2016

No Need to Fear Robots: Online "Bot" Use under the Computer Fraud and Abuse Act

Peter F. Bariso III

No Need to Fear Robots: Online "Bot" Use under the Computer Fraud and Abuse Act

Peter F. Bariso III*

I. Introduction

The Computer Fraud and Abuse Act (CFAA) is a powerful statute that can combat online theft and protect digital information.[1] Congress originally discussed these objectives in the early 1980s and enacted the CFAA in 1986 in the midst of the Digital Revolution.[2] As digital machinery began to quickly replace analog and mechanical devices, Congress needed a statute with the ability to grow alongside this new technology.[3] The CFAA was meant to be malleable and adapt over time with ever-changing innovation.[4] At inception in 1986, however, the idea of a global internet, not to mention numerous other online technologies that now exist, was not even conceivable.

Congress designed the CFAA to be flexible because digital technology was new, but this flexibility has been misused. If courts can freely expand the statute as broadly as they please, prosecutors will arguably be incentivized to exploit the CFAA and seek criminal sanctions based on untenable statutory interpretations.[5] The Committee on the Judiciary expressly recognized that deterring unwanted computer actions begins with the private website owners and not federal law

---

* J.D. Candidate, 2016, Seton Hall University School of Law; B.S., 2007, Indiana University Kelley School of Business. Thank you to Professor David Opderbeck for helping with this comment, from basic idea to finished product. Thank you also my family and to all of the members of the *Seton Hall Law Review*.

[1] *See infra* Part II.

[2] *See infra* Part II; *Digital Revolution*, TECHNOPEDIA, http://www.techopedia.com/definition/23371/digital-revolution (last visited Jan. 5, 2015).

[3] *See infra* Part II; *Digital Revolution*, TECHNOPEDIA, http://www.techopedia.com/definition/23371/digital-revolution (last visited Jan. 5, 2015).

[4] *See infra* Part II; *Digital Revolution*, TECHNOPEDIA, http://www.techopedia.com/definition/23371/digital-revolution (last visited Jan. 5, 2015).

[5] *See* Orin S. Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1557 (2010) ("The CFAA is a remarkably broad statute, and . . . federal prosecutors eventually will try to exploit the breadth and ambiguity of the statute to bring prosecutions based on aggressive readings of the statute.").

or the court system.[6] The CFAA and courts cannot be used to rubberstamp every website owner practice with a seal of approval, making any other action illegal. Not every objectionable internet behavior is criminal and covered by the CFAA. "More comprehensive and effective self-protection by private business" is the best means of prevention, and website owners bear this responsibility, not the government.[7]

A hacker can be either "an expert at programming and solving problems with a computer," or "a person who illegally gains access to and sometimes tampers with information in a computer system."[8] While the former definition encompasses benign activity, the latter has gained much more notoriety. This secondary definition focuses on CFAA violators in that it covers individuals who do not have authorization to access a computer as well as those who go beyond their authorized access.[9] Therefore, at least as to the second definition, hackers are synonymous with criminal violators. The first definition, while entirely accurate and still popular within the computer programming world, has transitioned outside of that sphere and somewhat merged with the second definition. The term hacker is now used much more broadly to add a negative connotation to anyone who uses a computer in a new or unconventional, although perfectly legal, way.[10] By using a word that connotes illegal behavior but may describe legal actions, website owners and prosecutors have persuaded courts to prohibit benign internet conduct.[11]

Website owners have successfully induced the court to extend the CFAA beyond what Congress intended.[12] This has resulted in criminal punishment for behavior not originally

---

[6] S. REP. 99-432, 3, 1986 U.S.C.C.A.N. 2479, 2481.
[7] *Id*. (quoting *Report on Computer Crime;* Task Force on Computer Crime, Section of Criminal Justice, American Bar Association; June 1984).
[8] *Hacker Definition*, MERRIAM-WEBSTER ONLINE, http://www.merriamwebster.com (last visited Jan. 29, 2015).
[9] 18 U.S.C. § 1030 (2008).
[10] Robert Siciliano, *Are All Hackers Bad?*, MCAFEE (Sep. 2, 2014), http://blogs.mcafee.com/consumer/are-all-hackers-bad (Tesla, Facebook, and Google all use individuals traditionally thought of as "hackers" in many ways).
[11] *Id*.
[12] *See, infra* Part III.

conceived as such under the CFAA's purview. As technology changes the ways in which the internet is used and online business is carried out, website owners try to protect their information and competitive edge by any means necessary. If private information is truly hacked, as per the second definition above, and acquired through unauthorized means, the behavior may be violating the CFAA. While this is not disputed, online businesses sometimes seek to punish users who gather publicly available information with identical penalties.[13] Automated programming code, often called "bots," "scrapers," "scrubbers," or "data mining," has become a useful tool to amass large amounts of data much faster and more efficiently than any individual or group of users.[14] Computer programmers generally develop an automated program that, once set in motion, works independently to pool whatever information the programmer created the "bot" to seek out. While this may be used to hack onto websites or servers and steal protected information, it is more commonly used to gather innocuous, public data.[15] The majority of "bot" executions search out and compile public information into user-friendly databases.[16]

Independent of the CFAA, website owners are free to develop their own contracts with website users. These contracts, often called Terms of Service, set the parameters of use for anyone who visits the website. They are often long, carefully drafted, legal documents which are overlooked

---

[13] *Id*.

[14] Michael Schrenk, Webbots, Spiders, and Screen Scrapers: A Guide to Developing Internet Agents with PHP/CURL 6 (2nd ed. 2012).

[15] *Data Mining and Analytics*, SOCIETY FOR INDUSTRIAL AND APPLIED MATHEMATICS, http://www.siam.org/activity/dma/ (last visited Oct. 27, 2014).

[16] AVI RAPPAPORT, ROBOTS & SPIDERS & CRAWLERS: HOW WEB AND INTRANET SEARCH ENGINES FOLLOW LINKS TO BUILD INDEXES, *available at* http://cis.poly.edu/cs912/rappoport.pdf; *See also*, Semrush, *Semrush Bot*, *available at* http://www.semrush.com/bot/ ("Most bots are both harmless and quite beneficial."); *but see*, Incapsula 2014 Global Bot Traffic Report: Understanding Bot behavior and threats to websites 2, *available at* http://lp.incapsula.com/rs/incapsulainc/images/2014-bot-traffic-report.pdf (reporting a new 50/50 split between good "bot" traffic and "bad" bot traffic on the internet over the past two years) (It should be noted, however, that Incapsula, Inc. specializes in website security and protection from "bots" and is thus incentivized to paint landscape with an increased threat. Semrush on the other hand is a marketing company that provides bot services to its customers and is equally incentivized to portray "bots" in a positive light. At the same time, the sources theoretically measure different values—the former being number of "bots" and the latter "bot" traffic.)

by the general public.[17] On occasion users have to click "I agree" to pass onto the website, but in most instances they are not even conspicuous and can only be viewed via a link on the bottom of the site. In any case, website owners are free to draft these Terms of Service for their individual domain names, thereby creating a contractual relationship with individual users which impose restrictions on the use of the website.[18] The problem arises when these Terms of Service are violated and the website owner seeks to use the CFAA as a remedy in lieu of a proper breach of contract claim.

Commenters and the courts alike have disagreed over whether the CFAA can be used to criminalize these contractual breaches in all situations. Some previous comments have focused on individual users obtaining public information from websites generally, without reference to "bots".[19] Others focused on whether a breach of a website Terms of Service could qualify as "unauthorized access" or "exceeding authorized access."[20] Additional comments addressed Terms of Service breaches and civil claims under the CFAA.[21]

While most of these comments agree that the courts should not apply the CFAA to a broad contract-based theory of liability, the majority argue that not every contract breach to acquire

---

[17] Rachel Feltman, *Londoners accidentally pay for free Wi-Fi with a firstborn, because no one reads anymore*, THE WASHINGTON POST (Sep. 29, 2014) (Proving that no one reads Terms of Service, an experiment in London had people agree to pay for WiFi service in exchange for permanent loss of a child); *See, also,* Mike Masnick, *To Read All Of The Privacy Policies You Encounter, You'd Need To Take A Month Off From Work Each Year*, TECHDIRT (Apr. 23, 2012), https://www.techdirt.com/articles/20120420/10560418585/to-read-all-privacy-policies-you-encounter-youd-need-to-take-month-off-work-each-year.shtml (Noting that for the average internet users, reading all the Terms of Service agreements on every webpage visited would take one month a year).

[18] *Best Practices for Drafting Terms of Use*, 6TH ANNUAL E-COMMERCE BEST PRACTICES CONFERENCE, https://www.law.stanford.edu/sites/default/files/event/266629/media/slspublic/BPfnlPresentation0608.pdf, (last visited Feb. 12, 2015).

[19] Christine D. Galbraith, Access Denied: Improper Use of the Computer Fraud and Abuse Act to Control Information on Publicly Accessible Internet Websites, 63 MD. L. REV. 320, 368 (2004).

[20] Orin S. Kerr, *Cybercrime's Scope: Interpreting Access and Authorization in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596, 1630 (2003).

[21] Patricia L. Bellia, *Defending Cyberproperty*, 79 N.Y.U. L. REV. 2164, 2186 (2004); *but see* Caroline G. Jones, *Computer Hackers on the Cul-De-Sac: Myspace Suicide Indictment Under the Computer Fraud and Abuse Act Sets Dangerous Precedent*, 17 WIDENER L. REV. 261, 267 (2011) ("theoretically the law fits the crime as charged").

public information on a website should be immune from the CFAA.[22] Some commenters argue that code based tools that provide extra security and deterrence should be a guide for the CFAA.[23] They argue that, if a website requires individual input or employs additional measures before access, such as checkout page encryption, CAPTCHA code, or internet protocol blocks, and subsequent use is obtained despite this, the situation is more akin to unlawful hacking and should be grounds for a CFAA claim.[24]

This Comment focuses on the use of electronic code and automated "bots," specifically on their use in buypage, or checkout page, encryption, Completely Automated Public Turing test to tell Computers and Humans Apart (CAPTCHA) protections, Internet Protocol blocks, and other measures used by website owners to enforce their Terms of Service contracts. Those commenters that argued the CFAA applies to all "bot" use often cite to prosecutorial discretion as a way to remedy the gap between less harmful "benign hacking" of public information and serious violations of the CFAA.[25] This public policy argument, while reasonable in theory, could have disastrous consequences in practice if an alleged violator piques the interest of a politician or prosecutor looking to make a name for themselves or set an example of the alleged violator. Courts similarly have analyzed breach of Terms of Service CFAA claims in different ways. While some courts found contractual breaches a sufficient basis for a CFAA claim[26] others recognized the dangers of such a broad policy.[27]

---

[22] Jones, *supra* note 21, at 265–66.
[23] *Id.* at 271; *see also* Katherine Mesenbring, *Field, Agency, Code, or Contract: Determining Employees' Authorization Under the Computer Fraud and Abuse Act*, 107 MICH. L. REV. 819, 821 (2009).
[24] Jones, *supra* note 21, at 271.
[25] Mesenbring, *supra* note 23, at 838–840 (focused more on employee/employer relationships and CFAA).
[26] Ebay, Inc. v. Bidder's Edge, 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000).
[27] LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. 2009); *see also,* United States v. Nosal, 676 F.3d 854, 863 (9th Cir. 2012).

