Legislative Tracing and Policy Analysis : Computer Fraud and Abuse Act of 1986

Justin Stutler

University of South Florida

LIS: 4414 Information Policy and Ethics

Dr. Karen Kaufmann

November 6, 2023

Introduction

In the early 1980s, the United States was experiencing a technological revolution by means of the computer. The federal government began operating tens of thousands of computers and was predicted to operate hundreds of thousands of computers by 1990 (Thurmond, 1986, p. 2). Computers were also popularized in the private sector, growing from roughly 5000 in 1978 to roughly 5 million in use by 1986 (Thurmond, 1986, p. 2). With the proliferation of computers, there was a "growing concern about the lack of criminal laws available to fight emerging computer crimes." (Jarrett & Bailie, 2008, p. 1). The wire and mail fraud laws addressed some computer crimes, but they were not established with the intention of addressing computer crimes. In order to fill in this gap in the law, congress passed the Comprehensive Crime Control Act of 1984 (Section 1030). This law made it a, "felony to access classified information in a computer without authorization and (made) it a misdemeanor to access financial records or credit histories stored in a financial institution or to trespass into a government computer."(Jarrett & Bailie, 2008, p. 1). Section 1030 addressed some areas of computer crimes, but even after it was passed, congress continued to question if the law needed further revision. After almost two years of discussion of computer crime bills, Congress passed the Computer Fraud and Abuse Act of 1986 (CFAA).

Legislative Tracking : Initial Law

The CFAA was introduced as two identical bills with one in the House of Representatives by Representative Hughes as H.R. 4562 and one in the Senate by Senator Trible as S. 2281 on April 10, 1986 (Thurmond, 1986, p. 4). By April 30, H.R. 4718, a revised version of H.R. 4562, officially began the CFAA's journey to becoming a law (Thurmond, 1986, p.4). Due to the

bicameral nature of the United States' government, in order for the CFAA to become a law, the House must pass its version of the law, the Senate must pass its version of the law, the differences between the versions must be resolved, and then the law must be signed by the President. H.R. 4718 began the process on April 4, 1986 and became Public Law No. 99-474 on October 16, 1986 (1). The original purpose of this bill was to provide separate legislation that addressed and punished computer crimes while protecting the operations of the government and financial institutions. As time went on, congress continued questioning if the law was comprehensive of computer crime.

Amendments

The CFAA was enacted in 1986 which means it has been amended 8 times in roughly 37 years with one time in each of the following years: 1988, 1989, 1990, 1994, 1996, 2001, 2002, 2008 (Jarrett & Bailie, 2008, p. 2). The most notable amendment to the CFAA is the inclusion of the term, "protected computer" which is defined as, "computers used in or affecting interstate or foreign commerce and computers used by the federal government and financial institutions." (Jarrett & Bailie, 2008, p. 4) This amendment expanded the boundaries of the CFAA to cover virtually any computer by including the ambiguous wording of, " affecting interstate or foreign commerce". "Several courts have held that using the Internet from a computer is sufficient to meet this element."(Jarrett & Bailie, 2008, p. 4) The Patriot Act amended this definition further to include computers outside the United States affecting interstate or foreign commerce or communication of the United States (Jarrett & Bailie, 2008, p. 4). The definition of protected computers allows the CFAA and the Patriot Act to be applied to virtually any computer.

Current Infringements and Sentences

The most recent version of the CFAA includes 7 crimes with varying sentences (years): obtaining nation security information (10), accessing a computer and obtaining information (1-5), trespassing in a government computer (1), accessing a computer to defraud and obtain value (5), intentionally damaging by knowing transmission (1-10), recklessly damaging by intentional access (1-5), negligently causing damage and loss by intentional access (1), trafficking in passwords (1), extortion involving computers (5) (Jarrett & Bailie, 2008, p. 3).

Policy Analysis : Clarity and Interpretation

The policy clearly lays out 7 different computer crimes with various sentences for each violation. The intention of the policy is understood as a policy attempting to regulate computer hacking and fraud. The policy addresses its intentions consistently throughout itself. Although the policy is clear about the punishments for the violations, the policy has ambiguous boundaries. Many of the prosecutions have involved the terms “without authorization”, “exceeding authorized access”, and “protected computer” due to the ambiguity of the boundaries of these terms (Jarrett & Bailie, 2008, p. 4-5). With the current definition of protected computer, virtually any computer could be considered to affect interstate commerce. This policy was originally intended to address a specific area of law that was going unaddressed, but now this policy has expanded to cover virtually all aspects of society.

Relationship with other Policies and Implementation

The Computer Fraud and Abuse Act, “makes a number of amendments to Section 1030 of Title 18 of the United States Code, dealing with computer fraud and related activity.” (Thurmond,

1986, p. 15). The CFAA provides additional revision to section 1030 without any contradictions. Section 1030 is directly a part of Title 18 which is the main criminal code of the United States.

