# Cybercrime, Hacking, And Legislation

Kimberly Pavlik, Walden University, USA

**ABSTRACT**

*As cybercrime continues to evolve, legislation will continue to play a key role in the prosecution of individuals committing computer related offenses. The public has witnessed the rapid change in computer technology, continued popularity of social media, and increased e-commerce. With those changes comes an increase in computer crimes being committed. This article gives an overview of the evolution of cybercrime, and its influence on current legislation.*

**Keywords**: Computer Fraud and Abuse Act; CFAA; Cybercrime; Hacker; Social Networking

With increased social networking and the ability to make more online purchases, personal information is required in order to utilize these sites. Personal and private information, such as bank account numbers and credit cards numbers, are linked through individual profiles created by users. Credit card information is stored for purchases and personal data remains saved within the user's online account. Consumers assume that their personal information is stored securely when shopping online on sites such as Amazon, or interacting on social media sites like Facebook (FB). What consumers fail to realize is that every time they conduct a search online, they are compromising their own privacy if they do not activate their user settings on social networking sites.

Social networking sites allow users to activate settings that enable online privacy for their accounts. For example, FB users select the specific privacy settings on their account which allows certain information to be shared with close friends and acquaintances. These same privacy settings also allow the user to block or *unfriend* other individuals to prevent interaction with people they do not wish to share information with online. Similarly, Amazon allows users to configure and manage their profile page and privacy settings. Having the ability to set your privacy settings for your particular account is helpful in preventing identity theft; however, it is no guarantee that these measures prevent hackers from getting into the system. The online users must be the ones that activate privacy settings at the time they create their account in order to safeguard their personal information. Thus, personal online information can easily be compromised and a user's privacy can be violated. Accounts such as Yahoo, Gmail, or LinkedIn can even be compromised whether they are used as a means for communication or for professional networking. In 2012, 117 million LinkedIn accounts were allegedly hacked and passwords and individuals credentials were stolen by a Russian citizen who was arrested in Prague in 2016 (Kottasova, 2016). This arrest goes to show that everyone is at risk for being hacked either domestically or internationally.

As technology continues to evolve around the globe, people should be concerned with the type of information they post on social media and networking sites. Individuals should remain vigilant in an effort to secure their personal information online in order to reduce the chance of being hacked and a victim of criminal activity. It is apparent that securing personal information, while accessing online social networking sites, has become a challenge for many users (Henson, Reyns, & Fisher, 2011). Therefore, this article explains what a hacker is and gives an overview of the evolution of cybercrime, and its influence on current legislation.

## HACKER

There are many definitions for the term *hacker*; however, there does not seem to be a universal definition or consensus on the term based upon a review of the literature. According to Taylor, Fritsch, and Liederbach (2015), *hackers* are individuals who gain unauthorized access to computers and exploit the weakness in the system. Conversely, hacking can also be done legitimately in order to ensure that a company's software is protected. While researching hacking, numerous articles revealed that hacking can be legitimate when one has permission to access the system (Taylor et al., 2015). An example of a legitimate hacker, as explained by Taylor et al. (2015), is a white hat. White hats are

individuals, such as security computer experts, who test the methodologies of the company's information system trying to find a flaw in the system (Taylor et al., 2015). On the other hand, black hats are individuals who are illegitimate hackers. They are malicious individual who create malware and intrude upon networks illegally (Taylor et al., 2015). Illegitimate hackers can be subject to prosecution depending upon the particular type of crime their action falls under according to legislation.

## INITIAL CYBERCRIME LEGISLATION

Criminal laws have been enacted by the U.S. Congress that outlaw unauthorized access to *protected* computers by individuals. Protected computers are defined under U.S. Code Title 18, Section 1030 and there are a number of state and federal statutes that focus on unauthorized computer access which are related to computer crimes. One example is the Computer Fraud and Abuse Act (CFAA) that was originally passed in 1986 and has been amended numerous times since then to simplify and increase the scope of an existing computer fraud law. According to Alexander (2007), the CFAA was designed to protect government classified information and financial institution information that was stored on computers. If the computer was connected to the internet, this Act makes it a criminal offense for an individual to access it without proper authority or in an attempt to obtain financial information illegally. However, according to Taylor et al. (2015), this Act appears very vague, and has been amended to include computer hacking offenses and the transmission of classified information in or outside the United States. The CFFA was originally designed by Congress to criminalize unauthorized access to computers (Kerr, 2015). This legislation was very broad when it was initially enacted, and now requires a clearer interpretation of the guidelines that prohibit the requirement for due process of law.

## CYBERCRIME LEGISLATION

There are several liabilities to consider if a computer was illegally accessed under the current CFAA statute. First, code-based liability would include hacking into a computer by using someone else's password to access the computer system (Taylor et al., 2015). This offense is considered a misdemeanor and can be upgraded to a felony if the information recovered is used for profit (Taylor et al., 2015). Second, contract-based liability is when an employee breaches a written employment agreement regulating access to an employer's computer. If the employee violates the agreement and by-passes a technological access barrier, then the employee can be in violation of the Act. Third, norms-based liability can be deemed an illegal action if unauthorized access is beyond socially accepted practices (Taylor et al., 2015). Once again, this violation can be considered a misdemeanor unless information obtained is used for profit. According to Taylor et al. (2015), this offense can also be upgraded if the information obtained is worth more than $5000. All three liabilities can involve imprisonment if certain criteria are met in a court of law.

