The Social Implications of the Federal Computer Fraud and Abuse Act

Christian Carrion

Department of Cyber Security, University of Old Dominion

CYSE 254W: Cybersecurity Strategy and Policy

Professor Duvall

November 13, 2024

Social Factors leading to the Federal Computer Fraud and Abuse Act

There were many social factors that led to the development of the Computer Fraud and Abuse Act. One of them is the rise of personal computers. In the early 1980s, computers were becoming more affordability and easily accessible to the public. This rise of PCs brought opportunities to the public for educational, personal, and professional purposes. However, this also brought a rise of cybercrime. The widespread use of computers causes difficulty in governing traditional laws like theft, and trespassing, since in the cyber environment it was hard to detect and determine if those laws were broken. This new technological environment called for new laws that were specifically meant to combat cybercrime. Hence the Computer Fraud and Abuse act was created.

Another social factor was the public awareness of hacking. During the early years of the internet, the term hacking was not seen as a concern. Most of the hacking done was merely pranks and relatively harmless. However, the hacks become more sophisticated and malicious. One famous case of this sort of hacking was Kevin Mitnick (One of the most famous convicted hackers and was one of the FBI's most wanted). In the 1980s and 1990s, he hacked into several major corporations such as Nokia, Sun Microsystems, and Motorola. These malicious attacks increased public awareness that laws governing computer security needed to be strengthened. This perception of a new threat, pushed for the development on new legal laws that can assist in strengthening digital security. In this case, one of these laws developed was the Computer Fraud and Abuse Act.

Social Consequences

Though the Computer Fraud and Abuse Act was designed to combat cybercrime, and enforce punishment, the policy unfortunately resulted in several social consequences. Some include:

1. Over-criminalization
    - The term "unauthorized access" is board in the CFAA and has resulted in unjust prosecutions. For example, in the court case U.S.V. Andrew Auer Heimer, Andrew tested AT&T's security system and discovered flaws. He was able to gather email addresses of customers. He notified AT&T personal, but they did not act. In response to this Andrew publicized the security flaws. Later AT&T contacted the federal government, who prosecuted Andrew. In terms of the CFAA, Andrew did not have unauthorized access and violated the CFAA. However, Andrew was conducting a security test that involved discovering vulnerabilities. (National Association of Criminal Defense Lawyers)
2. Legal Ambiguity
    - Due to the CFAA's ambiguity, the law is inconsistent. This leads to misunderstanding for people for what is considered illegal and legal cyber activities. An example is the Van Buren V. United States. Van Buren used his patrol vehicle computer to access a law enforcement database to retrieve information about a license plate number. After retrieving the information, he used that info in exchange for money. Under the CFAA, he was found guilty for "intentionally" accessing a computer without proper authorization. However, the police officer used his valid credentials to perform the

search. Technically speaking, the CFAA was not clear under this premise. So, the supreme court dismissed the case. (Supremecouret.org)

- In the same topic of legal ambiguity, In the article "The Computer Fraud & Abuse Act: Failing to Evolve with the Digital Age" the author mentioned a flaw that there is no way suppression remedy against hackers, since a defense could easily make a counter argument for civil damages against the government. (W. Cagney McCormick)

How culture influenced the shape of the policy

During the cold war, the government was concerned for national security, and the idea of foreign adversaries attacking the U.S computer systems. A major fear that spread through the public was espionage and cyber warfare. This fear will eventually drive the national government to create safeguards for national defense. This includes the CFAA being one of those safeguards/policies. This also, changed the mindset of the language of the law, emphasizing stronger laws to protect against cyber-attacks.

References

McCormick, W. Cagney. (2013). *The Computer Fraud & Abuse Act: Failing to Evolve with the Digital Age* (Vol. 16) [Review of *The Computer Fraud & Abuse Act: Failing to Evolve with the Digital Age*].

National Association of Criminal Defense Lawyers. (2022, July 14). *NACDL - CFAA Cases*. NACDL - National Association of Criminal Defense Lawyers. https://www.nacdl.org/Content/CFAACases

SUPREME COURT OF THE UNITED STATES. (2020). https://www.supremecourt.gov/opinions/20pdf/19-783_k53l.pdf