Part II of this Comment will first discuss an overview of automated software robots and their history in society. Part III will discuss a brief overview of the CFAA. Part III will also focus on the background of the CFAA. Part IV will discuss the history of automated software robots in the court system and evolving views on their legality. Part IV will also address previous CFAA decisions under civil law and the statute's potential expansion into the criminal sector. Part V will highlight the benefits of automated "bots" in the internet and how they can be useful in a multitude of areas. This part will then explain how the "damage" and "unauthorized" or "exceeding authorized" access prongs of the CFAA are not inherently met when "bots" are employed contrary to a website's Terms of Service. Part V will also discuss the dangers in allowing prosecutors to have too much discretion under the CFAA. Lastly, Part VI will conclude this Comment.

II. The Pros and Cons of Automated Software Robots

"Bots," like hacking, can be beneficial or injurious, and can either spur technological progress, or harm valuable resources, depending on the means and ends for which they are used.[28] The same technology goes into both "beneficial webbots" and malicious ones.[29] "Bots" do not inherently change the structure and meaning of the CFAA. Just like other powerful tools, if used improperly they can become a means to violate the CFAA.

"Webbots" are computer programs that are usually created for one specific purpose.[30] They automatically carry out their function once triggered by either a user action or automatically upon the occurrence of an event.[31] Once set in motion, "webbots" work according to their programmed

[28] Schrenk, *supra* note 14, at 6.
[29] *Id*.
[30] *Internet Bot*, TECHNOPEDIA, http://www.techopedia.com/definition/24063/internet-bot (last visited Feb. 12, 2015).
[31] *Id*.

orders.[32] Based on the creation of web and robot, a "webbot" works over the internet independently and does whatever it was created to do without sustained human involvement.[33]

Automated "webbots" can amass information at a much larger scale and much faster speed than any individual or large group of people.[34] "Webbots" can be created as a way to automate virtually any online task.[35] Since constant human input is not required, the "bot" works much more quickly and without any risk of human error.

At inception, "webbots" were seen as a limitless "untapped source of potential projects for software developers and a bountiful resource for business people."[36] "Webbots" were first developed to customize online applications and get catered results through internet web browsers.[37] Even now, the true potential of "webbots" goes beyond any current technological boundaries.[38] "Bots" are used primarily for legitimate business purposes to promote efficiency or sometimes just for convenience.

"Bots" are now a part of daily life. Even a standard search engine like Google or Yahoo! uses "bots" called "search engine spiders" to quickly find relevant results based on a given user inputted search term.[39] Even individuals hoping to get a good reservation for dinner can make use of

---

[32] *Id*.
[33] *Id*.
[34] Schrenk, *supra* note 14, at10.
[35] *Id*.
[36] *Internet Bot, supra* note 30 at 9.
[37] *Id*.
[38] Schrenk, *supra* note 14, at 9.
[39] Internet Bot, *supra* note 30. As an example, when someone uses Google to search for information that person types their query in the search box and prompts Google's "bots" to scour the internet for posted content that corresponds to the queried word or phrase. The "bots" used by Google are obviously substantially advanced and can even predict what you are trying to have them search for before you even finish typing. They can also correct your misspellings based on what the "bot" thinks you meant to type. At the same time, users can override the "bot" by using quotes around specific words as many "experienced" searchers may do.

"bots."[40] There are also conspiracy theorists who believe that "bots" can be used to predict major events and even an apocalypse.[41]

An increasingly large part of the economy is shifting towards automation. Customer service,[42] stock trading and banking,[43] surveillance,[44] shopping, and numerous other fields are moving away from human-dominated roles toward computerized solutions.[45] Naturally, there is much debate on the pros and cons of a largely computer-run economy as compared to traditional human-driven, day-to-day tasks.[46] Over the next two decades, it is estimated that 50% of all jobs in America will be automated.[47]

An increasing number of companies are now automating their customer service operations. Automated customer service solutions can reduce the operating and training costs that accompany a staff of human customer service agents.[48] The use of "bots" and avatars, as they are often called in customer service, is not without flaws, but it promotes competition and innovation. No logical

---

[40] Jessica Sidman, *What's the Toughest Reservation in D.C.?*, WASHINGTON CITY PAPER (Dec. 17, 2013).
[41] Tom Chivers, *'Web-bot project' makes prophecy of 2012 apocalypse*, THE TELEGRAPH (Sep. 24, 2009), http://www.telegraph.co.uk/technology/news/6227357/Web-bot-project-makes-prophecy-of-2012-apocalypse.html (Obviously this "bot" has since been proved not as all-knowing as Google's search predicting capability, see *supra* note 39.).
[42] Alisa Kongthon, Chatchawal Sangkeettrakarn, Sarawoot Kongyoung & Choochart Haruechaiyasak, *Implementing an Online Help Desk System Based on Conversational Agent*, PROCEEDINGS OF THE INTERNATIONAL CONFERENCE ON MANAGEMENT OF EMERGENT DIGITAL ECOSYSTEMS, Oct. 27, 2009, *available at* http://dl.acm.org/citation.cfm?id=1643823.1643908.
[43] Andrei A. Kirilenko & Andrew W. Lo., Moore's Law versus Murphy's Law: Algorithmic Trading and Its Discontents, 27 J. ECON. PERSP. 51 (2013), *available at* http://www.argentumlux.org/documents/Moores_Law_vs_Murphys_Law_Spring_2013_JEP.pdf.
[44] Ross Anderson, *An Eye Without an 'I': Justice and the Rise of Automated Surveillance*, THE ATLANTIC (June 14, 2012), http://www.theatlantic.com/technology/archive/2012/06/an-eye-without-an-i-justice-and-the-rise-of-automated-surveillance/258082/.
[45] *See, infra* Part IV.
[46] *Id*.
[47] Carl Benedikt Frey & Michael A. Osborne, *The Future of Employment: How Susceptible Are Jobs to Compterisation?* (Oxford Martin Programme on the Impacts of Future Technology, Working Paper, Sept. 17, 2013) *available at* http://www.futuretech.ox.ac.uk/sites/futuretech.ox.ac.uk/files/The_Future_of_Employment_OMS_Working_Paper_0.pdf; Aviva Hope Rutkin, *Report Suggests Nearly Half of U.S. Jobs Are Vulnerable to Computerization*, MIT TECHNOLOGY REVIEW (Sept. 12, 2013), *available at* http://www.technologyreview.com/view/519241/report-suggests-nearly-half-of-us-jobs-are-vulnerable-to-computerization/.
[48] Kongthon, et al., *supra* note 42.

argument has been advanced that suggests that the government should control the use of customer service bots or make it criminal.

Stock trading, particularly by hedge funds, has transitioned away from human buy and sell orders to computer algorithms designed to pick up on clues and trade faster than any human. So called "quant funds" or "high-frequency traders" use automated execution technology, a type of "bot," to execute trades based on certain triggers that the computer reads.[49] For example, when the volume of trades on a stock hits a certain point, signaling a large block of trading, the "bot" can act and execute trades before the incoming block trade is completed and before the stock price continues to rise.

While some have argued this financial strategy based on "bots" was responsible for the recent financial crisis[50], others praise its efficiency and ability to generate a profit.[51] Even small-time stock traders who trade based on limit orders use "bots" whether they know it or not. Charles Schwab, a brokerage and banking company, allows any investor to buy stocks using a limit order.[52] This means that the computer will buy the stock automatically when it reaches a given price.[53]

Financial trading "bots" can be used with less than noble intentions, but the solution is not criminalizing their use, it is competition. Institutional investors often use dark pools to keep their trades somewhat insulated from hedge fund "bots". Often using their own "bots", dark pools will execute large trades outside of the public forum so that quant funds see no triggers until the trade is completely executed. Some quant funds have responded by monitoring large transactions and

---

[49] RISHI K. NARANG, INSIDE THE BLACK BOX: A SIMPLE GUIDE TO QUANTITATIVE AND HIGH FREQUENCY TRADING 5 (2013).
[50] SCOTT PATTERSON, THE QUANTS: HOW A NEW BREED OF MATH WHIZZES CONQUERED WALL STREET AND NEARLY DESTROYED IT (2011).
[51] Narang, *supra* note 49.
[52] Stock Order Types: Limit Orders, CHARLES SCHWAB, http://www.schwab.com/public/schwab/nn/articles/Order-Types-Getting-to-Know-the-Basics#limitorder (last visited Nov. 1, 2014)
[53] *Id*. (A sell limit order can also be executed which naturally uses a "bot" to only sell once a given price it attained.).

essentially using bandwidth as a trigger for trading. Once again, competition has spurred private markets to combat this problem.[54] The process accelerates innovation and society is improved as a whole, whereas criminalizing the conduct initially does nothing but ensure one side maintains freedom from competition.

"Bots" are used by individuals as well as large corporations. While some "hackers" may use "bots" to pilfer data from private online sources, that behavior is far from the norm.[55] On an individual scale, executives can use "bots" to sift through millions of news articles and compile only relevant stories, substantially shortening the morning reading.[56] They can also be used by intellectual property holders to search out websites and ensure their patented creation is not being used elsewhere.[57] At the same time, just about every large internet company uses "bots". Massive internet corporations like Google and Yelp all use "bots" in a multitude of ways and users benefit from these "bots" daily.[58]

On third-party websites, when the "bot" owner is not the website owner, "bots" are most often used for one of three purposes: buypage encryption; internet protocol blocks; and CAPTCHA code. Buypage, or checkout page, encryption is used by some website owners to block access to the checkout page of a website.[59] It can have a valid purpose, most notably to restrict purchase ability to only those individuals who can legally buy—be it alcohol to minors or guns to registered

---

[54] Simone Foxman, *Those Flash Boys: How the "Navy Seals" of Trading are Taking on Wall Street's Predatory Robots*, QUARTZ (Mar. 31, 2014), http://qz.com/138388/how-the-navy-seals-of-trading-are-taking-on-wall-streets-predatory-robots/.

[55] Schrenk, *supra* note 14, at 325 (This so-called "dark side" use of "destructive webbots" is a small percentage of those in existence).

[56] *Id* at 18.

[57] *Id*.

[58] *What is Yelp's Recommendation Software*, YELP INC., http://www.yelp-support.com/article/What-is-Yelp-s-recommendation-software?l=en_US (last visited Nov. 1, 2014) (As discussed in Part IV, many of these same companies are those seeking to persuade courts to condone third-party "bot" use and allow them to set the terms of the CFAA through their Terms of Service.); see Internet Bot, *supra* note 30.

