An Exploration Into an Outdated and Vague CFAA

Ethical hacking is defined as the authorized attempt to gain access to computer systems, applications or data by duplicating the strategies and methods that would be used by a malicious hacker. Usually, this is conducted for the explicit goal of exposing vulnerabilities in applications before they are exploited by a more malicious party for their own personal gain or for more sinister purposes. Those whose systems are being tested and exploited often seek punishment and prosecute the adversary under the law of the United States. The most cited law in these cases, and a hugely controversial law is the Computer Fraud and Abuse Act. This statute was enacted in 1986 and was put into effect with the goal of prohibiting unauthorized access to a protected computer without authorization and to enforce strong internet security. However, it seems that this law is largely outdated being that it was last amended in 2008, ineffective in the standards of modern society, and actually causes much more harm than good. Those that find themselves prosecuted under this law often face harsh penalties for minor infractions. By imposing such harsh repercussions, it discourages the thorough testing of internet applications, and allows companies to continue to employ lax information security despite the numerous large scale data breaches that have affected the American public en masse. In order to combat this issue, the CFAA must be amended to better fit today's definition of good information security. To find an effective solution to this issue, one must thoroughly examine the diction of the CFAA. One instance in particular is the definition of a "protected computer," which as of now extends to practically all computers in use to reduce the coverage of this law. Another modification that should be made is to make the provisions in the CFAA less vague. This can help those that are treading a "gray" area understand the boundaries of where they operate. The benefits of having an improved CFAA is immense. In addition to better security in the computing ecosystem, companies will be held accountable for lax internet security, rather than the public and internet

do-gooders if a data breach occurs. By removing the legal basis to prosecute those that hack with moral intentions, a system can be thoroughly battle-tested before a larger-scale cyber attack by a more malicious party can occur.

Hackers can be grouped into three different categories in terms of morality. Taking inspiration from the common trope in cliche western movies, white hat hackers conduct their work for the benefit of society and its internet security while staying within the bounds of the law. On the other side of the spectrum, black hat hackers use illegal means to gain access to computer systems for malicious and unethical purposes. Grey hat hackers fall somewhere in the middle of the latter and the former meaning that they employ illegal means but for a moral purpose.

Disregarding the intentions and goals of a hacker, if they are caught they often face prosecution and harsh punishment under the enormous jurisdiction of the Computer Fraud and Abuse Act. The Computer Fraud and Abuse Act (CFAA) in short was enacted in 1986 following a viewing of the science fiction film WarGames at Camp David by then president, Ronald Reagan. The purpose of the enactment of this law was to prohibit a variety of conduct regarding computers. (Berris) However, given the context of the political atmosphere in the United States at the time, it can largely be seen as a political statute that was designed to mostly protect the government and its American financial institutions from its adversaries, domestic and foreign. (Curtiss)

A common criticism of the CFAA is that it is extremely outdated and that its vagueness leaves much to the interpretation of the court. This criticism is not unfounded; the CFAA's vague diction means that it is extraordinarily difficult for courts to interpret and apply the needed nuance to cases in the modern day. One of the often criticized terms within the CFAA is the term,

“protected computer.” As it stands right now, a “protected computer” at a very high level refers to a computer that is used for a financial institution or the United States government exclusively, or a computer that is used in or has the potential to affect interstate or foreign commerce or communication. Almost all computers in use have some capacity to communicate and interact with foreign countries and especially between states in the United States. Software and services for modern purposes are mostly distributed through protected servers owned by private and public entities, large and small, which means that the CFAA has jurisdiction over almost every meaningful computer in use. (Curtiss) Therefore the CFAA criminalizes and creates liability for those that “intentionally accesses a computer without authorization or exceeds authorized access, and thereby obtains … information from any protected computer.” (Cornell Law)

