2017

Computer Fraud and Abuse Act: Made for International Hackers or Average Internet Users

Dana Paolillo

I. Introduction

The Computer Fraud and Abuse Act ("CFAA") is an amendment to a federal statute created to shield specific computers that would be vulnerable to attacks. Since its origin, the code has grown and expanded far beyond its original scope. Courts are split on how the statute should be interpreted when there are issues of impersonation on social media and terms of service violations of websites. This report will discuss the legislative history and the intended use of the statute. Followed by how the statute has grown since its inception, this report will further discuss the future of the CFAA.

II. The Birth and Growth of the Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act ("CFAA") is a heavily contested amendment to the federal code 18 U.S.C. §1030[1]. Courts across the country are split on how and when the section should be applied. When the CFAA was passed in 1984 its application appeared straightforward[2]. As time passed and the Internet grew, the CFAA has been stretched by courts to cover many aspects of Internet governance, in some places, where it may not have been intended to apply. Since the CFAA's initial inception, the statute grew and in some courts has become a catchall for all computer crimes.

At its earliest inception, the proposed amendment was very specific. The initial is found in the "Health and Environment Miscellaneous" bill from the committee on Energy and Commerce in 1983[3]. The primary form of the statute was part of a medical reform bill, "Medical Computer Crime Act of 1984," to make unauthorized access to medical records "through a

---

1 18 U.S.C. §1030

2 *Id.*

3 Health and the Environment Miscellaneous, Part 4, 85 CIS H 36119 (1983)

telecommunication device…" a crime[4]. Not only was this specified to medical records, it was specific to unauthorized access or alteration of computerized medical records[5]

Congress held hearings to establish a computer crime statute in the early 1980's. The Judiciary Committee held hearings considering establishing criminal penalties for the Counterfeit Access Device and Computer Fraud Act of 1983[6]. The act expanded to protected computers owned or used by the federal government, financial institutions, and/or businesses engaged in interstate commerce[7]. The amendment originally stipulated to medical records now included much more under its large umbrella.

As CFAA was being discussed in various hearings, the potential abuse of computers became more evident. The act was expanded to include criminal penalties for computers "involving unauthorized access to financial information, and unauthorized access to Government information, including classified information related to foreign relations or national defense." The ever-growing amendment became a tool for national security and criminalized accessing government information.[8]

By the time the bill's senate floor debate was finished, it included: "unauthorized access to or alteration of information in Federal interest computers."[9] Federal interest computers were defined as "computers used by or for the Federal Government, those of federally insured financial institutions, those of stockbrokers registered with the SEC, or those used in different States…[i]ncludes provisions on illegal access to computerized individual medical record."[10]

---

4 *Id.*
5 *Id.*
6 Counterfeit Access Device and Computer Fraud and Abuse Act, 85 CIS H 52139 (1983)
7 *Id.*
8 H. Rpt. 98-894 at p.28 (1984)
9 99 CIS Legis. Hist. P.L. 474 (1986)
10 *Id.*

Moreover, the act made it a crime to engage in the sale of passwords or similar information that would allow unauthorized computer access.[11] Congress intended the amendment provide a well-defined assertion of prohibited activity to "the law enforcement community, those who own and operate computers, as well as those who may be tempted to commit crimes by unauthorized access."[12] Essentially, Congress intended those who would be affected by the law to have clearly defined parameters as to what actions would constitute a crime or lead to civil penalties.

To further ensure the act was correctly applied, the legislature changed "knowingly" to "intentionally" in 1986, heightening the required *mens* rea.[13]The statute's intent was to penalize intentional unauthorized access and not careless ones.[14] Although there was some concern that the knowing standard was difficult to apply to technology.[15] "'Intentional' means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective."[16] The user had to intend to go beyond his or her authorization. More than just knowing he did, the user had to intend for that to be his purpose.

Finally, the CFAA was officially codified in 1986, amending 18 USC §1030 of the US Codes [17]. The language includes: "intentionally accesses a Federal interest computer without authorization… alters, damages, or destroys information causes a loss…aggregating $1,000 or more during any one year period…or modifies or impairs the medical examination, medical

11 *Id.*
12 *Id.*
13 Senate Report No. 99-432 at 5-6
14 *Id.*
15 *Id.*
16 *Id.*
17 Congressional Record, Vol. 132 (1986)

diagnosis, medical treatment, or medical care…"[18] It included the unauthorized access of medical records for a specific purpose.[19]

A "federal interest computer was defined as "exclusively for the use of a financial institution or the United States Government, or…used by or for a financial institution or the United States Government and the conduct constituting the offense affects the use of the financial institution's operation or the Government's operation of such computer…"[20] The act includes two or more computers, used in committing the offense, that were not located in the same state.[21]

After the act was codified, there were several changes to the definitions and the scope of the statute. These changes were based on experience, technology, and world events. After 9/11, Congress pushed through numerous national security reforms including cyber security and the United and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (USA PATRIOT).[22] The USA PATRIOT Act amended the definition of "protected computer" to clarify the term includes computers outside of the United States so long as they affect "interstate or foreign commerce or communication of the United States."[23]