[59] Brief for Plaintiff-United States at 18, United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (No. CRIM. 10-114 KSH).

individuals. In this internet age, as compared to brick-and-mortar stores, it is much harder to limit alcohol sales to minors, or to restrict firearms purchases, or to protect credit card information.[60] Buypage encryption can cut out purchasing ability to certain people. It restricts certain individuals from tampering with the checkout page. This is done by the websites to shield them from liability.

Internet protocol (IP) blocks are also widely used to restrict unwanted users. They are designed to prevent certain users originating from known locations or regions from calling up a website. They can be used to prevent "hackers" from injecting viruses, to block access to banking information, and to stop mass spam emails.[61] They cannot, however, be used at the whim of the website owner to enforce his or her preference.[62] When Verizon blocked IP addresses from certain regions in Europe as a way of limiting spam to its members, it led to a class action lawsuit when users could not access needed emails.[63] Circumventing IP blocks has blossomed into a necessary market as well. Masking IP addresses can be a proactive way to self-protect from viruses or hacking.[64] Because IP addresses are unique to each user, they can compromise a user's location or identify. Individual users can just as easily hide their IP addresses through various free programs on the internet.[65]

---

[60] *See, e.g.*, Rebecca S. Williams & Allison Schmidt, *The Sales and Marketing Practices of English-Language Internet Alcohol Vendors*, 109 SOC'Y FOR STUD. ADDICTION RES. REP. 432 (2014); *But see*, Granholm v. Heald, 544 U.S. 460 (2005) (The court disagreed with New York that more protection was needed to protect online liquor stores from access by minor. The court found "little evidence that the purchase of wine over the Internet by minors is a problem," because minors need "instant gratification" and can go to local liquor stores in less time than internet retailers.).

[61] John Gartner, *Verizon's E-Mail Embargo Enrages*, WIRED, (Jan. 10, 2005), http://archive.wired.com/techbiz/media/news/2005/01/66226.

[62] Nate Anderson, *Verizon Proposes Settlement For Class Action Lawsuit*, (Apr. 5, 2006), http://arstechnica.com/uncategorized/2006/04/6525-2/.

[63] *Id*.

[64] UnThreat technology, UNTHREAT ANTIVIRUS, http://www.unthreat.com/technology (last visited Feb. 12, 2015).

[65] MASK MY IP, http://www.mask-myip.com/ (last visited Nov. 1, 2014).

CAPTCHA code, unlike the other two measures, is primarily used to foil automated "bots".[66] As the name implies, CAPTCHA stands for Completely Automated Public Turing Test to Tell Computers and Humans Apart and is designed to "capture" and trick computers.[67] CAPTCHA has a multitude of applications, only one of which is preventing malicious attacks on websites.[68] On a macro level, devices like CAPTCHA that distinguish humans from computers cannot "guarantee that bots won't read the pages; it only serves to say 'no bots, please.'"[69] CAPTCHA can also be used to advance artificial intelligence and lead to technological progression.[70]

At the same time, CAPTCHA defeating "bots" may be necessary for some users. Individuals with vision problems are often thwarted by CAPTCHA code which is based on distorted images.[71] Alternatives to CAPTCHA that can be used by the visually impaired are being created, but lag far behind in popularity to CAPTCHA.[72] Until these alternatives catch up, certain sections of the population need "bots" that can help them get around CAPTCHA devices and access a site just as anyone else can.

III. The Computer Fraud and Abuse Act

i. Brief Overview of the Computer Fraud and Abuse Act

---

[66] Brief for Plaintiff-United States at 19, United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (No. CRIM. 10-114 KSH).
[67] Luis von Ahn, Manuel Blum & John Langford, *Telling Humans and Computers Apart Automatically: How Lazy Cryptographers do AI*, 47 COMM. ACM 57, 58 (2004), *available at* http://www.captcha.net/captcha_cacm.pdf.
[68] *Id*.
[69] *Id*.
[70] *Id*., at 59–60.
[71] *Computer Pioneer Aids Spam Fight*, BBC NEWS, (Jan. 8, 2003), http://news.bbc.co.uk/2/hi/technology/2635855.stm.
[72] Hannah Alvarez, *Think Your Site Needs CAPTCHA? Try These User-Friendly Alternatives*, USER TESTING, (Apr. 9, 2014), http://www.usertesting.com/blog/2014/04/09/think-your-site-needs-captcha-try-these-user-friendly-alternatives/.

The Computer Fraud and Abuse Act (CFAA) prohibits "access" of a computer either "without authorization" or "exceeding authorized access."[73] The statute focuses on information protected for national defense,[74] financial records,[75] and certain other private information obtained fraudulently. As compared national defense documents and bank financial records, with private information the statute is more specific and requires actual "damage" to a "protected computer."[76]

The fundamental component of the CFAA is "access." Access, however, is an antiquated notion based on how computers worked in the 1980s when the CFAA was originally devised. Today with the internet dominating most computing and cybersecurity concerns, the notion of "access" makes little sense in many contexts. Historically, when computers were hardwired they needed to be physically accessed to be used, but the internet has completely changed this line of thinking. The internet has stripped part of what the CFAA was designed to do. Because of this, prosecutors have successfully persuaded courts to expand the scope of the CFAA. This behavior, however, can lead to a widening gap, in terms of Congressional intent, between the CFAA at inception and what is has become. Courts should leave it to Congress to update the CFAA into the modern technological world.

ii. Background of the Computer Fraud and Abuse Act

The Computer Fraud and Abuse Act was the product of an American Bar Association (ABA) report and Congressional debate. In 1984, the American Bar Association Task Force on Computer

[73] 18 U.S.C. § 1030 (2008).
[74] *Id*. § 1030(a)(1).
[75] *Id*. § (a)(2)(A).
[76] *Id*. § (a)(5)(A).

Crime issued the Report on Computer Crime that found about 48% of the 1,000 private and public agencies surveyed had experienced some form of computer crime in the previous year.[77] According to the Report on Computer Crime, the most serious types of computer crime consisted of theft of property, data destruction, financial skimming, software destruction, and fraud.[78]

This ABA report prompted Congress to reexamine computer crime and enact the Computer Fraud and Abuse Act (CFAA) in 1986.[79] The Congressional Committee on the Judiciary recognized that computer crimes cause severe financial losses and regulation was needed to safeguard against potential monetary theft.[80] The Committee also realized that identifying information, passwords, and medical records should be protected and their theft prohibited, even absent discrete financial loss.[81]

Prior to enacting the CFAA, it was suggested that the federal statute should be broad "so that no computer crime [was] potentially uncovered."[82] The Committee expressly rejected this suggestion and sought to limit the CFAA to Federal Government computers where "certain financial institutions are involved or where the crime itself is interstate in nature."[83]

Congress designed the CFAA to criminalize computer theft, fraud, hacking, and acts that damage electronic data and security.[84] Congress limited the CFAA's reach based on three core

---

[77] AM. BAR ASS'N SECTION OF CRIMINAL JUSTICE, REPORT ON COMPUTER CRIME -TASK FORCE ON COMPUTER CRIME (June 1984), *available at* https://www.ncjrs.gov/App/Publications/abstract.aspx?ID=95114 [hereinafter ABA COMPUTER CRIME REPORT].
[78] *Id.* (The report found action needed to be taken to discourage and punish "the use of computers to steal tangible or intangible assets, the destruction or alteration of data, the use of computers to embezzle funds, the destruction or alteration of software, and the use of computers to defraud.")
[79] S. REP. 99-432, *supra* note 6, at 2.
[80] *Id.*; ABA COMPUTER CRIME REPORT, *supra* note 77.
[81] S. REP. 99-432, *supra* note 6, at 2–3; ABA COMPUTER CRIME REPORT, *supra* note 77.
[82] S. REP. 99-432, *supra* note 6, at 4; ABA COMPUTER CRIME REPORT, *supra* note 77.
[83] S. REP. 99-432, *supra* note 6, at 4; ABA COMPUTER CRIME REPORT, *supra* note 77.
[84] S. REP. 99-432, *supra* note 6.

ideas: the first based on national security; the second focused on financial institutions; and the third based on private electronic theft.[85]

Under the national security provision, the individual must "knowingly access[] a computer without authorization or exceeding authorized access" and obtain information protected by an "Executive order or statute . . . against unauthorized disclosure for reasons of national defense or foreign relations."[86] An individual can also be guilty based on national security protection if they "intentionally, without authorization to access any nonpublic computer of a department or agency of the United States, access[] such a computer of that department or agency that is exclusively for the use of the Government of the United States."[87]

To protect financial information, the CFAA criminalizes an individual who "intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains . . . information contained in a financial record of a financial institution, or of a card issuer . . . [or] of a consumer reporting agency on a consumer."[88]

Private electronic information is also protected by the CFAA when an individual "knowingly and with intent to defraud, accesses a protected computer without authorization, or exceeds authorized access" and this conduct furthers the fraud, "unless the object of the fraud and the thing obtained consists only of the use of the computer and the value of such use is not more than $5,000 in any 1-year period."[89] The CFAA, like many Congressional statutes, can only apply to limited private actions based on the commerce clause. The only private electronic information protected is that on "protected computers," defined as the computers of a financial institution or the United

[85] *Id*.
[86] 18 U.S.C. § 1030(a)(1) (2008).
[87] *Id*. at § 1030(a)(3).
[88] *Id*. at § 1030(a)(2)(A).
[89] *Id*. at § 1030(a)(4).

States Government or, if not exclusively used by either of those two entities, computers that affect interstate or foreign commerce.[90]

Each of these three core ideas centers on the principles of damage, unauthorized access, and exceeding authorized access. In order to violate the CFAA, the individual must first be "unauthorized" or must deliberately "exceed[] authorized access."[91] "Unauthorized access" is reserved for situations where the individual is not granted access.[92] It does not speak to the means of access, but simply whether that individual was allowed.[93] "Exceed[ing] authorized access" covers individuals who are actually authorized to use a given computer.[94] It is only invoked when the individual goes beyond his or her access and actually obtains information that he or she was not entitled to, or alters information in the computer when he or she was not allowed to do so.[95]

At the same time, there must be a real, tangible harm and loss to meet the "damage" requirement of Section 1030(e)(8).[96] "Damage," encompasses harm to data or equipment that results in a loss.[97] "Damage" relates to physical, tangible impairment that leads to a real pecuniary loss.[98] The damage must be quantifiable and reach the aggregate threshold of $5,000.[99] It cannot be an arbitrary, theoretical harm.