The CFAA is often said to have exceeded the jurisdiction needed to effectively achieve the goals that it was meant to achieve, and has extended its reach beyond reason. Courts are split on how to interpret this statute; There are two sides to the argument, one side favors the “broad approach,” and one side favors the “narrow approach.” (Kane) Those that favor the broad approach, hold the belief “that an individual has been granted general permission to access a computer does not necessarily insulate him from CFAA unauthorized access liability.” (Kane) On the other hand, those that have adopted the narrow approach believe that “unauthorized access occurs only when an individual accesses a computer that he does not have permission to access.” This, in other words means that the accesser’s purpose does not matter. (Kane)

Proponents who support the CFAA in its current state, say that there is a reason for its flexibility and broad jurisdiction, specifically in order to protect American national security interests. (Curtiss) Those that do not support the CFAA as it is, believe that the CFAA is much too restrictive and vague to be effective in deterring cyber crime.

Unfortunately, due to the very nature and purpose of the law and the probable inexperience of lawmakers concerning hacking, this means that often, the law does not have the general public's best interests at heart nor is it probably the optimal solution to preventing malicious hacking. As seen above, it is blatantly obvious that the CFAA is not made with the public's best interest at heart, rather, it seems that it was created with the intent of shielding the United States government and important American infrastructure from national security threats. The CFAA is also kept intentionally vague in order to cast as wide of a legal net as possible. However, it has the side effect of using the American people as collateral, and shielding large corporations from taking responsibility for poor cybersecurity and shifting the blame to and prosecuting "bad actors" when their systems are inevitably hacked and exploited by a third party.

The vagueness of the CFAA was a controversial topic discussed in the legal case, United States v. Nosal. In October 2004, David Nosal left his job at Korn/Ferry International (KFI) in order to start a rival firm. Shortly after doing so, he asked former colleagues to use their login credentials to download confidential KFI information which was in violation of the CFAA. Nosal and colleagues were charged with "exceeding their authorized access' with intent to defraud." In a contentious court battle, Nosal's charges were eventually dismissed as he argued that the Ninth Circuit precedent preclude the CFAA's application to individual' "misuse [of] information they obtain by means of [authorized] access." (Harvard Law Review) However, the effect of this case was that the court found the CFAA text ambiguous and too broad to be interpreted effectively.

Law experts also agree that the jurisdiction of the CFAA is much too broad to be a fair policy. To quote former Attorney General and U.S Attorney for Rhode Island Sheldon Whitehouse, "How many Americans have shared an account password with a family member? Or have provided an inaccurate phone number when opening an account to avoid marketing

calls? Or have shaved a few digits off their age or weight when registering with a dating website? All of these mundane acts would constitute violations of terms of service agreements." He continues by saying "[a] law that criminalizes the conduct of virtually every American, and then allows prosecutors to pick and choose which targets are worthy of jail time, is simply bad policy." (Whitehouse)

In order to implement an effective solution to remediate the numerous issues of the CFAA, and to shift the focus of the CFAA to one that benefits the people of the United States instead of national infrastructure, examining the diction will be crucial. Particularly, focusing on the modification of the definition of a "protected computer" is a must. Another term that also needs to be updated is that of what exactly "exceeding authorized access" means and the modifications that must be made to prevent the misuse of this clause. Finally, another change that can have monumental effects is to hold companies criminally accountable, should they exercise poor judgment and lax response to data breaches and hacks.

The jurisdiction of a protected computer as it stands in the present day is far too vast for the public to possibly benefit from. Since the CFAA has jurisdiction over practically every practical computer, it is essential for ethical hacking that this be reigned back. To do this, the diction of what a protected computer is, and on the contrary, is not, must be changed. They can be changed in the following way. A protected computer is a computer "exclusively for the use of a financial institution or the United States government" or "which is used in or affecting interstate or foreign commerce or communication." The first clause is fine, in order to preserve national security interests, but the second clause should be omitted in its entirety. This will cut down the reach of this law significantly, as it no longer applies and holds power over most computers in existence. The intent of this change is to make it so internet activities such as

actively testing systems which may have previously been illegal, legal as now the computer that they are attacking is not governed under the CFAA.