Experience with the statute brought about expansions and revisions as computer crimes escalated and the government began to work with the CFAA.[24] Congress made revisions to the amendment, which eliminated some requirements and expanded the act's reach in 1988, 1989,

---

18 *Id.*
19 *Id.*
20 *Id.*
21 *Id.*
22 CRS Report for Congress: The Internet and the USA PATRIOT Act: Potential Implications for Electronic Privacy, Security, Commerce, and Government 3/4/2002
23 18 U.S.C. §1030(e)(2)(B) (2001).
24 Prosecuting Computer Crimes: Computer Crime and Intellectual Property Section Criminal Division Federal Prosecutor's at p. 2

1990, 1994, 1996, 2001, 2002, and 2008.[25] The amendments eliminated 18 U.S.C. §1030(a)(2)(C) which required information be stolen through interstate or foreign communication and 18 U.S.C. §1030(a)(5) which required a loss of more than $5,000 and created a felony when the damage affected 10 or more computers.[26] Eliminating those requirements increased the CFAA's scope.

Further changes included expanding 18 USC §1030(a)(7) to criminalize threats to cause computer damage and included threats to (1) steal data on a computer, (2) publicly disclose stolen data, or (3) not repair damage already caused to the computer.[27] The amendments criminalized conspiracy to commit computer hacking, and again, broadened the definition of a protected computer in 18 U.S.C. § 1030(e)(2) to include those computers used in interstate or foreign commerce or communication.[28]

The current CFAA applies to all "protected computers." A protected computer is any computer used in interstate commerce or communication and applies to Internet Service Providers and individual computers.[29] The CFAA creates seven crimes, including criminal penalties, when a user "intentionally accesses" without authorized access or exceeding their authorized access and attains information from a protected computer[30]. Furthermore, the statute definition of "damage" is a vague term that can mean anything that impairs the data of a program, system, or information.[31]

CFAA set forth criminal penalties and criminalized unauthorized access to a computer "knowingly with intent to defraud" and retrieving any information that may be valuable, unless

---

25 *Id.*
26 *Id.*
27 *Id.*
28 *Id.*
29 *Information Privacy Law* Solove and Schwartz, 5d 907 (2015)
30 18 U.S.C. §1030(a)(2)(c)
31 *Id.*

the object of the fraud consists only of the use of the computer and is less than $5,000 in a one year period.[32] Punishment for such crimes can be as minimal as fines ranging to a maximum of twenty years imprisonment depending on what part of the statute is violated.[33]

The statute also provides civil liabilities, "Any person who suffers damage or loss by reason of a violation of this section may maintain a civil action against the violator to obtain compensatory damages and injunctive relief or other equitable relief."[34] If the section is violated, "A civil action for a violation… may be brought only if the conduct involves 1 of the factors set forth in subclauses… subsection (c)(4)(A)(i)."[35] The statute limits damages to economic damages and sets the statute of limitations within two years of the date of the alleged act or discovery of the damage.[36]

III. Interpretations that Expand the Computer Fraud and Abuse Act

Courts across the nation have used the CFAA to prosecute and hold defendants civilly liable for damages when a person exceeds the authority of accessing an email account, or utilizing someone else's social media profile as their own. These courts have various reasons that impersonating someone on social media sites and through their e-mail violates the CFAA.

The District Court of Massachusetts held that accessing another's social media account, without his permission, created liability under the CFAA in *Mahoney v. Denuzzio,* 2014 U.S. Dist. (D. Mass. Jan. 29, 2014).[37] In *Mahoney,* James Mahoney and Danielle Denuzzio were once romantically involved and had a child together. Their relationship disintegrated and tensions rose regarding child custody.[38] Mahoney had visited Denuzzio's home and accessed his own

---

32 18 U.S.C. §1030(a)(4)
33 *Information Privacy Law* Solove and Schwartz, 5d 907 (2015)
34 18 U.S.C. §1030(g)
35 *Id.*
36 *Id.*
37 *Mahoney v. Denuzzio,* 2014 U.S. Dist. (D. Mass. Jan. 29, 2014)
38 *Id.* at 2.

personal Yahoo! e-mail and Facebook accounts using her computer.[39] DeNuzzio had disclosed two pages of racist emails to the Probate Court that were from Mahoney's Yahoo! Account."[40] DeNuzzio had intended to use the emails to show Mahoney was a racist and therefore, it would not have been in the child's best interest to be in his custody.[41]

Mahoney alleged that DeNuzzio composed the emails and the court order was the first notice he received that she obtained access to his accounts. He contends that he did not give her passwords to either his email or Facebook account.[42] Mahoney hired a computer forensics expert that concluded "on 502 occasions from January 1 through June 27, 2011, someone using the computer DeNuzzio regularly used had obtained access to Mahoney's Yahoo! e-mail account."[43] Mahoney suspected that Denuzzio obtained his password by using software that recorded his keystrokes and sought to file a criminal complaint but criminal charges were never pursued.[44]