IV. The Court System and the CFAA

---

[90] *Id*. at § 1030(e)(2).
[91] *Id*. at § 1030(a)(1).
[92] *See* Power Equip. Maint., Inc. v. AIRCO Power Servs., Inc., 953 F. Supp. 2d 1290, 1296 (S.D. Ga. 2013).
[93] *Id*.
[94] 18 U.S.C. § 1030(e)(6) (2008).
[95] *Id*. at § 1030(e)(6).
[96] *See* Czech v. Wall St. on Demand, Inc., 674 F. Supp. 2d 1102, 1108 (D. Minn. 2009); Yoder & Frey Auctioneers, Inc. v. Equipment Facts, LLC, No. 14-3002, 2014 WL 7247400, at *5 (6th Cir. Dec. 22, 2014).
[97] 18 U.S.C. § 1030(e)(8) (2008).
[98] Wall St. on Demand, Inc. 674 F. Supp. 2d at 1108.
[99] 18 U.S.C. § 1030(c)(4)(A)(i)(I) (2008).

i. Automated Software Robots in the Legal System

With the advent and ever-expanding capability of "bots," courts have inconsistently applied the CFAA to them. The CFAA's flexibility has been interpreted by different courts in different ways. Back in 2000, eBay, an online auction site, tried to defend its business against "bots" using the CFAA.[100] EBay argued that Bidder's Edge (BE), a company that used "bots" to search, copy, and aggregate eBay listings—as well as other online auction company listings—in one place, was in violation of the CFAA.[101] BE did not host any auctions, but based its business on allowing customers to view auctions from various sites in one place.[102] The United States District Court, for the Northern District of California, allowed an injunction against BE because it used "bots" in violation of eBay's Terms of Service.[103] Without deciding on any one ground, the court sided with eBay that when the software robot—which could execute thousands more tasks than a human in the same amount of time—was used, it drained eBay's capacity and resources, increasing the likelihood of a system crash.[104] The court only enjoined BE's activity as long as "bots" were involved and made clear that no information obtained with a non-automated program was precluded.[105]

The United States Court of Appeals for the Ninth Circuit, overseeing the District Court in California that decided *Ebay, Inc.*, vacillated on the relevance of "bots" to a valid CFAA claim.[106]

---

[100] Ebay, Inc. v. Bidder's Edge, 100 F. Supp. 2d 1058 (N.D. Cal.2000).
[101] *Id*.
[102] *Id* at 1061.
[103] *Id*.
[104] *Id*. at 1061-62 (The District Court allowed a preliminary injunction without evidence of any real crash, but merely a theoretical increased likelihood, but the case did not progress further.); *Id*. at 1071 (The court also recognized that "eBay does not claim that this consumption has led to any physical damage to eBay's computer system, nor does eBay provide any evidence to support the claim that it may have lost revenues or customers based on this use[.]").
[105] *Id*. at 1073.
[106] United States v. Nosal, 676 F.3d 854, 856, 862–63 (9th Cir. Cal. 2012).

When a former employee of an executive search firm convinced some of his former colleagues, who still worked at the firm, to transmit him confidential information from the company's server to help start a competing business, the employer sought sanctions via the CFAA.[107] The current employees were allowed to access the database, but could not disclose the confidential information to someone outside of the company.[108] Because of this, the employer argued that the "exceeding access" requirement was met.[109] The court avoided the question of whether Terms of Service could serve as the basis for a criminal CFAA claim.[110] The court did, however, find that using "bots" in contravention of a Terms of Service policy does not constitute "exceeding authorized access."[111] The CFAA is not concerned with misappropriation liability and "bots" that violate a contractual Terms of Service are outside the scope of the CFAA.[112]

The same District Court in California tried to reconcile past cases when Craigslist, another independent sales website, sought to limit "bot" use from a competitor through its Terms of Service.[113] 3Taps was a company that employed "bots" to copy content posted on Craigslist, aggregate it, and republish.[114] After 3Taps ignored a cease and desist letter, Craigslist brought a CFAA suit against 3Taps.[115] Craigslist argued that 3Taps violated the Terms of Service it implicitly agreed to by using Craigslist's website, and thus exceeded its authorized access under 1030(e)(8) of the CFAA.[116] The court looked to *Nosal* and found the term "exceeds authorized

[107] *Id.* at 856.
[108] *Id.*
[109] *Id.*
[110] *Id.* at 863 ("We need not decide today whether Congress could base criminal liability on violations of a company or website's computer use restrictions.").
[111] *Id.*
[112] *Nosal*, 676 F.3d at 863.
[113] Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 968–70 (N.D. Cal. 2013).
[114] *Id.* at 966.
[115] *Id.* at 967.
[116] *Id.*

access" only relates to access restrictions and not to how the information is used.[117] The District Court avoided the key question of whether a website's Terms of Service violation "can ever support liability under the CFAA."[118] The District Court did, however, find the cease and desist letter determinative for "unauthorized access" under 1030(a)(1).[119] Because Craigslist denied 3Taps access "for any purposes" via the cease and desist letter, any later use violated the CFAA.[120]

Another Federal District Court in similar circumstances to those presented in California Federal Court did not grant an injunction to the company seeking to insulate itself from "bots" through Terms of Service.[121] Southwest Airlines used a business model that awarded customers better boarding options depending on how quickly they checked-in once they were allowed.[122] Boardfirst used "bots" to automatically check-in Southwest customers as quickly as possible once they were allowed by Southwest.[123] Twenty-four hours before the flight Southwest allowed customers to check-in and any customers that paid Boardfirst $5 were virtually guaranteed to be checked-in first and thus granted priority boarding.[124] This is because the "bots" used by Boardfirst could complete their task in a fraction of the time any individual customer could. The "bots" could execute the task they were programmed to do and checked-in customers instantly, much faster than any actual Southwest customer could type southwest.com let alone go through the steps to check-in. Using a similar breach of the Terms of Service logic, Southwest argued Boardfirst was not

---

[117] *Id*. at 968 (citing *Nosal*, 676 F.3d at 860–62).
[118] *Craigslist Inc*., 942 F. Supp. 2d at 969. (The Court need not decide whether violating 'restrictions on access to information' contained in a website's terms of use can ever support liability under the CFAA.").
[119] *Id*. at 969.
[120] *Id*.
[121] Southwest Airlines Co. v. BoardFirst, L.L.C.,2007 U.S. Dist. LEXIS 96230 (N.D. Tex. Sept. 12, 2007).
[122] *Id* at *1 (All customers were able to check-in for their flight beginning twenty-four hours before the departure time. Those customers that checked-in as soon as possible once this ban was lifted—ie 23 hours before the flight as opposed to 2 hours before the flight—received better boarding options once the flight actually did depart.).
[123] *Id*.
[124] *Id* at *1-2

only violating the Terms of Service, but also the CFAA.[125] The United States District Court for the Northern District of Texas found that, contract claims aside, there was no federal violation[126] The CFAA charge was not valid and could not be used to sustain an injunction, especially given that Southwest's website was a "publicly available website that anyone [could] access and use."[127] The court was not swayed by a Terms of Service violation and found no actual impairment or damage.[128]

In a recent CFAA case involving "bots," criminal charges were brought against an events ticket reseller for using automated software.[129] Like many previous "bot" cases, a website owner tried to argue that criminal fraud occurs when the website Terms of Service are violated whereas the defendant argued the website owner's charge sought to regulate a legal secondary market.[130] Lowson, the defendant, and his company purchased large blocks of event tickets using "bots" and then resold the tickets in the secondary market for a profit.[131] Online ticket vendors used certain measures like buypage encryption, IP blocks, and CAPTCHA code to try and ensure the general public would be able to purchase tickets with no one gaining an advantage.[132] Lowson and his company used "bots" to avoid these measures and purchase tickets that were otherwise available to them and the rest of the general public.[133] The only issue was in the way Lowson's team purchased tickets. Lowson was indicted, but the case was resolved prior to a trial with all parties

[125] *Id* at *2.
[126] *Id* at 6-7.
[127] BoardFirst, L.L.C.,2007 U.S. Dist. LEXIS 96230 at *14.
[128] *Id* at 15.
[129] United States v. Lowson, 2010 U.S. Dist. LEXIS 145647(D.N.J. Oct. 12, 2010).
[130] *Id* at *1.
[131] *Id*.
[132] *Id*.; Brief for Plaintiff-United States at 18, United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (No. CRIM. 10-114 KSH).
[133] *Lowson*, 2010 U.S. Dist. LEXIS at *4.

agreeing out of court.[134] This case, like much of the law regarding the CFAAs reach as it pertains to "bots," failed to take a strong stance for or against their inherent legality.

ii. Civil Application of the CFAA in Other Contexts

Courts have permitted civil CFAA claims to succeed based on Terms of Service violations, but allowing these violations to carry into the criminal context can be a dangerous precedent. In the civil context when automated programming "bots" and "data mining" were involved, the court found CFAA violations without substantial analysis.

When a website owner sought to enforce its Terms of Service and stop defendants from sending "unsolicited bulk e-mail" messages, more commonly known as spam, to its members, it brought a CFAA claim in the Eastern District of Virginia.[135] The defendant, LCGM, maintained numerous America Online (AOL) memberships that provided the company with access to AOL chatrooms.[136] With this access, LCGM used an extractor "bot" to collect email addresses of other AOL members.[137] LCGM, which operated pornographic websites, sent approximately 300,000 unsolicited emails a day to the AOL email addresses it collected with the "bot."[138]

The District Court found AOL's Terms of Service controlling on what constitutes authorized access.[139] Without significant analysis, the court found AOL member email addresses to be protected information that was proprietary to AOL.[140] Because sending spam was contrary to

[134] *Id*. at *1; Brief for Plaintiff-United States at 16–18 United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (No. CRIM. 10-114 KSH).
[135] America Online v. LCGM, Inc., 46 F. Supp. 2d 444 (E.D. Va.1998).
[136] *Id*. at 448.
[137] *Id*.
[138] *Id*.
[139] *Id*. at 451 ("These actions were unauthorized because they violated AOL's Terms of Service").
[140] *Id*. at 450.