The clause “Access a computer with authorization and to use such access to obtain or alter information in the computer that the accessor is not entitled to obtain or alter” should be changed to accessing a computer with authorization and to use such access to obtain or alter information in a malicious manner in the computer that the accessor is explicitly not entitled to obtain or alter. The intent of this modification is to force companies to be explicit about what is, and what is not authorized for an employee to access. If an employee discovers a flaw in the company’s systems, then they are obligated to report it to the company. If they fail to do so, then and only then, should they be prosecuted. This will prevent companies from retaliating and prosecuting those with good intentions. If they are able to access sensitive information that has not been explicitly forbidden or properly secured, then that is a massive security risk for the general public, especially if the information is somewhat sensitive. The company should be held liable for poor security infrastructure, not the individual.

The last change that I propose is to have some sort of mechanism in place to hold companies liable for inaction or poor security of people’s information as is alluded to above. Specifically, if the company is slow or doesn’t make a good faith attempt to immediately remediate a data breach. The clause I propose is to hold executives criminally responsible with the threat of considerable jail time, if there isn’t sufficient remediation immediately in the aftermath of a data breach or there is an extensive history of gross negligence regarding information security. It is difficult to completely prevent the actions of black hat hackers, and it is nigh impossible to account for every single possible vulnerability. However, it is not impossible for strong damage control, and a strong response should a situation inevitably arise.

Regarding the proposed solutions, there are a multitude of reasons it may have a beneficial effect. A better definition to what a protected computer is has long been needed and this will return the law to what it should have been in the beginning, which is benefitting the individual people of the United States, rather than the government. Time and time again, society has seen misguided laws such as those that impose harsh penalties on minor drug offenses, which hurt and ruin the future of the very individuals they are meant to protect. Only when punishments and the guidelines of what constitutes a drug offense become more lenient, has the negative effects slowed down. (Ashtiani) How the CFAA stands right now is no different.

Changing the definition of the term "exceeds authorized access" can have the effect of forcing companies to be especially careful about their information security infrastructure. Many times, CFAA cases have argued over the meaning of "exceeds authorized access" and their decisions are based on how an individual court interprets the statute. By changing the definition of "exceeding authorized access" to the proposed solution, the onus is explicitly placed on the company, as they cannot claim that an employee accessed somewhere they were not authorized, if it was never explicitly said that it was not authorized. Therefore, if an employee discovers that there is extremely weak security in a system, they will not be afraid to speak out to mitigate the situation and protect the information of users.

The third clause will be a strong motivator for action following a data breach. Society has seen companies drag their feet far too often when it comes to information security, whether it is from just sheer laziness or from a fiscal viewpoint. Despite the multitudes of fines that a company is hit with following a data breach, it does not seem sufficient enough a motivator, because the fines are often laughable in comparison to what the company is worth. Take for example the Meta data breach in April 2021. They were fined only $276 million in a data breach

that exposed the data of more than 533 million users.(The Verge) This is close to nothing when taking into account the worth of Meta as a company. By holding individuals criminally liable for the consequences of a data breach, we can prevent and mitigate the effects because now there will be a real consequence to the individuals in charge.

In order to make sure these changes can actually happen and have any sort of effect, society must be better informed of what hacking actually is. Instead of using hacking as an umbrella term for computer crimes, society must have a more nuanced take on the matter, taking the numerous benefits and potential consequences into account. This can be achieved through the funding and implementation of more computer literacy courses in a world where computers dominate. It can also be achieved by portraying hacking in media with a better light and understanding of what is going on behind the scenes. If society continues to demonize hacking, then there will never be change on this matter. When societal views on hacking change, then it will be up to the lawmakers and computer activists to implement this change.

