The Effectiveness 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 25, 2024

Introduction

Cybersecurity has brought a source of threats in the digital environment. During the early years of internet, the term “hacker” or “threat actors” was not a concern for cyber security at the time. The hackings that were done back then were mostly pranks and trolling purposes. However, technology and the internet continued to develop, so too the hacks. The term hackers started to catch attention as they started to develop more sophisticated and malicious attacks. In 1984, Congress established the Computer Fraud and Abuse Act. The main objective of the policy was to combat cybercrimes and penalize cybercriminals/hackers who deliberately break into systems and networks with authorized access. The Computer Fraud and Abuse Act was one of the first laws designed to address computer-related crimes. Over the years, it has been highly debated on the overall effectiveness of the policy, because it has its strengths and weaknesses. The paper will cover an overview of its effectiveness.

Social implications

In the social view, the Computer Fraud and Abuse Act can be seen as an effective policy to combat cybercriminals. Since the malicious hacks were rising public awareness, this pushed the government to develop stronger cyber security measures, and legal laws to combat against the emerging threat of cyber-attacks. However, there were social consequences that will deem it ineffective. According to W. Cagney McCormick that CFAA was flawed since there is no way suppression remedy against hackers (The Computer Fraud & Abuse Act: Failing to Evolve with the Digital Age”). It can be assessed in terms of social implications, there were rightful intentions behind the creation of the CFAA, however the was a lack of specifics, and lack of consideration of the social consequences that potentially could arise. Also, theses lead legislation to push for reforms, to update and clarify definitions on what constitutes criminal violations.

Ethical Implications

In the ethical view, the CFAA has address certain rights, but also lead to several reforms For example, one of the rights protected under the CFFA is securing personal information. This ensures that the confidentiality of sensitive data is protected. According to Jonathan S. Keim, he compares tort law to computer intrusions as being similar (Updating the Computer Fraud and Abuse Act"). The CFFA policy addresses the rights of individuals, and in doing so shows that it does effectively secure personal information and keep it confidential. However, one ethical dilemma of the CFAA its prosecution of whistleblowers. There was a court case Sandvig v. Sessions were academic researchers filed a lawsuit against the CFAA for violent freedom of speech (Komal Patel). This and other cases like Van Buren v. United States would lead to the clarification of the term "Exceeding Authorized Access. Based on these assessments, CFAA did have flaws which led to inequity in prosecution, and excessive penalties for non-malicious behavior. Similar to social implications, it led to several reforms of the CFAA.

Political Implications

In terms of political implications, the CFAA has been revised many times to strengthen the policy. However, it still suffered from its lack of definition of the term "unauthorized access" and board language. The CFAA led to the misuse of law, and the policy was rarely used in court cases due to its board language of law. Other polices like the Digtial Millennium Copyright Act and Cybersecurity Information Sharing Act have been developed due to the CFAA's shortcomings. Based on this assessment, the CFAA was not an effective policy and was not successful.

Conclusion

Overall, in my view, the CFAA was not much of an effective policy to combat cybercriminals and cybercrimes based on the ethical, social, and political implications. It suffered from board language, lack of clarification of the term “unauthorized access”, over-criminalization, and it was an outdated policy. Since the cyber environment is growing rapidly the CFAA did not have the capability to keep up and address the complexity of modern cyber threats. However, it was successful in one thing. It started up a framework for future cyber security related polices.

References

Keim, J. (2016). *Updating the Computer Fraud and Abuse Act* [Review of *Updating the Computer Fraud and Abuse Act*]. *13*(3).

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*].

Patel, K. (2017). *Testing the Limits of the First Amendment: How a CFAA Prohibition on Online Antidiscrimination Testing Infringes on Protected Speech Activity* [Review of *Testing the Limits of the First Amendment: How a CFAA Prohibition on Online Antidiscrimination Testing Infringes on Protected Speech Activity*].