AOL's Terms of Service, the court reasoned that it constituted "exceeding authorized access" when obtained via "extractor software programs"—data mining, "bots".[141] The court determined that LCGM was liable under §1030(a)(2)(C) for exceeding any access AOL had granted it as a member when it used "extractor software programs" that violated AOL's Terms of Service.[142] The court also found the requisite damage to AOL's computer network because the defendants used "bots" to "camouflage[] their identities, and evade[] plaintiff's blocking filters and its members' mail controls."[143]

In a similar case in the Northern District of Iowa, AOL sought to enforce its Terms of Service through the CFAA against a third-party email sender.[144] Defendant National Healthcare Discount, Inc., purchased leads (email addresses) from an independent contractor and sent marketing materials to the purchased addresses.[145] Despite recognizing that "the evidence presented at trial failed to clear the murky water sufficiently" to determine if Terms of Service violations constitute "without authorization," the court relied on its preliminary conclusion, without analysis, that it "exceeds authorized access."[146] The court also found the requisite damage based on evidence that each unsolicited email sent over AOL's system cost AOL $0.00078 and diminished AOL's capacity to serve its customers.[147]

The United States Court of Appeals for the First Circuit also found that an express provision limiting "the use of scrapers" in a website's Terms of Service to be dispositive on whether access was authorized.[148] Absent an express provision, inferring a violation of the CFAA would not be

---

[141] LCGM, Inc., 46 F. Supp. 2d at 450.
[142] *Id*.
[143] *Id*. at 451.
[144] Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890 (N.D. Iowa 2001).
[145] *Id*. at 896.
[146] Nat'l Health Care Disc., Inc., 174 F. Supp. 2d at 899 (N.D. Iowa 2001).
[147] *Id*. (*citing* America Online, Inc. v. National Health Care Discount, Inc., 121 F. Supp. 2d 1255, 1274-75 (N.D. Iowa 2000)).
[148] Ef Cultural Travel Bv. v. Zefer Corp., 318 F.3d 58, 62 (1st Cir. Mass.2003).

practical and the website owner would likely have to show that the information was confidential.[149] EF Cultural Travel, a travel company, brought suit under the CFAA against a competitor (Explorica) as well as the "scraper" creator company (Zefer).[150] Zefer, the "bot" creator, developed a computer program that copied price information for various travel options on EF Cultural Travel's website.[151] Explorica hired Zefer to create this tool and provide it with EF Cultural Travel's pricing information. Explorica used the information to set its prices slightly below Explorica's and gain a competitive advantage.[152] EF Cultural sued under both the CFAA and copyright statutes. The court found the copyright claim to be meritless, but allowed the CFAA claim even though the behavior did not violate any stated Terms of Service.[153]

The First Circuit Court of Appeals recognized that Explorica could have compiled the same database of EF Cultural Travel's pricing information, albeit not as quickly, without "scrapers," but differentiated the two situations without any further explanation.[154] The court held that it "would raise serious public policy concerns" to allow the CFAA to enforce an explicit provision in a website's Terms of Service that limits competitors from manually using public information on the website to create a database, but failed to address how a competitor that compiles the same information more efficiently with "bots" could be condemned without issue.[155] While the court stated these broad propositions without practical support and its arguable general fear of "bots" is unfounded, neither issue directly influenced the court's holding. The key reason for the court's civil injunction was based on the existence of a confidentiality agreement signed between

[149] *Id*. at 63.
[150] *Id*. at 60.
[151] *Id*.
[152] *Id*.
[153] *Id*. at 62–63.
[154] Zefer Corp., 318 F.3d at 60 ("Strictly speaking, the accessed information is…available to anyone who views the site.").
[155] *Id*. at 63. (*citing* Food Lion, Inc. v. Capital Cities/ABC, Inc., 194 F.3d 505, 516-18 (4th Cir. 1999)).

defendant employee of a competitor and the website owner which clearly exceeded access of the computer servers.[156]

Some courts analyzing a CFAA claim based on a beach of contract recognized the danger in allowing contracts to form the basis of federal statutory violations.[157] When an employee had access to an employer computer and network, but violated a term of his employment contract by using the computer to email company documents, including financial statements and client lists, to his personal computer prior to leaving the company, the United States Court of Appeals found there was no valid CFAA claim.[158]

LVRC brought a CFAA claim against a former employee alleging that his use of company computers violated §1030(a)(2)(4) because it was unauthorized and his use of company email to send himself documents exceeded any authorization he was given.[159] Brekka, the former employee was given access and log-in information for LVRC's computers as part of his employment.[160] The information he emailed to himself likewise was related to his work for LVRC.[161] After termination, Brekka used his unexpired log-in information to send himself additional information from his company email address.[162] LVRC argued this use was unauthorized or alternatively exceeded any authorization he had when his employment terminated.[163]

The Ninth Circuit Court of Appeals recognized that Brekka may have acted against LVRC's wishes, but that does not rise to a CFAA violation. Just because the individual violated a duty of loyalty or state law claim does not mean they violated the CFAA.[164] "Nothing in the CFAA

---

[156] *Id*. at 61.
[157] LVRC Holdings LLC v. Brekka, 581 F.3d 1127 (9th Cir. Nev. 2009).
[158] *Id*. at 1128–30.
[159] *Id*. at 1128.
[160] *Id*.
[161] *Id*.
[162] *Id*. at 1129–30.
[163] *Brekka*, 581 F.3d at 1130.
[164] *Id*. at 1135.

suggests that a defendant's liability for accessing a computer without authorization turns on whether the defendant breached a state law duty of loyalty to an employer."[165] The court understood that contracts cannot govern distinct federal laws.[166] The individual also logged onto the company website to access statistics and other company information using an old password, over a year after his employment ended.[167] Even after the employment ended and the individual became a competitor, the court found no basis for a CFAA claim. So long as individuals are authorized to use a computer, they "remain authorized… even if the [individual] violates those limitations."[168]

V. The CFAA Does Not Criminalize The General Use Of Automated "Bots" That May Be Contrary To Terms Of Service Contracts

"Bots" do not inherently violate the CFAA. They are tools that can be used both legally for valid business purposes or illegally to cause harm. Like almost any other new technology, "bots" have unknown potential and can be either abused or esteemed.[169] New technology scares people. Until they can fully understand it, some people will fear it and try to condemn its use.[170] Because of this, leaving "bot" use practices to prosecutorial discretion has failed. It has proven to be an insufficient way of dealing with the new technology and its potential criminal component.

The internet is not a foreign unknown like it once was and has not been so for a long time. In 2011, the United States Census Bureau found that nearly 76% of households had a computer, up

---

[165] *Id*.
[166] *Id*.
[167] *Id*. at 1130.
[168] *Id*. at 1133.
[169] *See, e.g.*, ARTHUR C. CLARKE, PROFILES OF THE FUTURE, HAZARDS OF PROPHECY: THE FAILURE OF IMAGINATION (1973).
[170] *Id* at 12 ("Any sufficiently advanced technology is indistinguishable from magic.").

from just under 62% in 2003 and roughly 8% in 1984 when the CFAA was first conceived.[171] It is not reasonable to argue that just because a term references computers it is automatically ambiguous and confusing. While some commenters argue the CFAA is ambiguous and can be stretched by courts to cover a wide array of behavior, most of these arguments focus on the internet as a great unknown.[172]

At the same time, if we are to follow previous commenters reasoning that the language is ambiguous because of the technical nature of the internet and website use, it cannot be followed that the statute suddenly covers Terms of Service contract issues without some legislative guidance. "Legislatures and not the courts should define criminal activity."[173] Congress could not have conceived that Terms of Service breaches would fall under the provisions of the CFAA because websites didn't even exist in 1986 when the statute was adopted.[174] On April 30, 1993, CERN published a statement that put CERN software into the public domain, essentially making the internet available to the public.[175] In a time before publicly-available computers or websites, Congress could not have contemplated "unauthorized access" to include violation of a website's Terms of Service.[176] When the CFAA was created, the idea of a global internet used daily by hundreds of millions of people was not even contemplated. While it is important for statutes to be flexible and grow with time, allowing such profound changes as granting private website owners discretion to set the limits of criminal activity cannot be permitted.

---

[171] Computer and Internet Use in the United States: Population Characteristics, U.S. CENSUS BUREAU (U.S. 2013), http://www.census.gov/prod/2013pubs/p20-569.pdf.
[172] *See*, Orin S. Kerr, *supra* note 20, at 1621.
[173] United States v. Bass, 404 U.S. 336, 347 (1971).
[174] Scott Gilbertson, *The Very First Website Returns to the Web*, WEBMONKEY (Apr. 30, 2013), http://www.webmonkey.com/2013/04/the-very-first-website-returns-to-the-web/.
[175] *CERN Statement Concerning CERN W3 Software Release Into Public Domain*, CERN DOCUMENT SERVER, https://cds.cern.ch/record/1164399 ; *see also*, Gilbertson, *supra* note 174.
[176] Nicolas R. Johnson, I Agree to Criminal Liability: Lori Drew s Prosecution Under § 1030(A)(2)(C) of the Computer Fraud and Abuse Act, and Why Every Internet User Should Care, 2009 U. ILL. J.L. TECH. & POLY 561, 567 (2009).

In enacting the CFAA, the Judiciary Committee found Federal criminal penalties "appropriate punishment for certain acts" not for every unwanted computer activity and it should be reinforced with improved security programs.[177] If the CFAA can be used to criminalize breach of contract disputes, everything from "making a fake Facebook account for your cat" to letting your "friend log in to your Pandora account could land you with felony charges," all because you clicked "I agree."[178]

Breach of contract based CFAA claims could easily prove unmanageable given the prevalence of arbitration clauses. Recently many online companies have incorporated arbitration clauses into their Terms of Service.[179] If breach of a Terms of Service agreement can serve as the basis for a CFAA violation, proof of the breach would be a required element of the offense. This element may not be so easy to adjudicate, however, given required forums specified in the contract. "Mini-trials on breaches of contract would be required to establish criminal liability."[180]

Some have argued that as a broad policy, Terms of Service violations cannot serve as the foundation for a CFAA claim, but using automated software code is more akin to unlawful "hacking" and should be barred by the CFAA.[181] According to proponents of this theory, the purpose of automated programs is to bypass security and defeat barriers to access.[182] "Data mining," "scrubbers," "scrapers," and other automated programs, however, are less about attacking

---

[177] S. REP. 99-432, *supra* note 6, at 3.
[178] *Our Internet Policy Shouldn't be Stuck in the 80's; The History,* FIX THE CFAA, http://www.fixthecfaa.com/#/history (last visited Oct. 27, 2014).
[179] Sherman Kahn and David Kiferbaum, Browsewrap Arbitration? Enforcing Arbitration Provisions in Online Terms of Service, 5 N.Y. STATE BAR ASSOC. N.Y. DISPUTE RESOLUTION LAWYER 36 (2012), available at http://media.mofo.com/files/Uploads/Images/121029-Browsewrap-Arbitration-Enforcing-Arbitration-Provisions-in-Online-Terms-of-Service.pdf.
[180] Brief for Defendant at 12-13, United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (No. CRIM. 10-114 KSH).
[181] Brief for Defendant at 2, United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (No. CRIM. 10-114 KSH).
[182] Brief for Defendant at 12-13, United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (No. CRIM. 10-114 KSH).

security measures and more focused on efficiency.[183] The CFAA cannot be applied by fiat to any Terms of Service contractual theory just because a "bot" was used.

i. Automated Bots Are Useful Tools to Promote Competition and Improve Efficiency

"Data mining" is a valuable tool with "enormous application in numerous fields."[184] According to the Society for Industrial and Applied Mathematics International Conference on Data Mining, high-performance analysis and algorithms can pool large, complex datasets and extract useful information for businesses.[185]

Automated programming code, just like anything else, can be used properly and for a beneficial purpose or can be used to deleterious ends. The purpose of the CFAA is to criminalize certain illegal behavior over the internet in regards to computer access. "Bots," just like hacking, connotes a scary and malicious image, but only because certain groups have been successful in persuading courts and people in power to believe so. The technology that goes into a "beneficial webbot" as compared to a destructive one designed to disrupt networks, infect servers with viruses, or "hack" private information, is identical.[186] The main difference is intent. The CFAA cannot be used to broadly sweep over all automated programs that collect public information and should be reserved

[183] Schrenk, *supra* note 14; *See also*, Jason Frand, *Data Mining: What is Data Mining?*, UCLA ANDERSON SCHOOL OF MANAGEMENT, http://www.anderson.ucla.edu/faculty/jason.frand/teacher/technologies/palace/datamining.htm (last visited Oct. 29, 2014).
[184] *2015 SIAM International Conference on DATA MINING*, SOCIETY FOR INDUSTRIAL AND APPLIED MATHEMATICS, http://www.siam.org/meetings/sdm15/ (last visited Oct. 29, 2014) (describing data mining as "the computational process for discovering valuable knowledge from data…[with] enormous application in numerous fields.").
[185] *Id*.
[186] Schrenk, *supra* note 14, at 6.

for only those that violate the Act's provisions, either by using fraud and causing damage, mining confidential financial information, or accessing protected government information.