Consequences

The consequences of maintaining the archaic CFAA also does not bode well for society. Not only is the law hilariously outdated by today's standards in legislation and technology, it has been used as a weapon to ruin the lives of those who are unfortunately found guilty under it even for a relatively minor crime. One only needs to look at the story of Aaron Swartz, cofounder of Reddit and programming genius. Swartz was charged and indicted in the year 2011 for "allegedly attempting to download all of the electronically archived materials maintained by JSTOR while accessing them through a computer network operated by the Massachusetts Institute of Technology." (Curtiss) Facing up to 35 years in prison, he opted to commit suicide instead. Many believed that Swartz was trying to make research materials free and available to

the general public. If the CFAA were to be amended before his passing (Add how solution would help)

By amending the CFAA, we can help clear the names of individuals who have been unfairly charged and prosecuted under the CFAA. Society has an overwhelmingly negative view on hackers. Media produced regarding this topic have consistently portrayed hackers, no matter their morality as criminals. If the CFAA is changed in the near future, we can help remove the negative stigma toward hackers by removing the brand of criminal, and replacing the title with the victim of poor legislation.

Not only can we obtain justice for those that have suffered already under the CFAA, a modified version of the CFAA can prevent data breaches in the future. Take for example the Ashley Madison hack of 2015. Ashley Madison is a website that arranges extramarital liaisons, so it is obvious that user privacy is extremely sensitive in nature. Ethics regarding the service aside, after thousands of users and their information were exposed online in a hack, divorces, public shamings, and even suicides resulted as a part of this scandal. (M2 Presswire) Poor information security leads to serious consequences for those that are affected. By holding companies and their executives accountable for gross negligence, then perhaps society will see less case studies like this one.

There are hefty monetary implications of an unaltered CFAA. The Ponemon institute which is an organization dedicated to studying information security/privacy and its education has estimated that the average cost of a data breach to be $3.86 million dollars. (Nicholson) This includes the cost of a company's lost revenues, regulatory fines, and damage control following a data breach.

This doesn't take into account the reputational damage that a firm may occur as a result of a massive compromise of user data. Take for example, the infamous Yahoo data breach in the time period of 2013-2016. Not only were the fines and class action lawsuits many and enormous; $35 million dollars and 41 lawsuits filed respectively (UpGuard), Yahoo essentially lost all of its trust and goodwill with its users. Today, only around 3% of users on the internet use Yahoo, and it also holds the record for most compromised data records worldwide. (Statista) In conjunction with other poor business practices and decisions, the company's value fell from more than $125 billion during their dotcom bubble peaks, to a measly $4.48 billion when they were finally acquired by Verizon. (Axios) In lieu of this massive scandal, this almost torpedoed an acquisition by Verizon and caused Verizon to lower their initial offer by $350 million dollars. At the end, it was revealed that nearly 3 billion users were affected by this data breach that exposed names, email addresses, phone numbers, birthdates, and passwords just to name a few. (Ny Times)

Considering that we as individuals have the ability to obtain most of the world's information at the click of a button, it is exceedingly easy to learn information about any system. This is a double edged sword. Although this has negative implications for black hat hackers, those that fall into the categories of white hat hacking, and gray hat hacking are able to find and weed out any weaknesses and flaws in network security. (UI Haq) As it stands, ethical hackers often use the same techniques and technology (Nmap and Acunetix) as black hat hackers; it is a matter of morality rather than strategy. Therefore, it is of utmost importance that white hat hackers and gray hat hackers have the ability to conduct their penetration testing unimpeded and away from the confines of the CFAA to conduct their operations unimpeded.

Should the above solutions be implemented, the benefits of a better and more just CFAA has limitless potential. As cybersecurity expert Keren Elazari puts it, "hacking is our internet's

immune system." (Elazari) While there may be some unwanted side effects, the long term benefits for society outweigh the short term consequences. By providing increased leeway for white hat and gray hat hackers, they may be able to detect and expose vulnerabilities before a more malicious party is able to exploit it. Through the removal of potentially extreme and unjust prosecution and perhaps a monetary award through bug bounty programs, talented individuals in the hacking community may be more motivated to attempt to gain access to systems through previously illegal means and snuff out any potential vulnerabilities before they are exploited.