## SIGNIFICANT DIFFERENCES

There are some significant differences between the initial and current legislation regarding CFAA. The first difference is that there is a specific dollar amount associated with whether or not the offense committed is a misdemeanor or felony (Kerr, 2015). The second difference is that the CFAA revolutionized the computer era and can be used and/or cited in civil lawsuits. The third difference is that *authorized access* was not clearly defined in the legislation (Orin, 2003). With that said, hackers did not have to worry about breaking any laws during the 1950s-1970s since there were no laws in place (Taylor et al., 2015). Today, laws must be more stringent in order for there to be a deterrent for cybercrime offenses. The new legislation thus allows prosecutors the ability to increase the punishment from fines to imprisonment if the criteria are met.

## EVOLUTION OF CYBERCRIME

The term *hacker* originated years before computers existed. The Massachusetts Institute of Technology (MIT) routinely created college pranks on campus known as hacks, which ranged from building a replica of a police car and placing it on the university roof, to hiding the president's office door with a bulletin board (Taylor, et al., 2015). In the 1960s, the concept of hacker went from college pranks to military applications, which was attributed to the Vietnam War (Taylor, et al., 2015). During this time period, programmers were infuriated because they believed computer information should be free, readily accessible, and would thus change their lives for the better. According

to Taylor et al. (2015), during the 1970s phone phreaking, or phone technology tampering, was developed. In 1988, the first computer virus, Morris Worm, was distributed on the internet and became known as the modern-day cybercrime (Lee, 2015). During the early 2000s, many criminals realized that collecting information from infected computers could be very profitable and decided to capitalize on stolen data, thus making cybercrime easier to achieve (Lee, 2015). In an effort to minimize online identity theft, individuals should be proactive and utilize encryption software to safeguard their personal information from being hacked (Lee, 2015). This is an inexpensive way to safeguard your computer.

It appears that computer hacking can lead to other crimes such as theft, fraud, and terrorists activity. For instance, criminals have been known to use computer technology as a way to conceal their location in an effort to commit a crime. As different types of cybercrimes continue to evolve, legislation will continue to play a key role in the prosecution of individuals committing computer related offenses. With the evolution of the IPad, the public has witnessed the rapid change in computer technology, continued popularity of social media, and increased e-commerce. With those changes comes an increase in computer crimes being committed. Police agencies will need to employ computer savvy detectives and forensic examiners that specialize in computer crime offenses. Court personnel will also need advanced computer training knowledge to objectively handle cases that will flood the criminal justice system. Even federal agencies need trained personnel as well so that they can remotely access and search computers, storage devices, and phones in cases where victims have had their computers infected with malware. In closing, the media continues to bring to light that no one is exempt from hacking to include government agencies, personal online accounts, financial institutions, and retail stores. Online anonymity, privacy concerns, and the security of cyberspace should be a concern of anyone that uses the internet.

## AUTHOR BIOGRAPHY

**Kimberly Pavlik** is currently a Ph.D. candidate in the Criminal Justice program at Walden University. Kimberly plans to explore the migration patterns of human trafficking in Middle East North Africa region in an effort to identify the victims, eliminate trafficking demand, and seek prosecution of individuals that commit trafficking offenses. Kimberly received her Master's in Higher Education with a minor in Criminal Justice from Union Institute & University (UI&I). She received a Bachelor of Science in Business Administration from Nova-Southeastern University (NSU) together with a Legal Assistant/ Paralegal Studies certificate. Furthermore, Kimberly also received her Associate of Science in Criminal Justice from Broward College (BC) and a diploma from the American Institute of Applied Science (AIAS) in Advanced Forensic Science. In 2016, Kimberly received a TESOL certificate from TEFL International, Fort Hayes State University and has taught beginner and intermediate English courses to children and adults in Florence, Italy.

## REFERENCES

Alexander, G. (2007). The emergence of cybercrime and the legal response. *Journal of Security Education* 2(2), 47-79. doi:10.1300/j460v02n02_04

Henson, B., Reyns, B.W. & Fischer, B.S. (2011). Security in the 21st century: Examining the link between online social networking activity, privacy, and interpersonal victimization. *Criminal Justice Review 36*(3), 253-268. doi: 10.1177/0734016811399421

Kerr, O. (2015). Obama's proposed changes to the computer hacking statute: A deep dive. *The Washington Post.* Retrieved from: https//www.washingtonpost.com/news/volokh-conspiracy

Kottasova, I. (2016). Arrested Russian linked to theft of 117 million LinkedIn passwords. CNN Tech. Retrieved from http://money.cnn.com/2016/10/20/technology/russian-hacker-arrested-linkedin-password/

Lee, M. (2015). The evolution of cybercrime: From Julius Caesar and Prince Philip to state-sponsored malware. *International Business Times.* Retrieved from: http://ibtimes.co.uk

Orin, S.K. (2003). Vagueness challenges to the computer fraud and abuse act. *Minnesota Law Review*, 1561-1587. Retrieved from http://minnesotalawreview.org

Taylor, R. W., Fritsch, E. J., & Liederbach, J. (2015). *Digital crime and digital terrorism.* (3rd ed.). Upper Saddle River, NJ: Pearson

**NOTES**