"Webbots" have vast untapped potential and can make e-commerce and internet use as a whole immensely more efficient.[187] "Webbots" can acquire useful information in an infinitesimally small fraction of the time it takes an individual or even a team of individuals. "Webbots" can be created for specific tasks and can automate virtually any process, notifying a user only when something requires their attention.[188] While some of those tasks may be illegal, others are not only legal, but beneficial. Speed and efficiency are key for a business advantage and "webbots" can even be used to locate and track information quickly, as is the case with this google short url footnote.[189] "Webbots" improve business efficiency and competition. A sweeping policy against them all, aside from being overbroad and reaching perfectly legal actions, will have a severe chilling effect that will hurt economic growth.[190]

Everything from customer service, to stock trading and banking, to surveillance, is progressing towards automation.[191] While some people appreciate the efficiency and cost reductions that go along with automation, others prefer a reversion back to pre-robot interaction.[192] Preferences are permissible, but they do not correspond to legality. While automated customer service is not

---

[187] *Id*. at 10.
[188] *Id*.
[189] Graham Charlton, *How to use Google Analytics URL builder to track campaigns*, ECONSULTANCY, http://goo.gl/ccHphs (last visited Oct. 29, 2014) (Google allows individuals to employ google "bots" to create short urls for any website so that they can be more easily copied. Google also allows users to track how often their distributed short urls are clicked and used by others, once again via "bots.").
[190] Jones, *supra* note 21.
[191] *See*, *supra* Part III.
[192] *See, e.g.*, Tim Burrows, *I Hate Most Automation! This One, well…*, WALKING THE SOCIAL MEDIA BEAT (Oct. 11, 2012), http://walkingthesocialmediabeat.com/2012/10/11/i-hate-most-automation-this-one-well/; *but see*, Jason Miller, *Stop Hating on Marketing Automation, Try a Little Tenderness Instead*, COPYBLOGGER, http://www.copyblogger.com/marketing-automation/ (The views of bloggers differ tremendously in this space, as is seen by these two points of view. These two commenters, however, may be particularly polarized in their views given that the former is Police Officer who lectures on criminal investigations and the latter a Senior Manager for Content and Social at Linkedin Marketing Solutions).

something most consumers want, few would argue that it should be criminalized. It is likely that nearly half of all jobs in America will be automated in the next 20 years.[193] Opponents of this argue that unemployment will rise and the economy will suffer. Proponents, however, argue that machines will likely not replace human involvement in the economy, but will actually allow individuals to focus on other tasks and improve efficiency.[194]

While many customers would prefer interaction with a real human being, they would not prefer the increased costs that go along with it. There are some inherent flaws, and "bots" can be created with nefarious intent, but the pros outweigh the cons. Automated business solutions can reduce operating and training costs, promote competition and innovation, and protect individual privacy.[195]

The solution for overcoming competitive "bot" use is not criminalizing it outright, but allowing free competition for non-harmful "bots" and focusing enforcement efforts only on those acts that actually violate the CFAA by causing damage or accessing unauthorized, non-public information. Otherwise, large companies with more bargaining power can seek to criminalize innocent conduct and insulate themselves from any real competition.[196]

---

[193] Carl Benedikt Frey & Michael A. Osborne, *The Future of Employment: How Susceptible Are Jobs to Compterisation?* (Oxford Martin Programme on the Impacts of Future Technology,Working Paper, Sept. 17, 2013) available at http://www.futuretech.ox.ac.uk/sites/futuretech.ox.ac.uk/files/The_Future_of_Employment_OMS_Working_Paper_0.pdf; Aviva Hope Rutkin, *Report Suggests Nearly Half of U.S. Jobs Are Vulnerable to Computerization*, MIT TECHNOLOGY REVIEW (Sept. 12, 2013), http://www.technologyreview.com/view/519241/report-suggests-nearly-half-of-us-jobs-are-vulnerable-to-computerization/.

[194] Martin Ford, *Will Robots Cause Mass Unemployment in China?*, THE FISCAL TIMES (Aug. 20, 2012), http://www.thefiscaltimes.com/Articles/2012/08/20/Will-Robots-Cause-Mass-Unemployment-in-China (last visited Feb. 12, 2015); Reddit http://www.reddit.com/r/Automate/comments/1uoxnj/can_we_talk_about_the_belief_that_automation_will/.

[195] Kongthon, et al. *supra* note 42; Anderson *supra* note 44; Kevin Macnish, *Unblinking Eyes: The Ethics of Automating Surveillance*, Abstract, 14 ETHICS & INFO. TECH. 51 (2012), *available at* http://link.springer.com/static-content/lookinside/20/art%253A10.1007%252Fs10676-012-9291-0/000.png.

[196] Simone Foxman, *Those Flash Boys: How the "Navy Seals" of Trading are Taking on Wall Street's Predatory Robots*, QUARTZ (Mar. 31, 2014), http://qz.com/138388/how-the-navy-seals-of-trading-are-taking-on-wall-streets-predatory-robots/.

Automated "bots" are used by the same companies that seek to criminalize the behavior by those that visit the companies' sites. Buried as one of Yelp's restrictions on its Terms of Service page is a prohibition on "any robot, spider, site search/retrieval application, or other automated device, process or means to access, retrieve, scrape, or index any portion of the Site or any Site Content."[197] To maintain its competitive edge and ensure it provides a valuable service however, Yelp uses automated bots regularly on its site.[198] There is even a video explaining the automated software, how it was designed, and how it automatically and efficiently seeks out certain posted material for exclusion without human input.[199] The company goes so far as to seek feedback from the public to improve its "bots."[200] As is the natural competitive process, marketing companies have emerged to defeat Yelp's "bots" and avoid its automated filters.[201] Just like any other "bots," defeating Yelp's automated bots can have nefarious intent. The main reason these defeating "bots" are used however, is to preserve legitimate, positive reviews.[202] Nevertheless, the intent is to get around Yelp's "bots." Clearly this behavior is frowned upon by Yelp. No one has sought criminal punishment against Yelp when the site uses its own "bots" to maintain the integrity of its reviews. If, however, these marketing companies used "bots" that were smarter than Yelp's own "bots" to preserve their positive reviews, somehow Yelp would argue it becomes a criminal violation.

As discussed, "bots" are most often used for one of three purposes on third-party websites: buypage encryption; internet protocol blocks; and CAPTCHA code.[203] "Bots" are used in these arenas both for benign and malicious purposes. While some users employ "bots" to illegal ends,

---

[197] *Terms of Service*, YELP INC., http://www.yelp.com/static?p=tos&country=US (last visited Nov. 1, 2014).
[198] *What is Yelp's Recommendation Software*, YELP INC., http://www.yelp-support.com/article/What-is-Yelp-s-recommendation-software?l=en_US (last visited Nov. 1, 2014).
[199] *Id*.
[200] *Id*.
[201] Trevor Sumner, *The Definitive Guide To Avoid The Yelp Review Filter*, LOCALVOX (Apr. 18, 2013), http://localvox.com/blog/how-to-avoid-the-yelp-review-filter-and-get-more-positive-reviews/.
[202] *Id*.
[203] *See, supra* Part III.

others have valid, beneficial reasons. On checkout screens, or buypages, "bots" can be used illegally to extract others' purchasing information, but also legally to access checkout pages and purchase goods efficiently and quickly. Companies that seek to criminalize all bot use do not do it for altruistic reasons, but mainly to limit competition and insulate themselves. Website owners can freely determine what is illegal and what is not at the federal level if the CFAA will blindly enforce any action that may be against the preferences of private website owners and contrary to the private Terms of Service contracts they create with users.

While it has been argued that using a "bot" on a website's buypage is "akin to drilling through the side of a bank vault,"[204] the analogy only holds if the purpose of the drilling is to put more money in the bank. Buypage encryption can be used legitimately by website owners to restrict purchases for certain individuals.[205] When used properly it can help the website owner limit his or her liability.[206] Some websites, however, use it to stop purchases that occur in quick succession, a clear indication of "bot" use. In this regard, the website is stopping valid sales that bring the site more revenue faster. Just as with any "bots," use on buypages can be benign and done to efficiently pay the website or can be done with nefarious intent. The CFAA should be narrow enough to effectively handle the latter without criminalizing the former. Legal "bot" use that is unwanted can be limited through a buypage block, but the access is not unauthorized and thus not illegal. It is up to website owners to keep out who they do not want, not the courts.

Internet protocol (IP) blocks can help website owners to keep "hackers" out and not allow them to damage information,[207] but they cannot be installed to bottleneck certain users or enforce

---

[204] Brief for Plaintiff-United States at 18, United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (No. CRIM. 10-114 KSH).
[205] Brief for Plaintiff-United States at 18, United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (No. CRIM. 10-114 KSH).
[206] *See*, *supra* Part III.
[207] John Gartner, *Verizon's E-Mail Embargo Enrages*, WIRED, (Jan. 10, 2005), http://archive.wired.com/techbiz/media/news/2005/01/66226.

preferences in all situations.[208] If left up to the individual websites to determine legality and that is freely enforced by the CFAA, "IP blocking can have profound impacts on the ability to communicate freely."[209] If any user who gets around an IP block is violating the CFAA, any validly used IP masking tool is a criminal offense. Individual users who want to protect their identity and location and avoid viruses themselves, can hide their IP addresses using a number of tools on the internet,[210] Theoretically then, anyone who hides their IP address should face federal criminal charges. Using a "bot" versus doing it yourself should have no impact on the outcome. Because courts have argued it would be against public policy to hold individuals liable criminally just because a website would prefer they not do something,[211] the fact that they use a "bot" to do the same should be of no importance.