This in turn ensures the safety of online users and their personal information and ensures that the general public are not the collateral in a data breach when it inevitably occurs in a system that has poor cybersecurity. Many companies already employ some type of bug bounty system that have 'safe harbor' policies in place. By further expanding the scope of what is allowed rather than what is not allowed in penetration testing, we can further ensure better vetted systems.

By enacting the proposed changes of modifying the terms "protected computer" and "exceeds authorized access," there will be less prosecutions under the CFAA. Inducing criminal liability for inaction and negligent actions by companies will also serve to protect the American people from data breaches that have serious, real world consequences on our collective well beings.

There is much else that can be done to make the CFAA more just and fair. There are plenty of other scenarios and poor clauses that have not been accounted for under the proposed solution. There also may be unintended consequences from enacting legislation that has not been tried before. Society should continue to monitor and adjust the CFAA as needed, and implement solutions that benefit humanity.

Works Cited

"Ashley Madison Hacking Scandal 1 Year Later; ProfileDefenders.Com Helps Victims of the Ashley Madison Hack with their Reputation Management Services." *M2 Presswire,* Aug 08 2016, *ProQuest.* Web. 11 Nov. 2023

Ashtiani, M. (2021). The Racially Disparate Effects of Drug Arrest on High School Dropout. Socius, 7. https://doi.org/10.1177/23780231211027097

Berris, Peter G. *Cybercrime and the Law: Computer Fraud and Abuse Act (CFAA) and the 116th Congress*. , . *HeinOnline*, https://heinonline-org.ezproxy.bu.edu/HOL/P?h=hein.crs/govdbyt0001&i=2.

“Biggest Data Breaches in US History [Updated 2023]: Upguard.” *RSS*, www.upguard.com/blog/biggest-data-breaches-us. Accessed 12 Nov. 2023.

Coffin, Abbey P. "Cyber law - dismissing employer's claim under the CFAA against former employees who allegedly misappropriated trade secrets." *Suffolk University Law Review*, vol. 46, no. 4, fall 2013, pp. 1261+. *Gale OneFile: LegalTrac*, link.gale.com/apps/doc/A362350601/LT?u=nellco_bpll&sid=bookmark-LT&xid=be6f349b. Accessed 1 Nov. 2023.

"Court Tackles Meaning of 'Authorization' in CFAA." *Telecommunications Reports* 82.1 (2016): 17. *ProQuest.* Web. 1 Nov. 2023.

“Definition: Protected Computer from 18 USC § 1030(e)(2) | LII / Legal Information Institute.” *Legal Information Institute*, Legal Information Institute, www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=18-USC-695191731-692694672&term_occur=999&term_src=title%3A18%3Apart%3AI%3Achapter%3A47%3Asection%3A1030. Accessed 12 Nov. 2023.

“Definition: Exceeds Authorized Access from 18 USC § 1030(e)(6) | LII / Legal Information Institute.” *Legal Information Institute*, Legal Information Institute, www.law.cornell.edu/definitions/uscode.php?width=840&height=800&iframe=true&def_id=18-USC-1178319080-692694676&term_occur=999&term_src=title%3A18%3Apart%3AI%3Achapter%3A47%3Asection%3A1030. Accessed 12 Nov. 2023.

Eichten, Molly. "The Computer Fraud and Abuse Act - a survey of recent cases." *Business Lawyer*, vol. 66, no. 1, Nov. 2010, pp. 231+. *Gale OneFile: LegalTrac*, link.gale.com/apps/doc/A245805791/LT?u=nellco_bpll&sid=bookmark-LT&xid=477c81de. Accessed 30 Oct. 2023.

Elazari, Keren. “Hackers: The Internet’s Immune System.” *Keren Elazari: Hackers: The Internet’s Immune System | TED Talk*, www.ted.com/talks/keren_elazari_hackers_the_internet_s_immune_system?language=en. Accessed 12 Nov. 2023.

