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

Computing professionals are bound by a specific code of ethics derived from more general ethical viewpoints. Broad ethical principles such as honesty, integrity, producing good, and avoiding causing harm take specific form when applied to computing professionals utilizing their expertise. The foundation of this code is rooted in both deontological and consequential ethical theories. Professionals must consider both their duties, in a Kantian sense, and judge their actions based on the effects they produce in a Utilitarian sense. Combining these perspectives provides the set of obligations and constraints that computing professionals are bound by.

Honesty is the first obligation of computer professionals. Computer experts possess deep insights that lay persons do not, and lay persons must rely on professionals completely as to the working of computer systems. The obligation of honest clearly precludes outright lying about what a product does or how it operates. This duty is directly rooted in Kantian ethics Furthermore, because lay persons often do not know what questions to ask or concerns to have, it also includes the duty to proactively communicate information lay persons do not know they need. The ethical professional must be an advocate on behalf of the ignorant. Merely refraining from making false statements is not sufficiently ethical. This obligation emanates in part from “imperfect duty” to help others posited by Kant, and is further supported from the Utilitarian perspective by considering the consequences of uninformed users operating technology.

Professionals are also obligated to be both competent and assiduous. These duties find direct support from Utilitarianism. Computing professionals wield great and hidden power. Through incompetence they may reduce privacy, greater enable cybercrimes such as fraud and theft easier, create an artificial intelligence that does harm, or allow patients to be delivered dangerous levels of radiation. Risks such as these obligate professionals to proceed only with competence and to refrain from proceeding when competence is lacking. There is also an implied duty to grow competence over time. This is supported by Kant’s imperfect duty to improve oneself.

Assiduity is also an obligation on the same grounds because competence is necessary but not sufficient to avoid potential harms such as the ones mentioned above. The application of competence must be careful and intentional. It is one thing to know how to secure personal information sent between web hosts. It is another to ensure that the software is implemented without error.

Professionals are also obliged to respect the rights and wellbeing of others. Data belonging to private persons or organizations should be used as agreed or in accordance with their wishes. Technology should operate transparently and as users intend. Product and design choices should be made with focus on the impacts on and the consequences for society in general and stakeholders in particular. Respect for the rights of others is central to Kant’s humanity formulation of the Categorical Imperative. Others must be treated as ends in themselves having intrinsic value. Consideration of the wellbeing of all is supported by the Utilitarian perspective that ethical actions increase the overall good or do the least harm.

The Software Engineering Code of Ethics and the ACM Code of Ethics and Professional Conduct are both high consistent with the obligations described above. Many of the tenants in these codes are more specific formulations of the broad responsibilities stated here. However they do contain additional areas of focus. Both contain sections with policies for professionals managing others. These provide principals on how organizations that employ computing professionals should be organized and disposed toward employees and clients. Both also contain principals relating to the obligations between professionals themselves including professional review, assistance, education, and respect.

Of the two codes, there is one possible discrepancy. The ACM Code of Ethics and Professional Conduct lists “know and respect existing laws pertaining to professional work” as a responsibility of computing professionals. Professionals ought to be bound by ethics rather than mere legislation. It so happens that often laws are often rooted in ethics, but sometimes they are not. State sponsored espionage of citizens, limitations on privacy, and strong censorship are lawful in some countries. In such countries and such cases, professionals may submit to related laws if their conscience allows, but ethical behavior should be prioritized over lawful behavior.

Prompt 3

Begin…

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.