CAPTCHA code, like most other devices employed by websites can serve a valid purpose as protection from illegal uses, but allowing any user navigation that conflicts with website tools like CAPTCHA code to be criminalized by the CFAA is a slippery slope. With CAPTCHA code, unlike buypage encryption or IP blocks, "bots" are the principal targets.[212] CAPTCHA does, however, have numerous uses and effects besides preventing malicious attacks on websites.[213] Website owners can use CAPTCHA code as a way of enforcing their preferences against "bots," but using the federal government through the CFAA to carry out these preferences is reaching too far. Even worse than making those who want to protect their IP addresses criminals, certain disabled people need CAPTCHA defeating software. Criminalizing these "bots" would make any

---

[208] Nate Anderson, *Verizon Proposes Settlement For Class Action Lawsuit*, (Apr. 5, 2006), http://arstechnica.com/uncategorized/2006/04/6525-2/.
[209] Sascha D. Meinrath, James W. Losey & Victor W. Pickard, *Digital Feudalism: Enclosures and Erasures from Digital Rights Management to the Digital Divide*, 19 COMMLAW CONSPECTUS 423, 441–42 (2011).
[210] MASK MY IP, http://www.mask-myip.com/ (last visited Nov. 1, 2014).
[211] Zefer Corp., 318 F.3d at 63.
[212] Brief for Plaintiff-United States at 19, United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (No. CRIM. 10-114 KSH).
[213] Luis von Ahn, *supra* note 67, at 58, 60; *see also supra* Part III.

visually impaired person a potential criminal offender if they use legal software to improve their internet experience.[214]

ii. Automated Bots Do Not Inherently Cause Damage to any Statutorily Protected Computer Nor Presumptively Violate the CFAA

"Bot" use to acquire otherwise public information does not cause the requisite damage to any protected computer. Using terms like "hacking" and "virtual breaking and entering" connotes destruction of property, but persuasive language is not the same as actual damage. While the damage need not be physical destruction of the computer or server, there must be a tangible negative harm to the website or the owner's system. Criminal punishment is not justified by a theoretical, non-quantifiable harm.[215]

While some website owners seeking to enforce their Terms of Service through the CFAA have successfully convinced courts that "bots" damage computer systems,[216] their proof of damage was unpersuasive. Most arguments that "bot" activity causes damage relate to bandwidth, server capacity, and the ability of other users to access the site. Website owners argue that because "bots" can search through data at a much faster rate than individuals they "consume at least a portion of plaintiff's bandwidth and server capacity."[217] The argument is akin to using more than your allotment of a finite resource so there is less for everyone else. Even without evidence that this

---

[214] *Computer Pioneer Aids Spam Fight*, BBC NEWS (Jan. 8, 2003), http://news.bbc.co.uk/2/hi/technology/2635855.stm.; Hannah Alvarez, *Think Your Site Needs CAPTCHA? Try These User-Friendly Alternatives*, USER TESTING (Apr. 9, 2014), http://www.usertesting.com/blog/2014/04/09/think-your-site-needs-captcha-try-these-user-friendly-alternatives/.

[215] *See supra* Part II.

[216] Ebay, Inc. v. Bidder's Edge, 100 F. Supp. 2d 1058, 1071 (N.D. Cal. 2000); Am. Online, Inc. v. Nat'l Health Care Disc., Inc., 174 F. Supp. 2d 890, 899 (N.D. Iowa 2001) (*citing* America Online, Inc. v. National Health Care Discount, Inc., 121 F. Supp. 2d 1255, 1274-75 (N.D. Iowa 2000)).

[217] *Ebay, Inc.*, 100 F. Supp. 2d 1058 at 1071.

actually cost the website owner revenue or customers, the court found the requisite damage.[218] The key distinction for the court was the use of "bots." If a group of people engaged in the same behavior and used the same share of bandwidth it is highly unlikely the website owner would have sought help from the CFAA and the federal courts.

This deference to the website owner's discretion touches on the real reason "bots" are targeted by website owners and as a matter of public policy. They are used primarily by competitors. Website owners have convinced the courts that "bots" are akin to unauthorized hacking in order to prevent competition in a public forum. The real impetus for website owners is not actual harm to their computer systems but protection from increased competition.[219] "Established online merchants have a substantial incentive … to interfere with the flow of price and product information on the Internet."[220]

In many cases, the "bots" do exactly what an individual user would and provide the same economic benefit to a website. In a similar case to Bidder's Edge, ticket resellers were indicted under the CFAA for purchasing bulk event tickets.[221] Ticketmaster doesn't mind if someone buys all of the tickets they sell, considering that is exactly what they are in business to do. But they successfully got a competitor indicted for doing the same thing just because the competitor planned to resell the tickets later for a mark-up.[222] Either way, Ticketmaster sold the tickets they wanted to sell.

In other cases, "bots" pool public information off of websites for use in marketing or other business practices. Courts have allowed CFAA claims to persist even when the information

---

[218] *Id*.
[219] Gailbraith, *supra* note 19, at 333 (*citing* Brief of Amici Curiae in Support of Bidder's Edge, Inc., Appellant, Supporting Reversal, at 6, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000) (No. 00-15995)).
[220] *Id*. (*quoting* Brief of Amici Curiae in Support of Bidder's Edge, Inc., Appellant, Supporting Reversal, at 6, eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d 1058 (N.D. Cal. 2000) (No. 00-15995)).
[221] United States v. Lowson, 2010 U.S. Dist. LEXIS 145647(D.N.J. Oct. 12, 2010).
[222] *Id*.

obtained was public simply because the website owner argued the "bot" impaired the website's capacity to serve the rest of its customers.[223] Congress clearly did not intend the CFAA to be a tool against economic competition and protectionism especially given most legislation in the area of economic activity favors free market competition and penalizes anti-competitive practices.[224]

"Bot" use that goes against a website's terms of service is also not inherently unauthorized or exceeding authorized access. Courts have previously held that contractual restrictions, while they may speak to misappropriation, do not invoke the CFAA."[225] The CFAA is focused on "unauthorized" or "exceeding authorized" access and damage that subsequently arises. Despite the fact that "bots" may use the information provided in a different way, the access is not violated. "Bots" may be at odds with a Terms of Service policy, but may still access a company's website for its intended function and thus is not a CFAA violation.[226] Websites are designed to allow users to accomplish some specific purpose. Especially with public websites that anyone can access and use, "in no sense can [a "bot"] be considered an 'outside hacker.'"[227]

The CFAA does not forbid using a "protected computer" for any prohibited purpose, but only for "unauthorized" or "exceeding authorized" access.[228] Terms of Service do not govern who has authorization to access, which could be more in-line with "access."[229] They may speak to

---

[223] Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 980 (N.D. Cal.2013).
[224] *See, e.g.*, 15 U.S.C. §§ 1–7 (Sherman Antitrust Act prohibited certain business activities that are anticompetitive); 15 U.S.C. §§ 12-27 (Clayton Antitrust Act prohibited specified anticompetitive conduct and established and enforcement mechanism.).
[225] *See e.g.* United States v. Nosal, 676 F.3d 854, 863 (9th Cir. Cal.2012) ("The phrase 'exceeds authorized access' in the CFAA does not extend to violations of use restrictions. If Congress wants to incorporate misappropriation liability into the CFAA, it must speak more clearly."); *See also*, Power Equip. Maint., Inc. v. AIRCO Power Servs., Inc., 953 F. Supp. 2d 1290, 1296 (S.D. Ga. 2013) ("The language of the CFAA simply prohibits accessing information either without authorization or in excess of authorized access. 18 U.S.C. § 1030. It does not confer upon employers the ability to sue their employees in federal court for violations of company policy regarding computer usage.").
[226] Southwest Airlines Co. v. BoardFirst, L.L.C.,2007 U.S. Dist. LEXIS 96230 (N.D. Tex. Sept. 12, 2007).
[227] *Id*.
[228] *Id*.
[229] Craigslist Inc. v. 3Taps Inc., 942 F. Supp. 2d 962, 969 (N.D. Cal. 2013).

measures, but this goes beyond "access" and into topics not under the CFAA.[230] Website owners can limit means of access contractually through Terms of Service, but Congress never intended to criminalize Terms of Service violators under the U.S. Code, and did not incorporate contractual breaches into the design of the CFAA.

Previous CFAA convictions based on Terms of Service breaches often concerned behavior that was independently illegal or touched on public policy concerns. When an individual engaged in cyberbullying that ultimately resulted in a suicide, the jury originally convicted the individual under the CFAA.[231] The court recognized that a website owner should be able to determine the extent that the public can view information on his website. Likewise, the court found that website owners "can relay and impose those limitations/restrictions/conditions by means of written notice such as Terms of Service or use provisions placed on the home page of the website."[232] While this is true, it is an entirely different argument to say that those members of the public who do not abide by the owner's terms go beyond breach of contract and into potential criminal sanctions. The court found that it was conceivable "access" could be limited by Terms of Service based on standard definitions, and other courts have interpreted "access" in this way.[233] Nevertheless, such an interpretation of "access" cannot be used to justify criminal convictions.[234] If a "conscious breach of a website's [T]erms of [S]ervice" is enough to be deemed "access without authorization or in excess of authorization," the law becomes too tenuous and affords too much discretion to law enforcement and too little notice to internet users.[235] Because of the court vacated the jury conviction.[236]

---

[230] *Id*.
[231] United States v. Drew, 259 F.R.D. 449 (C.D. Cal.2009).
[232] *Id*., at 461.
[233] *Id*., at 461.
[234] *Id*. at 467.
[235] *Id*.
[236] *Id*.

Some courts have found the CFAA potentially applicable in cases where the user acted as any individual would in providing business to the website owner, but did so using means against the Terms of Service. In a case involving event ticket resellers, the website owner sought criminal charges when a competitor purchased bulk tickets off the owner's website.[237] Although the case settled prior to any potential conviction, the District Court allowed an indictment to stand despite the fact that the alleged violator purchased tickets, for the same price any user would have and only used "bots" to acquire as many tickets as possible, providing the website owner with income.[238] Although the defendant argued code-based restrictions were basically means for the website owner to enforce its contractual agreement and not grounds for a CFAA claim[239], the court found the CFAA potentially applicable even when the only information obtained was accessible to other users.[240] Interpreting the Drew case, the court found breach of contract claims not necessarily covered by the CFAA, but breach of code-based restrictions more in line with "hacking."[241]

iii. Prosecutorial Discretion Is Not A Valid Means of Controlling The CFAA

Some commenters argue that the district court and jury had the law right in Drew and "theoretically the law fit[] the crime as charged."[242] The argument is that prosecutors did the right thing in favoring a misdemeanor charge as opposed to a felony.[243]

---

[237] United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010).
[238] Brief for Defendant, United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (No. CRIM. 10-114 KSH).
[239] *Id.* at *3
[240] United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010).
[241] *Id.* at *16.
[242] Jones, *supra* note 21.
[243] *Id.*

While prosecutorial discretion can theoretically fill the gap between what is a serious criminal wrong and what is unwanted but, to some, borderline illegal, in practice it provides too much leeway in sentencing and places way too much power in non-legislative government hands. At the same time, if Terms of Service set the parameters for a CFAA violation any time automated programs or "bots" are used, the scope of the government's prosecutorial authority is determined by private parties in how they unilateral draft the terms.[244] CFAA violations based on Terms of Service contracts allow website owners to, in essence, become private attorneys general and control the limits of legal internet use.

