Jon Bowen

Dr. Jeffrey P. Ogle

PH 3370 Computers, Ethics, and Society

Final Exam

December 12, 2017

Prompt 1

The Computer Fraud and Abuse Act (CFAA), passed in the mid-80’s, is the primary US antihacking law that applies to government computer and financial systems and all computers used in interstate and international commerce and communication (Baase 289). A law such as this is needed to criminalize some activities that were not anticipated by previous laws. Examples of such activities include remotely reading, altering, or deleting data on a networked computer when unauthorized, obtaining user credentials through trickery, and disrupting or impairing services offered by the government or an organization. Such activities can clearly must be prohibited or restricted, but were often only tangentially covered or were covered by extension of existing laws. For example laws regarding privacy, trespassing, vandalism, and intellectual property did not anticipate digital computers, new forms of information storage, or the consequence of connecting computers over a network.

While such a law is necessary, the CFAA is often too broad and applies penalties that are often disproportionate to the harm done by or intended effects of offenses. The fact that the law applies to all computers used in interstate and international commerce or communication effectively means it applies to every computer, cell phone, and tablet and, increasingly, refrigerators, coffee makers, and light bulbs. In effect, it applies to a vast array of the ordinary activities of citizens rather than just malicious computer experts. It elevates, in theory, violating the terms of service of a website, the lengthy inscrutable documents that few users read or are even equipped to understand, to a federal crime with a prison sentence. Clearly sharing a Netflix password with a relative or pretending to be someone else on Facebook should not be a federal case. Beyond the application of the law to activities not normally associated with “hacking,” the law also fails to distinguish the nature of the hacking.

There is good hacking, socially beneficial hacking, and purely malicious hacking. Academics and students engage in hacking activities to learn about cybersecurity and prevent malicious hacking. Some security professionals try to gain unauthorized access to systems precisely to alert the owners of those systems of their vulnerabilities. Some of these activities would be serious violations of the CFAA, but both provide a clear benefit to society.

Some hacking activities should be illegal, but are different in kind from criminal enterprise. A hacker at MIT was caught bulk downloading academic papers in violation of the website’s terms of service. This alone was enough to faces years in federal prison, a sentence that appears rather excessive for violating website policy. He may have intended to make the research freely available online, a clear theft of intellectual property. However making research often conducted with federal funding freely available to tax payers provides a clear social benefit and has other than malicious motivation. Another law, the Digital Millennium Copyright Act made it illegal to produce or disseminate technology that circumvents Digital Rights Management methods. Hackers who right such software are not inherently stealing intellectual property. Users of such tools who are merely converting their purchase from a DVD to another format also do not seem nefarious. It seems rather disproportionate to punish this kind of hacking as severally as stealing classified documents from the Central Intelligence Agency or stealing intellectual property on a commercial scale.

Purely malicious hacking, on the contrary, is exactly the activity that the CFAA intends to target and penalize. Creators of bot nets that steal CPU cycles of unsuspecting computer owners to mine bit coin, hackers using phishing schemes to collect and sell credit card and social security numbers, experts engaging in theft of intellectual property and state secrets for sale to the highest bidder should indeed face large fines federal prison time. This kind of hacking is very harmful and produces no social good. Prosecutors, judges, and legislators need to distinguish between these differences in kind and degree when applying and writing laws.

A few concepts should aid in distinguishing between various kinds of hacking. Motivation matters. Curiosity and challenge are clearly more ethical than doing harm or making money. Punishment should be proportional to harm. Changing some content on a website to be funny or offensive is much less damaging than encrypting a hospital system’s data. Intent modifies the appropriate punishment for harm done. Suppose a virus spreads rapidly and allows a master program to do calculations on host machines. The harm done is perceived differently if the offender is an academic researcher that accidentally released his Ph.D. thesis compared to a hacker ring building a bot net to mine bit coin. Finally age should be a factor in deciding consequences. There is a difference between an immature 16 year old pushing limits and making bad decisions and a mature professional making calculated choices. Weighing all these factors together encourages balanced application and authorship of antihacking laws.

Prompt 2

Works Cited

Baase, Sarah and Timothy M. Henry. *A Gift of Fire: Social, Legal, and Ethical Issues for*

*Computing Technology*. Fifth Edition, Pearson, 2017, New York.