Additions : Aaron's Law

I believe the Aaron's Law Act of 2013 should have passed through congress, but it did not. This amendment to the CFAA would establish boundaries making the law less ambiguous by excluding terms of service violations. Aaron Swartz was a technologist who helped improve the digital public in many ways including helping develop the technical architecture, RSS, for Creative Commons ("Aaron Swartz," 2023). Creative Commons is a non-profit organization that distributes copyright licenses free of charge to the public ("Creative Commons license," 2023). Creative Commons is dedicated to improving, "educational access and expanding the range of creative works available for others to build upon legally and to share." ("Computer Fraud and Abuse Act," 2023). Swartz was arrested in 2011 for violating the terms of service of JSTOR, a digital library, when downloading millions of academic journals ("Aaron Swartz," 2023). Swartz was charged with wire fraud, computer fraud, unlawfully obtaining information from a protected computer, and recklessly damaging a protected computer. Swartz was then charged with breaking and entering with intent, grand larceny ,and unauthorized access to a computer network. Eventually these charges were dropped in efforts of a federal prosecution which led to a prosecution of Swartz with potential for 50 years of imprisonment and $1 million in fines ("Aaron Swartz," 2023). Swartz was prosecuted for over 2 years with the only viable option given to him being a plea bargain where he has to admit guilty to 13 federal crimes and spend 6 months in a low security prison. Swartz committed suicide in 2013 because of this excruciating prosecution. Tim Wu wrote in the New Yorker that Swartz's act was harmless with JSTOR

suffering no losses and not pressing charges ("United States v. Swartz," 2023). The Aaron's Law Act of 2013 was drafted in order to protect others from what happened to Aaron Swartz.

Evaluation

The effects of the policy can be evaluated in a number of ways. The primary way to gauge the effectiveness of the policy is to evaluate the law's effectiveness in preventing hacking on government or financial computers. As hacking incidents among the government or financial institutions bring about bad press, these incidents are often hidden from the public eye. This can play a factor in the data regarding hacking incidents. It is truly a difficult task to determine the effectiveness of the CFAA. Another way of determining the effectiveness would be to understand the extent of its use in prosecution. The prosecution and subsequent suicide of Aaron Swartz provides some perspective in this sense. The CFAA clearly has been misused by the prosecutors in this case, and unfortunately resulted with the world losing an amazing individual responsible for serving the public good.

Ethics

I believe there are many ethical implications associated with the CFAA. From a virtue ethics perspective, Aaron Swartz was a virtuous individual who helped create technologies for the greater good of society and helped enlighten millions through his work with the Creative Commons. Aaron's violation of JSTOR terms of service was justified in this ethical perspective due to his intention to make information more accessible to the public. By making millions of academic journals publicly available on the internet at no cost, Aaron was performing a public

service. From this ethical perspective, Aaron was acting ethically and was unreasonably prosecuted for 2 years until he was driven to suicide. It was unethical from this perspective for the prosecutors to relentlessly attempt to charge Aaron as a felon.

Conclusion

One of the most interesting aspects of the CFAA is how often it is attempted to be amended. Swartz's law was stalled in congress on two separate occasions preventing it from becoming a law. There have been many attempts to alter the CFAA, and many of the changes have passed, altering the law, but also many attempts have resulted in no changes as well. The CFAA, although intended to protect the government and financial institutions from the dangers of hacking, has been expanded multiple times and now is available as a tool to prosecute those acting in an undesirable manner such as the case with Swartz. I believe the law is too ambiguous and too expansive in domain, but I also believe it was necessary at the time to construct some sort of law addressing computer crimes as to relieve the mail and fraud laws of this duty.

References

Aaron Swartz. (2023, October 21). Wikipedia, the free encyclopedia. Retrieved November 7, 2023, from https://en.wikipedia.org/wiki/Aaron_Swartz

Computer Fraud and Abuse Act. (2023, July 24). Wikipedia, the free encyclopedia. Retrieved November 7, 2023, from https://en.wikipedia.org/wiki/Computer_Fraud_and_Abuse_Act

Creative Commons license. (2023, November 7). Wikipedia, the free encyclopedia. Retrieved November 7, 2023, from https://en.wikipedia.org/wiki/Creative_Commons_license

H.R.4718 - Computer Fraud and Abuse Act of 1986. (n.d.). congress.gov. https://www.congress.gov/bill/99th-congress/house-bill/4718?overview=closed

Jarrett, H. M., & Bailie, M. W. (2008). Prosecuting computer crimes. Office of Legal Education Executive Office for United States Attorneys. https://www.justice.gov/d9/criminal-ccips/legacy/2015/01/14/ccmanual_0.pdf

Thurmond. (1986, September 3). Computer Fraud and Abuse Act of 1986 Report 99-432. cia.gov. https://www.cia.gov/readingroom/docs/CIA-RDP87B00858R000400480020-8.pdf

United States v. Swartz. (2023, October 5). Wikipedia, the free encyclopedia. Retrieved November 7, 2023, from https://en.wikipedia.org/wiki/United_States_v._Swartz