The civil court found that the complaint plausibly stated grounds for relief.[45] The computer was involved in interstate commerce, and according to the court, all computers connected to the Internet are considered "protected."[46] DeNuzzio did not have the authority to access Mahoney's e-mail or social media accounts.[47] The plaintiff's monetary loss was reasonable in response to "…an offense, conducting a damage assessment, and restoring . . . the system . . . to its condition prior to the offense, and any revenue lost, cost incurred, or other consequential damages incurred because of interruption of service."[48] Mahoney's costs include

---

39 *Id.*
40 *Id.* at 4
41 *Id.*
42 *Id.*
43 *Id.*
44 *Id.* at 5
45 *Id.* at 11
46 *Id.* at 12
47 *Id.*
48 18 U.S.C.S. §1030

hiring a computer forensics firm and hiring an attorney to remedy the breach in the probate court.[49]

The court held that the motion could survive a motion to dismiss, but no further action was taken at the time of this report. Consequently, the facts of the case fall directly under CFAA's civil liabilities allowed.[50] Mahoney's monetary damages were directly related to DeNuzzio's unauthorized use of his e-mail account because the damages included investigation and attorney's fees for his lawsuit.[51]

Sewell v. Bernardin, 795 F.3d 337 (2d Cir. 2015) is a case of first impression from the Court of Appeals for the Second Circuit. The lower court dismissed the complaint as being time barred by the two-year statute of limitations.[52] Sewell and Bernardin were in a romantic relationship until 2011.[53] Throughout their relationship, Sewell maintained a private e-mail and Facebook account.[54] Bernardin did not have the passwords or access to these accounts.[55]

In August 2011, Sewell was notified that her AOL password had been changed and the unauthorized user sent out malicious emails, regarding her sexual activities, to her family members.[56] In February of 2012, Sewell was unable to log into her Facebook account and on March 1, 2012 someone posted a public message containing malicious statements about Sewell.[57]

On August 2, 2014, the United States District Court for the Eastern District of New York granted Bernardin's motion to dismiss, holding that "Sewell's claims were time-barred under the

---

49 *Denuzzio* at 12.
50 *Id.*
51 *Id.*
52 *Sewell v. Bernardin*, 795 F.3d 337 (2d Cir. 2015)
53 *Id.*
54 *Id.* at 339
55 *Id.*
56 *Id.*
57 *Id.*

CFAA's and SCA's applicable two-year statutes of limitations."[58] Sewell then appealed and on appeal the lower court's decision to dismiss was affirmed.[59] The AOL account breach was time barred by the statute.[60]

On appeal, the circuit court concluded that there were two separate CFAA claims: 1) from the AOL account when she had notice in August 2011 and from the defendant accessing her Facebook account in February of 2012.[61] The court held that the CFAA claim "is premised on impairment to the integrity of a computer owned and operated by AOL, not of her own physical computer."[62] CFAA claims are for the programs that were utilized by the user and trespasser and not just the trespass of the physical computer, itself.[63]The court held that there were two valid claims under the CFAA and that one, regarding unauthorized use of her Facebook account, was not time barred under the statute.[64] There were no further court proceedings at the time. Here, the court sought to clarify the a CFAA claim does not focus on the victim's personal computer but of the computers of the programs that are accessed.

The most recent case litigated under CFAA is *Facebook, Inc. v. Power Ventures, Inc.*, 2016 U.S. App. 12781 (9th Cir.). Power Ventures, the defendant, created a social networking website that operated by aggregating a user's previously existing social networking accounts and information.[65] The "Power user" could see all their contacts from multiple social networking sites through a single program and could click through the central Power website to individual social networking sites.[66]

---

58 *Id.*
59 *Id.*
60 *Id.* at 340
61 *Id.*
62 *Id.* at 341
63 *Id.*
64 *Id.*
65 *Facebook, Inc. v. Power Ventures, Inc*., 828 F.3d 1068 (9th Cir. 2016)
66 *Id.* at 1071

At the time of Power's promotional campaign, Facebook.com, the plaintiff, had 130 million users and allowed limited access to non-members.[67] Third party software developers, or websites that want to contact Facebook users through its website, must enroll in "Facebook Connect," a program that requires a user to agree to an additional Developer Terms of Use Agreement.[68]

In December 2008, Power began a promotional campaign where they placed an icon on their website to entice users to share Power.com by stating, "First 100 people who bring 100 new friends to Power.com win $100."[69] Once a user clicked "Yes, I do!" Power would create an event, photo, or status on the Facebook user's profile.[70] Depending on a Facebook user's settings, Power would send a message or e-mail to the user's friends within Facebook's system.[71]

For example, if a Power user shared the promotion through an event, Facebook generated e-mail to an external e-mail account from the user to their friends.[72] The e-mail provided the name and time of the event, listing Power as the host, and said the Power user was inviting them to the event.[73] "The external e-mails were form e-mails, generated each time that a Facebook user invited others to an event. The 'from' line in the e-mail stated that the message came from Facebook; the body was signed, 'The Facebook Team.'"[74]

