F. Supp. 2d at 522; EF Cultural Travel BV v. Explorica, Inc., 274 F. 3d 577, 585 (1st Cir. 2001).

[179] *Thurmond*, 171 F. Supp. 2d. at 680-81 (demonstrating the court's reliance on the Justice Department's interpretations of the CFAA made by the justice department made that do not accurately reflect Congress' intentions).