Computer Fraud and Abuse Act of 1986

Kenisha Sands, Samijo Grant and Monica Molina

GBA 327

4/10/2019

In 1986, just a short 5 years after the first laptop was invented, a computer law called The Computer Fraud and Abuse Act (CFAA) was created with the purposed of protecting and securing computers (18 U.S. Code § 1030 - Fraud and related activity in connection with computers). This act was enacted with the intention of "reducing the hacking and cracking of government or other sensitive institutional computer systems" (Computer Fraud and Abuse Act), which is known today to be a true problem and has led the United States to regularly work on improving the security of its computer systems. The law prohibits accessing a computer without proper authorization, and if violated can lead to fines or imprisonment for the parties involved. Prior to the act computer crimes were prosecuted as mail and wire fraud, but the applying law was often insufficient even with the risk of punishment, so it has led to amends in years following because of improved technology. The CFAA has proven to be the initiation of more protection of security. (Computer Fraud and Abuse Act)

The Computer Fraud and Abuse Act was first implemented to ensure that computer frameworks by the U.S. government and some budgetary foundations were protected. The act is now being utilized all around comprehensively by the administration to accuse programmers, yet also by private organizations to help protect exchange insider facts and other restrictive data. The goal of the Computer Fraud and Abuse Act is to preclude taking or trading off information about national protection, foreign relations, nuclear vitality, or other confined data. This has resulted in increased unapproved access to computers possessed by any office or bureau of the U.S. government. Hence criminal offenses under the act stem from accessing information from banks or other monetary foundations, Intercepting or generally barging in on correspondence between conditions of outside nations, taking steps to harm computer frameworks to blackmail cash or different assets from people, organizations, or establishments. The original 1986 act was enacted

in response to concern that computer-related crimes might go unpunished. Over the years the act has continued to be amended to refine the definitions and to expand coverage in other aspects of cybercrime. Between 1988 and 2008, the law was amended nine times and update to include: protection to financial institutions and other private computers, civil actions under the auspices of the act, tampering and attempted extortion, taking information off systems and the expansion of types of predicate offenses for enhanced penalties

However, although the Computer Fraud and Abuse Act was enacted to protect and secure computers, the act has created much controversy. For example, the shocking passing of Internet extremist Aaron Swartz, who murdered himself amid arraignment for downloading 4.8 million academic articles from JSTOR (Goldman). This has put the Computer Fraud and Abuse Act under serious open investigation. The law was the reason for 11 of the 13 crime accusations against Swartz, who confronted over three decades in jail and a potential $1 million fine for his activities. A portion of these CFAA-related charges in part comes from the way that Swartz abused JSTOR's Terms of Service (Computer Fraud and Abuse Act Reform).

In addition, the CFAA is that it is said to have been motioned due to the movie War Games, a movie about a young adult who hacks into the “War Operation Plan Response system” (Wydeven) and starts a World War III. Despite this being a fictional occurrence, it is said that President Ronald Reagan, the current President at that time, asked the “chairman of the Joint Chiefs of Staff” (Wydeven) if that could actually happen, and he replied yes, so the administration of President Reagan “demanded legislation” (Wydeven) for this matter, and that is when the CFAA was introduced (Wydeven).

On the other hand, to put the CFAA into perspective, the term hacker hasn't generally been the negative title that it is today. A hacker initially portrayed an individual with a longing to find

out about innovation and investigation and who was, in fact, capable with whatever frameworks they hacked. Then again alluded to as cybercrime, e-wrongdoing, electronic wrongdoing, or hey tech wrongdoing. Cybercrimes are any wrongdoings that include a computer and a system. Now and again, the computer may have been utilized to perpetuate the wrongdoing, and in different cases, the computer may have been the objective of the wrongdoing. The U.S. Branch of Justice (DOJ), in its manual on computer wrongdoing, characterizes such wrongdoing as "any infringement of criminal law that includes learning of computer innovation for their execution, examination, or arraignment." Hence Computer wrongdoing is a demonstration performed by a proficient computer client, occasionally alluded to as a programmer that illicitly peruses or takes an organization's or person's private data. Now and again, this individual or gathering of people might be damaging and crush or generally degenerate the PC or information documents.