Facebook was unaware of Power's promotional campaign until December 2008, and when they did they sent a "cease and desist" letter to Power.[75] Facebook attempted to have

---

67 *Id.*
68 *Id.*
69 *Id.*
70 *Id.*
71 *Id.*
72 *Id.*
73 *Id.*
74 *Id.*
75 *Id.*

Power register in Facebook Connect and sign the special Developer Terms of Use Agreement.[76] When they refused Facebook established an Internet Protocol ("IP") block to prevent them from accessing Facebook's website.[77] Power switched IP addresses to avoid the block and continued its promotion even though it utilized Facebook.com without Facebook's permission.[78] In total, over the course of Power's campaign, they sent more than 60,000 external emails using Facebook's system, and countless internal messages.[79] By April 2011, Power had gone out of business.[80]

Facebook argued violations under the CFAA, which prohibits acts of computer trespass by those unauthorized users or users who exceed their authorization.[81] The court held that Facebook suffered a loss and was entitled to civil penalties because Facebook employees "spent many hours, totaling more than $5,000 in costs, analyzing, investigating, and responding to Power's actions"[82].

The court concluded that Power accessed Facebook's computers knowing they did not have authorization.[83] The court based its analysis on two previous cases: *United States v. Nosal*, 676 F.3d 854 (9th Cir. 2012) also known as "*Nosal I"* and *United States v. Nosal*, No. 14-10037, 2016 U.S. App. LEXIS 12382, (9th Cir. July 5,2016) known as "*Nosal II*".[84] There are two general rules the court needs to follow using *Nosal*'s analysis: first, a defendant can violate the CFAA when he lacks permission to access a computer or when his permission has been

76 *Id.*
77 *Id.* at 1074
78 *Id.*
79 *Id.*
80 *Id.*
81 *Id.* at 1078
82 *Id.*
83 *Id.*at 1082
84 *Id.* at 1085

explicitly revoked.[85] Using better technology or a third party to help access a site does not excuse the violating user of liability.[86] Second, violating the terms of use for a website, alone, cannot be a basis for liability.[87]

IV. Interpretations that Narrow the Computer Fraud and Abuse Act

In some courts, the interpretation has been broadened beyond what the original intent may have been. On the other hand, there are a number of courts that construe the terms narrowly. In doing so, the vague statute is being tapered to apply in a smaller number of circumstances.

United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) is a well-known case involving the CFAA. The issue in the case was whether a violation of the "Terms of Service" ("TOS") for a website constitutes a crime under the CFAA.[88] Drew, a resident of Missouri, entered a conspiracy to intentionally access a computer used in interstate commerce, without authorization, in order to commit a tortious act (infliction of emotional distress) on Megan Meier, a thirteen year old girl.[89] Drew, and conspirators, impersonated 16-year-old boy named "Josh" they began a romantic relationship via MySpace until the conspirators told Megan he did not like her and "the world would be a better place without her in it."[90] Megan killed herself later that day.

Their actions violated the MySpace Terms of Service ("TOS")[91] Drew was indicted for one count of conspiracy and three counts of violating the felony portion of the CFAA "which prohibit accessing a computer without authorization or in excess of authorization and obtaining information from a protected computer where the conduct involves an interstate or foreign

---

85 *Id.*
86 *Id.*
87 *Id.*
88 *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009)
89 *Id.*
90 *Id.*
91 *Id.*

communication and the offense is committed in furtherance of a crime or tortious act."[92]

The court went through an analysis of the Myspace TOS. In 2006, to be a Myspace member, a person had to access the sign up section for the Myspace website and register by filling out information meeting specific age requirements.[93] The information required included: name, e-mail, and date of birth, country, zip, code, and gender.[94] The registrant had to click the "I agree" box for Myspace's TOS and Privacy Policy.[95] The Terms of Service did not appear on the same page, and to read them the user had to scroll to the bottom to click on the "Terms" hyperlink.[96] Unsurprisingly, a person could easily become a member of the Myspace community without ever reading the TOS section.[97]

The TOS prohibited posting content that could be offensive and "promotes…harasses or advocates harassment of another person…promotes illegal activity… or promotes illegal activities or conduct that is abusive, threatening…includes a photograph of another person…without their consent…"[98] The Myspace TOS reserved the right to take legal action against anyone who engaged in the prohibited activity which included "a) 'criminal or tortious activity', b) 'attempting to impersonate another Member or person', c) 'using any information obtained from the Services in order to harass, abuse, or harm another person', d) 'using the Service in a manner inconsistent with any and all applicable laws and regulations'… "[99]

The TOS warned other users that other Myspace members may have false or misleading information on their profiles, and further indicated that Myspace will not be held liable.[100]

---

92 *Id*. at 451
93 *Id.*
94 *Id.*
95 *Id.*
96 *Id.*
97 *Id.*
98 *Id.* at 454
99 *Id.*
100 *Id.*