Those who believe any "bot" use contrary to a website's Terms of Service can lead to criminal liability may argue the true purpose of the CFAA would be deterrence. The threat of criminal liability, according to some, should be enough to deter individuals who would otherwise employ automated programs to act against a website owner's preferences.[245] It is easy to argue small-time "bot" use will not be punished by the CFAA and prosecutors will seek to only penalize those who operate on a large scale with malicious intent. Theory, however, rarely comports to reality.

While the threat of criminal prosecution may deter individuals from using automated "bots" contravening a website's Terms of Service, it could also lead to an actual criminal prosecution and jail time. Relying on the discretion of private website owners and government prosecutors to set the scope of a federal act is dangerous and unprecedented. What happens when the alleged contract violator meets a prosecutor who wants to set an example or the controversy touches on a political candidate's platform, or hits a nerve with some other individual in power?[246]

---

[244] Brief for Defendant at 13, United States v. Lowson, 2010 WL 9552416 (D.N.J. Oct. 12, 2010) (No. CRIM. 10-114 KSH).

[245] *See* Dodd S. Griffith, The Computer Fraud and Abuse Act of 1986: A Measured Response to A Growing Problem, 43 VAND. L. REV. 453, 455–56 (1990); *See also*, Samantha Jensen, Abusing the Computer Fraud and Abuse Act: Why Broad Interpretations of the CFAA Fail, 36 HAMLINE L. REV. 81 (2013).

[246] David Porter, *Wiseguy Online Ticket Ring BUSTED: Hackers Charged With Running $29 Million Scam*, THE HUFFINGTON POST, (May 2, 2010), http://www.huffingtonpost.com/2010/03/02/wiseguy-tickets-charged-

Aaron Swartz, a computer programmer responsible for building RSS, Reddit, and Creative Commons used his technology based skillset to promote information transparency over the internet.[247] His creations are used daily by millions of people.[248] In late 2010 and early 2011 Swartz allegedly downloaded 4.8 million JSTOR articles from MIT servers, most likely to make the academic research freely available to the public.[249]

There is no debate that what Swartz did was illegal and technically violated the CFAA—the information was not otherwise public, but was password protected. Swartz seemed to recognize this as well, but also knew that MIT promoted freedom of information and the power of collective thought and Swartz believed he "likely wouldn't get in too much trouble,"[250] because the only real damage he caused by making journal articles publicly available was delay in access time for true JSTOR users.

Swartz's belief was wrong and the government abused discretion and decided to use him as an example. Initially, the court issued a blanket protective order keeping Swartz from distributing the documents.[251]

Swartz was indicted on numerous federal charges including multiple violations of the CFAA[252] In an apparent attempt to use Swartz as a sacrificial lamb and discourage future CFAA violations,

---

w_n_481988.html (Operation ignored until New Jersey became involved, possibly because Bruce Springsteen and Bon Jovi, New Jersey locals, were involved.); *White House Won't Take Action Against Aaron Swartz's Prosecutors,* RT, (Jan. 8, 2015), http://rt.com/usa/220967-aaron-swartz-response-watt/ (Thousands of petitioners called for action against prosecutorial misconduct and abuse of discretion that lead to defendant's suicide.).

[247] Marcella Bombadieri, *The Inside Story of MIT and Aaron Swartz*, THE BOSTON GLOBE ONLINE, (Mar. 30, 2014), http://www.bostonglobe.com/metro/2014/03/29/the-inside-story-mit-and-aaron-swartz/YvJZ5P6VHaPJusReuaN7SI/story.html; *see also*, Allison D. Burroughs, Benjamin L. Mack & Heather B. Repicky, When Is Hacking A Crime? Potential Revisions to the CFAA, 58 BOS. B.J. (Page 13) (2014).

[248] *Traffic Statistics*, REDDIT, http://www.reddit.com/r/AskReddit/about/traffic (last visited Nov. 1, 2013).

[249] Bombadieri, *supra* note 247.

[250] *Id*.

[251] United States v. Swartz, 945 F. Supp. 2d 216, 217 (D. Mass. 2013).

[252] Indictment of Aaron Swartz, United States v. Swartz, 945 F. Supp. 2d 216 (D. Mass. Sept. 12, 2012) (No. 11-CR-10260-NMG), *available at* http://ia700504.us.archive.org/29/items/gov.uscourts.mad.137971/gov.uscourts.mad.137971.53.0.pdf.

the US Attorney indicted Swartz on charges that carried a potential 35 years in prison and a $1 million fine.[253] Rather than face criminal prosecution and serious prison time, Swartz committed suicide in January 2013.[254]

Political figures and members of the public recognized the danger in leaving so much discretion to prosecutors. Even a prominent US Senator who endorsed the CFAA and argued digital theft is still theft questioned the US Attorney's conduct.[255] Senator John Cornyn wrote to Attorney General Eric Holder, questioning the prosecutorial misconduct surrounding the Aaron Swartz case.[256] Cornyn questioned the proportionality of the conduct to the penalty and the retaliatory motives of the prosecution.[257] To prevent a similar a similar situation and alleviate any fears for prosecutorial abuse, Aaron's Law was proposed.[258] Unfortunately the law has stalled and there remains the fear that prosecutors can arbitrarily enforce the CFAA how they please.

Prosecutorial discretion is also a problem because of the duplicative nature of the statute. By using redundant terms, the CFAA punishes one act multiple times.[259] A prosecutor can easily stack charges on an individual, threatening them with serious jail time.[260] This leverage can pressure a violator to accept a deal and plea to one charge, thinking it is their best alternative given the situation.[261] This bullying tactic can be abused both at trial and sentencing to severely punish

---

[253] Burroughs et al., *supra* note 247.
[254] Bombadieri, *supra* note 247.
[255] Colleen Taylor, *Senator John Cornyn Wants Answers: Did U.S. Attorney Carmen Ortiz Aim To 'Make An Example' Of Aaron Swartz?*, TECHCRUNCH, (Jan. 19, 2013), http://techcrunch.com/2013/01/19/sen-john-cornyn-asks-attorney-general-eric-holder-did-carmen-ortiz-aim-to-make-an-example-of-aaron-swartz/.
[256] Letter from John Cornyn, Senator, United States Senate, to Eric Holder, Attorney General, United States Department of Justice (Jan. 18, 2013), *available at* http://www.cornyn.senate.gov/public/?a=Files.Serve&File_id=74c0afb3-1bc2-49f5-9150-0a8f004ef438.
[257] *Id*.
[258] Aaron's Law Act of 2013, H.R. 2454, 113th Cong. (1st Sess. 2013).
[259] *Id*. at § 3.
[260] Zoe Lofgren and Ron Wyden, *Introducing Aaron's Law, a Desperately Needed Reform of the Computer Fraud and Abuse Act*, WIRED (June 20, 2013 9:30 AM), http://www.wired.com/2013/06/aarons-law-is-finally-here/.
[261] *Id*.

individuals who may commit minor infractions given the language of the statute.[262] Unfortunately, it can also lead to suicide when the threats become too real and an unknowing violator is backed into a corner.[263]

At the same time, if a fear of prosecutorial abuse were not troublesome enough under the current CFAA structure, the Obama administration has called for stronger CFAA penalties, which would tip further towards possible abuses of discretion.[264] The Obama administration has altered its stance numerous times over the previous few years, but consistently favors increasing penalties for most "bot" or code-based actions.[265] While the proposal aims to ensure "that insignificant conduct does not fall within the scope of the statute," and supposedly focuses more on prosecuting "insiders who abuse their ability to access information to use it for their own purposes," some of the proposed text would still increase "bot" penalties and leave much to discretion.[266] The original proposed criminal provisions, and those still currently proposed, would add a mandatory three-year minimum penalty for damaging certain computers.[267] Most criminal violations of the CFAA would have increased potential penalties under the Obama administration's proposal.[268] The newest proposal for the CFAA would expand on the definition of "exceeds authorized access" and encompass uses that the accesser knows the computer owner would not want.[269]

---

[262] *Id*.
[263] *Id*.
[264] CONGRESSIONAL RESEARCH SERVICE, THE OBAMA ADMINISTRATION'S CYBERSECURITY PROPOSAL: CRIMINAL PROVISIONS (July 2011), *available at* http://fas.org/sgp/crs/misc/R41941.pdf. [hereinafter OBAMA CYBERSECURITY PROPOSAL]; UPDATED ADMINISTRATION PROPOSAL: LAW ENFORCEMENT PROVISIONS, *available at* http://www.whitehouse.gov/sites/default/files/omb/legislative/letters/updated-law-enforcement-tools.pdf.
[265] Orin Kerr, *Obama's proposed changes to the computer hacking statute: A deep dive,* THE VOLOKH CONSPIRACY (Jan. 14, 2015), http://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/01/14/obamas-proposed-changes-to-the-computer-hacking-statute-a-deep-dive/.
[266] Press Release, The White House Office of the Press Secretary, SECURING CYBERSPACE - President Obama Announces New Cybersecurity Legislative Proposal and Other Cybersecurity Efforts (Jan. 13, 2015) (*available at* http://www.whitehouse.gov/the-press-office/2015/01/13/securing-cyberspace-president-obama-announces-new-cybersecurity-legislat).
[267] OBAMA CYBERSECURITY PROPOSAL, *supra* note 264; UPDATED ADMINISTRATION PROPOSAL, *supra* note 264.
[268] OBAMA CYBERSECURITY PROPOSAL, *supra* note 264.
[269] UPDATED ADMINISTRATION PROPOSAL, *supra* note 264.

Leaning towards the opposite end of the spectrum, the justice department acknowledged the potential for abuse and inferred it was open to shoring up some ambiguity.[270] The justice department recommended congressional action to amend the CFAA and make it more difficult for the government to prosecute less serious statutory violations.[271]

VI. Conclusion

The Computer Fraud and Abuse Act (CFAA) is a useful tool to limit theft and damage to digital information, but courts and prosecutors have arbitrarily enforced and overextended it.[272] It has been stretched beyond what Congress intended, to include actions that cannot legitimately be deemed criminal. Prosecutors will have no reason to focus their energy on truly harmful criminal behavior if courts continue to construe the CFAA more and more broadly, and encroach on rulemaking themselves.[273]

When Congress first created the CFAA and some state legislatures followed suit with related state statutes, no one had any idea that there would be something like the global Internet, much less "bots" that would be mining data on such a huge scale. "Bots," just like any technology, can be encouraged and used in a positive way or exploited and misused. They are not inherently bad, but in fact can lead to tremendous advances. The CFAA was designed to be flexible and adapt to future technology and innovation, but it has proven unable to keep pace. It is really a case of a

[270] Brian Fung, *The Justice Department Used This Law to Pursue Aaron Swartz. Now It's Open to Reforming It*, THE WASHINGTON POST ONLINE, (Feb. 7, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/02/07/the-justice-department-used-this-law-to-pursue-aaron-swartz-now-its-open-to-reforming-it/.
[271] *Id*.
[272] *See*, *supra* Part II.
[273] *See*, Kerr, *supra* note 5.

statute that has been left in the dust by technology. The answer to this problem is legislation, not judicial or prosecutorial interpretation and expansion.