Simmons, Ric. "The Failure of the Computer Fraud and Abuse Act: Time to Take an Administrative Approach to Regulating Computer Crime." *George Washington Law Review,* vol. 84, no. 6, December 2016, pp. 1703-1724. *HeinOnline*, https://heinonline-org.ezproxy.bu.edu/HOL/P?h=hein.journals/gwlr84&i=1788.

Kane, Samuel. "Available, Granted, Revoked: A New Framework for Assessing Unauthorized Access Under the Computer Fraud and Abuse Act." *The University of Chicago Law Review* 87.5 (2020): 1437-77. *ProQuest.* Web. 12 Nov. 2023.

Nakhjavan, Alicia. "The "Worst Law in Technology": How the Computer Fraud and Abuse Act Allows Big Businesses to Collect and Sell Your Personal Information." *Brooklyn Law Review,* vol. 87, no. 3, Spring 2022, pp. 1077-[ii]. *HeinOnline*,

Curtiss, Tiffany. "Computer Fraud and Abuse Act enforcement: cruel, unusual, and due for reform." *Washington Law Review*, vol. 91, no. 4, Dec. 2016, pp. 1813+. *Gale Academic OneFile*, link.gale.com/apps/doc/A481518718/AONE?u=mlin_b_bumml&sid=bookmark-AONE&xid=506e7b46. Accessed 30 Oct. 2023.

Nicholson, Scott. *How Ethical Hacking Can Protect Organisations from a Greater Threat, Computer Fraud & Security, Volume 2019, Issue 5, 2019, Pages 15-19, ISSN 1361-3723*, www.sciencedirect.com/science/article/pii/S1361372319300545. Accessed 12 Nov. 2023.

Perlroth, Nicole. “All 3 Billion Yahoo Accounts Were Affected by 2013 Attack.” *The New York Times*, The New York Times, 3 Oct. 2017, www.nytimes.com/2017/10/03/technology/yahoo-hack-3-billion-users.html.

Samantha Jensen*. "ARTICLE: ABUSING THE COMPUTER FRAUD AND ABUSE ACT: WHY BROAD INTERPRETATIONS OF THE CFAA FAIL." *Hamline Law Review,* 36, 81 2012 / 2013. advance-lexis-com.ezproxy.bu.edu/api/document?collection=analytical-materials&id=urn:contentItem:58PR-9MT0-00CV-R0FT-00000-00&context=1516831. Accessed November 1, 2023.

Ul Haq, H. B., M. Hassan, M. Hussain, R. Khan, S. Nawaz, H. Khokhar, and M. Arshad. “The Impacts of Ethical Hacking and Its Security Mechanisms”. *Pakistan Journal of Engineering and Technology*, Vol. 5, no. 4, Dec. 2022, pp. 29-35, doi:10.51846/vol5iss4pp29-35.

"The vagaries of vagueness: rethinking the CFAA as a problem of private nondelegation." *Harvard Law Review*, vol. 127, no. 2, Dec. 2013, pp. 751+. *Gale OneFile: LegalTrac*, link.gale.com/apps/doc/A355249039/LT?u=nellco_bpll&sid=bookmark-LT&xid=d21884dd. Accessed 11 Nov. 2023.

Trevor A. Thompson*. "Comment: Terrorizing the Technological Neighborhood Watch: The Alienation and Deterrence of the "White Hats" Under the CFAA." *Florida State University Law Review,* 36, 537 Spring, 2009. advance-lexis-com.ezproxy.bu.edu/api/document?collection=analytical-materials&id=urn:contentItem:4XMM-7Y90-00CW-100Y-00000-00&context=1516831. Accessed November 1, 2023.

Whitehouse, Sheldon. *Hacking into the Computer Fraud and Abuse Act: The CFAA at 30: Keynote*, George Washington Law Review. Accessed 12 Nov. 2023.

Why Verizon Sold AOL and Yahoo for about 1% of Their Peak Valuation - Axios, www.axios.com/2021/05/04/verizon-aol-yahoo-valuations. Accessed 12 Nov. 2023.