Moreover, Myspace reserved the right to change their TOS at any time, which meant a member would have to check the TOS every time they logged on to ensure they were not violating the terms.[101]

The relevant issue was whether a computer user's intentional violation of a websites terms of services satisfies the first element of U.S.C. § 1030(a)(2)(C): defendant intentionally accessed without authorization of a computer.[102] If the answer was yes, then any conscious violation will constitute a CFAA misdemeanor.[103] The following elements are always met when a person utilizing a computer contacts or communicates with a website.[104] Accessing information can be as minimal as observation of the data.[105] Targeting the data for collection or corruption is not needed to prove a violation.[106]

The district court analyzed the first element, intentionally accessed without authorization of a computer, focusing on three undefined terms.[107] "Intentionally' is undefined, the court uses the legislative history of the CFAA. The court interpreted Congress's actions of raising the scienter from knowing to intent to show a heightened *mens rea*.[108] The legislator intended for a defendant to mean to cross an unauthorized threshold and not just know they crossed it. The court uses the dictionary definition of "access" "to gain or have access to; to retrieve…"[109] The third undefined and necessary term, "without authorization" is a term that will change depending on the nature of the circumstances, according to the court.[110]

---

101 *Id.*
102 *Id.*
103 *Id.*
104 *Id.*
105 *Id.*
106 *Id.* at 458
107 *Id.*
108 *Id.*
109 *Id.* at 459.
110 *Id.*

Applying this to the facts of the case, the only factual basis to conclude Drew intentionally accessed Myspace's servers without authorization was her violating Myspace's TOS by deliberately creating the fake "Josh Evans" profile using a photo of a juvenile without permission just to communicate with Meagan.[111] The court concludes that an intentional breach of the MSTOS can potentially constitute accessing the Myspace server without authorization under the statute.[112]

The owner of a website has the right to institute the boundaries of information their members can access or applications available on their website.[113] As a right of law, an owner can relay and impose "limitations/restrictions/conditions" by a written notice like the terms of service or use provisions on a homepage.[114] Most courts that have reviewed TOS cases have held that a website's TOS can define what is authorized regarding a website.[115]

The court concluded that basing a CFAA misdemeanor upon the violation of a websites TOS would contravene the void-for-vagueness doctrine.[116] When it comes to "clickwrap" agreements, like the Myspace TOS, the issue is whether a person of "common intelligence" would be on notice that a breach of the terms would create a CFAA violation.[117] First, the statute itself does not put people on notice, they may be aware of civil penalties but not criminal charges.[118]

Second, the TOS does not specify which breached term leads to termination of authorized

111 *Id.* at 460
112 *Id.*
113 *Id.* at 462
114 *Id.*
115 *Id.*
116 *Id.* at 464
117 *Id.*
118 *Id.*

access for the user.[119] The court concluded that "if any violation of any term of service is held to make the access unauthorized, that strategy would probably resolve this particular vagueness issue; but …render the statute incredibly overbroad and contravene the second prong of the void-for-vagueness doctrine as to setting guidelines to govern law enforcement."[120]

Third, by utilizing the TOS as the basis for a crime, it makes the website owner the party who defines criminal conduct.[121] It is possible that the description in the TOS is so vague that a reasonable person might be unsure of what the TOS covers.[122]Fourth, because the TOS are a contractual way to set the scope of authorized access "a level of indefiniteness arises from the necessary application of contract law in general and/or other contractual requirements within the applicable terms of service to any criminal prosecution."[123]

The court concluded that treating a website's TOS violation as an 18 U.S.C. §1030(a)(2)(C), would turn the section "into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent Internet users into misdemeanant criminals."[124] Concluding any other way would create a law that "that affords too much discretion to the police and too little notice to citizens who wish to use the [Internet]."[125]

Tan v. Doe, 2014 U.S. Dist. LEXIS 61972 (S.D.N.Y. May 1, 2014), narrowed the definition of a "protected computer" and what it means to "damage" a computer. This case was litigated under the CFAA private right of action.[126] Tan involved two business partners whose partnership ended antagonistically.[127] The plaintiffs were a married couple, Miah, co-founded a

---

119 *Id.*
120 *Id.*
121 *Id.*
122 *Id.* at 465
123 *Id.*
124 *Id.* at 465-466
125 *Id.* at 466
126 *Tan v. Doe*, 2014 U.S. Dist. LEXIS 61972 (S.D.N.Y. May 1, 2014) at 1
127 *Id.*

digital music company called UrFilez.[128] There was a dispute between Miah and the co-founder and in August 2012, the plaintiffs claim that derogatory posts appeared on several blogs, including their wedding photo.[129] The posts accused the couple of fraudulent and unethical misconduct, which included siphoning money from UrFilez.[130]

The plaintiffs allege that the blogs have spread to social media sites and have resulted in irreparable damage to their personal and professional reputations.[131] Their complaint against "John Doe" included an application to subpoena non-party websites including Twitter and Facebook to help them identify who "John Doe" was and a temporary restraining order "directing these companies to remove the derogatory statements from their website."[132]