A lot of this broadness is because of the way that the CFAA precludes anybody from getting to a PC "without approval" or by "surpassing approved access" for specific purposes, which incorporates endeavors to "acquire data" from a "secured PC" if doing as such incorporates "interstate or outside … correspondence". Presently, this presumably seems like a group of lawful blather. However, it is a lawful blather that could influence any individual who the Web. "Without approval" while the CFAA does unequivocally characterize what a PC is ("an electronic, attractive, optical, electrochemical, or other fast information preparing gadget performing legitimate, number-crunching, or capacity works, and incorporates any information storeroom or interchanges office straightforwardly identified with or working related to such gadget, however such term does exclude a computerized or typesetter, a versatile handheld adding machine, or another comparative gadget"), it doesn't characterize what "approval" signifies. What's more, that is a major issue; along these lines, investigators can translate this to imply that infringement of a site's

Terms of Service are equivalent to getting to that site's PCs "without approval." "Get data" could be defined as a lot of things, from downloading top-mystery atomic dispatch codes to stacking a Web page. Also, this legalese could be utilized to contend that somebody has disregarded the CFAA and has along these lines submitted a lawful offense. "Interstate or remote correspondence" One is very likely captivating in "interstate or outside correspondence" by perusing everything that I have expressed in this paper. At the end of the day, utilizing the Internet is, nearly by definition, "interstate or outside correspondence" with a PC. A "Secured PC" under the CFAA is any PC that is associated with an administration arrange or is utilized for "interstate or outside trade or correspondence." So, if the PC is associated with the Internet, it is "ensured."

Generally, the CFAA can be said to have multiple setbacks. These include its vagueness, its criminalization of everyday activities, and its great penalties. In terms of its vagueness, there is much left to interpretation in the word *authorization*, as the definition of authorization is not clear. Also talking about “protected computers” (O’Driscoll), with the description of, “computers used in or affecting interstate or foreign commerce and computers used by the federal government and financial institutions” (O’Driscoll), and every computer can fall under one of the aforementioned categories, making the list of “protected computers” (O’Driscoll) broad. Including that of the phrase, “obtaining information” (O’Driscoll), which could really mean anything depending on the interpretation. Because of the reason that it is so vague and could be interpreted in many different ways, then it could be said that everyday actions by computer users could be considered breaking the law, like for example using Facebook at work could be considered to violate the CFAA, or really doing anything against the terms and services of a website could be considered a violation. CFAA’s violations are considered a felony, punishable with fines or imprisonment, so the question is, what is not punishable? (O’Driscoll)

Finally, the initial reason for the establishment of this act was with the intention of establishing initiative for avoidance of security breach. This was a good move for the government as the future only promised more technological and programming developments which could be a threat to security, so in establishing this act, the threat of future problems was anticipated. This could be said to have been a stepping stone into higher security and avoidance of security breach crime, especially in efforts to protect confidential data of the United States.

In conclusion, the computer fraud and abuse act serve as a stance against computer related crimes. The future of the act is uncertain because of its varying controversy and these sorts of abuses pale in comparison to the potential for abuse by malicious prosecutors. The ability to throw potential jail time at accused hackers for relatively minor offenses can make the Act a serious threat to freedom. The continuing rapid advance of technology and imprecision of the language in the Act also creates as many problems for cybersecurity professionals as it solves. To this day, the CFAA continues to protect the privacy and security of computer data, yet sometimes in vain, the establishment of it had the initiative towards the avoidance of it, and the amends that followed have replenished that which the CFAA has lacked in.

References

18 U.S. Code § 1030 - Fraud and related activity in connection with computers. (n.d.). Retrieved from https://www.law.cornell.edu/uscode/text/18/1030

Computer Fraud and Abuse Act – Cybersecurity masters. Retrieved April 9. 2019. https://www.cybersecuritymastersdegree.org/what-is-the-computer-fraud-and-abuse-act/

Computer Fraud and Abuse Act - Definition from Techopedia. (n.d.). Retrieved April 9, 2019, from https://www.techopedia.com/definition/27434/computer-fraud-and-abuse-act-cfaa

Computer Fraud and Abuse Act Reform. (n.d.). Retrieved from https://www.eff.org/issues/cfaa

Goldman, E. (2015, January 14). The Computer Fraud and Abuse Act Is a Failed Experiment. Retrieved from https://www.forbes.com/sites/ericgoldman/2013/03/28/the-computer-fraud-and-abuse-act-is-a-failed-experiment/#2a7afe275e90

O'Driscoll, A. (2018, October 05). What is the Computer Fraud and Abuse Act? Retrieved April 10, 2019, from https://www.comparitech.com/blog/information-security/computer-fraud-and-abuse-act/

Wydeven, R. (2018, May 12). Reg Wydeven column: 'War Games' movie prompted introduction of computer fraud act. Retrieved April 10, 2019, from https://www.postcrescent.com/story/money/2018/05/12/war-games-prompted-introduction-computer-fraud-and-abuse-act/590388002/