The plaintiffs' complaint asserts copyright infringement, defamation, tortious interference, false light, and a violation of the CFAA.[133] The court analyzed the plaintiff's CFAA claim, and found they failed to state a claim for three reasons:[134] The court found the complaint failed to allege a "protected computer let alone a "computer" that was accessed or damaged as a result of alleged conduct.[135]

CFAA defines a protected computer to include a "computer…used in interstate or foreign commerce or communication."[136] To satisfy this, the court held the facts must evince a plausible inference of a substantial use of the computer related to interstate commerce.[137] The fact a computer is connected to the Internet and able to be used in interstate commerce is not enough to

---

128 *Id.*
129 *Id.*
130 *Id.*
131 *Id.*
132 *Id.*
133 *Id.*
134 *Id.* at 2
135 *Id.*
136 18 U.S.C. 1030(e)(2)(B)
137 *Id.*

be considered actually used in interstate commerce.[138]

Consequently, if the court assumed that the defendant's utilizing Facebook to retrieve their wedding photo was unauthorized access of a protected computer, their CFAA clam still fails.[139] The CFAA claim does not allege the access resulted in any damage to the computer.[140] Downloading and circulating the wedding photo, even if it were confidential information, does no destruction or impairment to the "underlying data."[141] Plaintiffs did not allege their photo was destroyed or impaired.[142]

The *Tan* Court's analysis is completely different than the court in *Drew* which held the elements are always met when a person communicates with a website and even observing the data is enough to prove a violation.[143] The court based the interpretation in senate reports.[144]

Finally, the plaintiff's financial damages are not the types that were considered under the CFAA.[145] They allege that the aggregate losses resulting from the defendant's conduct was more than $10,000, the damages are not discernable under the statute.[146] CFAA "'loss …is limited to the 'cost of investigating or remedying damage to a computer, or cost incurred because the computer's service was interrupted…"[147] The loss plaintiffs alleged pertained to their business reputation which is not what the CFAA designates as a loss.

However, in 2015, another CFAA interpretation came to light which further narrowed its scope. *Bittman v. Fox*, 107 F. Supp. 3d 896 (N.D. Ill. 2015) interprets the CFAA to exclude

138 *Tan v. Doe* (2014) at 3
139 *Id.*
140 *Id.*
141 *Id.*
142 *Id.*
143 *United States v. Drew* (2009) at 456
144 *Id.*
145 *Tan v. Doe* (2014) at 3
146 *Id.*
147 18 U.S.C. 1030(e)(11)

cases of social media impersonation, even if there were financial damages.[148] Plaintiff Bridget Bittman is a marketing and public relations employee at the Orland Park Public Library.[149] In the fall of 2013, Fox and DuJan complained that the library was providing unfiltered access to the Internet and lobbied the library to change their policies.[150] Bittman, in charge of public relations, responded to the defendant's complaints.[151]

Subsequently, Bittman, Fox, and DuJan began a special media war with Fox and DuJan making defamatory statements about Bittman.[152] Fox posted comments about Bittman on her Facebook page, accusing Bittman and the public library of presenting a "hatefest" and making false police complaints against Fox and DuJan.[153]

Fox posted a photo of Bittman holding a champagne bottle and accused her of "being drunk to claim the ridiculous things she does about the library in the media…"[154] Fox then posted photos of Bittman's home on the Internet, which Bittman alleged was an attempt to harass her.[155] Fox published a video titled "Bridget Bittman commits Disorderly Conduct/Breach of Peace on 7/8/14 according to Officer Schmidt" and several captions of defamatory statements. [156]

Furthermore, Fox and DuJan created a Facebook page, "Sassy Plants Illinois" impersonating Bittman and her floral business.[157] They utilized her personal photos and photos of her floral arrangements without her authorization and posted statements to convince people that Bittman, in reality, controlled the page.[158] The statements included derogatory references

148 *Bittman v. Fox*, 107 F. Supp. 3d 896 (N.D. Ill. 2015)
149 *Id* at 898.
150 *Id.*
151 *Id.*
152 *Id.*
153 *Id.*
154 *Id.*
155 *Id.*
156 *Id.*
157 *Id.*
158 *Id.*

imply that Bittman was prejudiced.[159] Finally, in January 2015, Bittman filed a thirteen-count complaint including one count under the CFAA.[160]

The CFAA prohibits unauthorized users from intentionally accessing secure computers and damaging the computer or data.[161] Bittman argues Fox and DuJan are liable for creating the Sassy Plants Facebook Page, violating Facebook's terms of use.[162] By creating the page, using photographs of herself and her floral arrangements, Fox and DuJan violated the terms of use and exceeded their authorized access to Facebook's computers.[163]

The court concluded that Bittman presented no evidence which suggested the CFAA provided a cause of action for the alleged transgression.[164] The court held, "the statutory purpose of the CFAA is to punish trespassers and hackers."[165] They looked to the legislative history of the act, and surmised that Congress was concerned with hackers attacking using viruses and possibly disgruntled computer programmers.[166] CFAA was not enacted to punish people who create fake social media accounts, violating the website's terms of service.[167]

The court hypothesizes that even if Fox and DuJan violated Facebook's terms of use by creating the fake account to impersonate and defame Bittman, the action does not constitute "exceeding authorization" as envisioned in CFAA.[168] Fox and DuJan did not damage, steal, or tamper with Bittman's data.[169] They had no intention in permanently harming Bittman's

---

159 *Id.*
160 *Id.*
161 18 U.S.C. § 1030
162 *Bittman v. Fox*, 107 F. Supp. 3d at 900
163 *Id.*
164 *Id.*
165 *Id.*
166 *Id.*
167 *Id.*
168 *Id.* at 901
169 *Id.*

computer data.[170]

V. The Future of the Computer Fraud and Abuse Act

Differing interpretations of the CFAA have caused disconnect in the courts regarding how and when the CFAA applies to cases involving social media websites and email accounts. Some courts interpret "protected" as any computer utilized in interstate commerce.[171] While others use a stricter definition, requiring the computer be used in interstate commerce, being connected to the Internet is not enough to require federal protection.[172] Unauthorized access of information can be simply accessing information without authorization with no actual objective necessary for a violation.[173]

The conflicts have become so contentious that the Department of Justice recently published a memo, dated September 11, 2014 on their website in October of 2016.[174] The memo, written by Eric Holder as the Attorney General, stated that the memo was to provide guidance for prosecutors.[175] The memo provided prosecutors with eight factors. The first, and major factor, was to consider whether prosecution would serve a substantial federal interest.[176] Though ambiguous, the factor would help separate serious hackers and threats to cybersecurity from computer users who violate a website's terms of service.

Some other factors include: 1) sensitivity of the affected computer system or the information transmitted by or stored on it; 2) the national security implications of the crime

---

170 *Id.*
171 *United States v. Drew*, 259 F.R.D. 449 (C.D. Cal. 2009)
172 *Tan v. Doe*, 2014 U.S. Dist. LEXIS 61972 (S.D.N.Y. May 1, 2014)
173 S. Rep. No. 99-432, at 6-7 (1986)
174 *DOJ releases controversial cybercrime prosecution memo*, FCW: THE BUSINESS OF FEDERAL TECHNOLOgy, https://fcw.com/articles/2016/10/28/cfaa-enforcement-carberry.aspx (last visited Nov. 30, 2016).
175 *Id.*
176 *Id.*

impact of the crime on victims; 3) the deterrent value of the investigation; 4) whether the crime can be prosecuted by another jurisdiction if it is declined for federal prosecution; 5)if information is obtained by exceeding authorized access.[177]

Only a minority of states enacted legislation regarding identity theft on social media sites, allowing them to prosecute the crime avoiding utilization of the CFAA.[178] Texas is an example of a state law regarding online impersonation: "a person commits an offense if the person, without obtaining the other person's consent and with the intent to harm, defraud, intimidate, or threaten any person, uses the name or persona of another person to:(1) create a web page on a commercial social networking site or other Internet website…"[179]

Due to the ambiguous language and tough punishments for violations there has been an outcry for change. An article in Scientific American exemplified a harsh fact: "CFAA allows prosecutors to pursue the same draconian measures—punishments ranging from five to 15 years per charge—for acts as benign as violating the terms of a vendor's service agreements and those as malicious as a concerted effort to break into a computer and steal credit card numbers."[180]

Congress has considered amending the CFAA to clarify "access without authorization."[181] "Aaron's Law Act of 2015" is an attempt by lawmakers to reform the CFAA which is an "overly broad law currently allows breathtaking levels of prosecutorial discretion…"[182] The main objective of Aaron's Law's is to retain the parts of the CFAA that work while eliminating the portions prone to abuse.[183]

---

177 *Id.*

178 COMMENT: Identity Theft on Social Networking Sites: Developing Issues of Internet Impersonation, 29 Touro L. Rev. 455

179 Tex. Penal Code § 33.07 (LexisNexis, Lexis Advance through the 2015 regular session, 84th Legislature)

180 *It's Time to Reform the Computer Fraud and Abuse Act*, SCIENTIFIC AMERICAN, https://www.scientificamerican.com/article/its-times-reform-computer-fraud-abuse-act/ (last visited Nov. 30, 2016).

181 Statements on Introduced Bills and Joint Resolutions, 161 Cong Rec S 2302

182 *Id.* at 2303

183 *Id.*

One of the proposed changes includes replacing the term "exceeds authorized access" with "access without authorization means (A) to obtain information on a protected computer; (B) that the accesser lacks authorization to obtain; and (C) by knowingly circumventing one or more technological or physical measures that are designed to exclude or prevent unauthorized individuals from obtaining that information;''[184] Such a change would create a more concrete definition for a critical term used in the statute.

Furthermore, the proposed amendment would make criminal penalties proportional to the crime committed under the act.[185]" By striking 'conviction for another'' and inserting 'subsequent'; and (B) by inserting 'such' after 'attempt to commit''; by inserting after 'financial gain' the following: 'and the fair market value of the information obtained exceeds $5,000…'"[186] The offense would be committed "…furtherance of any criminal act in violation of the Constitution or laws of the United States or of any State punishable by a term of imprisonment greater than one year, unless such criminal acts are prohibited by this section or such State violation would be based solely on accessing information without authorization…"[187]

The proposed changes would tailor the CFAA back to its original legislative intent: an anti-hacking law. There would be less room for courts to apply the law in cases of social media impersonation and other situations where it did not belong. An amendment would protect the CFAA from abuse and overreach. State legislatures have the power to create such laws and only a minority of state legislated such statutes. The alteration of the sentencing section would enhance the sentencing portion by eliminating the problem of minor offenses being punishable the same as more severe violations.

---

184 *Id.*
185 *Id.*
186 *Id.*
187 *Id.*

On the other hand, there is an argument for more power under the statute.[188] Some lawmakers believe that in the age of cyber-attacks and technological warfare, the CFAA should be much stronger. In 2011, President Obama issued the Cyber Security Legislative Proposal urging Congress to give the government, and the private sector, more powerful tools and harsher punishments.[189] Part of the plan includes an increase in penalties and expansion of the government's power for enforcement of the CFAA.[190] Instead of the minimum penalty being merely a misdemeanor, the least offensive violation would still be considered a felony, with a ten-year maximum.[191] At a Congressional hearing witnesses, including FBI agents, stated hacktivists were among their adversaries.[192] Their reforms would give the government more power but go after serious threats to national security.

To better prosecute these crimes law enforcement would require the appropriate tools to investigate and prosecute cybercrimes. It also reaffirms important components of 2011 proposals to update the Racketeering Influenced and Corrupt Organizations Act, applying it to cybercrimes. [193]Finally, the proposal modernizes the Computer Fraud and Abuse Act by ensuring that insignificant conduct does not fall within the scope of the statute, while making clear that it can be used to prosecute insiders who abuse their ability to access information to use it for their own purposes.

---

188 *Obama's proposed changes to the computer hacking statute: A deep dive*, THE WASHINGTON POST, https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/14/obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive/?utm_term=.e4f7e2174f95 (last visited Nov. 30, 2016).

189 *SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts*, THE WHITE HOUSE, https://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat (last visited Nov. 30, 2016).

190 *Id.*

191 *Id.*

192 *The Trouble with Aaron's Law*, COLUMBIA JOURNALISM REVIEW http://www.cjr.org/cloud_control/aarons_law.php (last visited Nov. 30, 2016).

193 *Id.*

Moreover, "exceeds authorized access" includes "… when he accesses information 'for a purpose that the accesser knows is not authorized by the computer owner.'"[194] In some cases, the language would prohibit breaching a written condition, like a Terms of Service written by a website.[195] The addition would create havoc in the courts as to what the computer owner would and would not allow when it is not a written condition. It gives prosecutors across the country a large amount of discretion as to what the unauthorized user was on notice about as to what they had the authority to access.

The proposed legislation would add a provision that would punish a user who "intentionally exceeds authorized access to a protected computer, and thereby obtains information from such computer" if one of three conditions are met: "(i) the value of the information obtained exceeds $5,000; (ii) the offense was committed in furtherance of any felony … or (iii) the protected computer is owned or operated by or on behalf of a governmental entity."[196] Also, instead of requiring the government to prove "intent to defraud" prosecutors would have to establish "willfulness," criminalizing unlawful trafficking of access to "other types of wrongdoing perpetrated using botnets" and not just password and similar information.[197]

VI. Conclusion

It is clear the CFAA needs to be amended. The amount of ambiguity and discretion has allowed to a vast array of applications often, far beyond the original legislative intent. The Internet has grown a great deal since the CFAA was established and in turn requires more specific federal legislation. Many agree that the CFAA needs modification. However, they

194 *Id.*
195 *Id.*
196 *Id.*
197 *Id.*

cannot decide on if the government should have more control or less control. The CFAA needs to be broadened in some areas and restricted in others.

The future of the CFAA should include serious punishments that fit the violation committed. Cyber-attacks are a dangerous threat to national security and should be treated as such. The sentences should be a grave deterrent for potential hackers. However, a user utilizing someone else's Twitter account should not be as punishable as a more serious violation, like a cyber-attack on a government computer. The sentencing requirements must be clearly stated to ensure judges know what to apply during sentencing.

Unambiguous definitions are necessary for the CFAA to become a useful statute going forward. Two terms that need to be dealt with are: "exceeding authorized access" and "without authorization." These terms must be neatly tailored to a select group or done away with completely. Currently, there are a large amount of internet users that fall into this very broad category. Change is necessary and it needs to be done quickly.