Thomas George
IFSC 2200
Final Project
Dr. Berleant
December 9, 2013

Computer Ethics

Ethics deals with placing a “value” on acts according to whether they are “good” or “bad”. Every society has its rules about whether certain acts are ethical or not. These rules have been established as a result of consensus in society and are often written into laws.
When computers first began to be used in society at large, the absence of ethical standards about their use and related issues caused some problems. However, as their use became widespread in every facet of our lives, discussions in computer ethics resulted in some kind of a consensus. Today, many of these rules have been formulated as laws, either national or international. Computer crimes and computer fraud are now common terms. There are laws against them, and everyone is responsible for knowing what constitutes computer crime and computer fraud.

The Ten Commandments

The Ten Commandments of computer ethics have been defined by the Computer Ethics Institute.

1) Thou shalt not use a computer to harm other people:
2) Thou shalt not interfere with other people's computer work:
3) Thou shalt not snoop around in other people's files:
4) Thou shalt not use a computer to steal:
5) Thou shalt not use a computer to bear false witness:
6) Thou shalt not use or copy software for which you have not paid:
7) Thou shalt not use other people's computer resources without authorization:
8) Thou shalt not appropriate other people's intellectual output:
9) Thou shalt think about the social consequences of the program you write:
10) Thou shalt use a computer in ways that show consideration and respect:

On the flip side of the coin computer hackers have their own set of ethics. Some but not all of their ethics go directly against the ethics set in place by the Computer Ethics Institute.

The idea of a "hacker ethic" is perhaps best formulated in Steven Levy's 1984 book, Hackers: Heroes of the Computer Revolution. Levy came up with six tenets:

1) Access to computers - and anything which might teach you something about the way the world works - should be unlimited and total. Always yield to the Hands-On imperative!
2) All information should be free.
3) Mistrust authority - promote decentralization.
4) Hackers should be judged by their hacking, not bogus criteria such as degrees, age, race, or position.
5) You can create art and beauty on a computer.
6) Computers can change your life for the better.

Hackers

A hacker is a slang term for a computer enthusiast, i.e., a person who enjoys learning programming languages and computer systems and can often be considered an expert on the subject(s). Among professional programmers, depending on how it used, the term can be either complimentary or derogatory, although it is developing an increasingly derogatory connotation.

The pejorative sense of hacker is becoming more prominent largely because the popular press has cooped the term to refer to individuals who gain unauthorized access to computer systems for the purpose of stealing and corrupting data. Hackers, themselves, maintain that the proper term for such individuals is cracker.

Among hackers there are also different classifications and within these classifications there are different attitudes and views as to what they do and what a hacker is.

White hat

A white hat hacker breaks security for non-malicious reasons, perhaps to test their own security system or while working for a security company which makes security software. The term "white hat" in Internet slang refers to an ethical hacker. This classification also includes individuals who perform penetration tests and vulnerability assessments within a contractual agreement. The EC-Council, (Moore) also known as the International Council of Electronic Commerce Consultants, is one of those organizations that have developed certifications, course-ware, classes, and online training covering the diverse arena of Ethical Hacking (Wilhelm).

Black hat

A "black hat" hacker is a hacker who "violates computer security for little reason beyond maliciousness or for personal gain" (Moore). Black hat hackers form the stereotypical, illegal hacking groups often portrayed in popular culture, and are "the epitome of all that the public fears in a computer criminal" (Moore). Black hat hackers break into secure networks to destroy data or make the network unusable for those who are authorized to use the network.

Grey hat

A grey hat hacker is a combination of a black hat and a white hat hacker. A grey hat hacker may surf the internet and hack into a computer system for the sole purpose of notifying the administrator that their system has a security defect, for example. Then they may offer to correct the defect for a fee (Moore)

Elite hacker

A social status among hackers, elite is used to describe the most skilled. Newly discovered exploits will circulate among these hackers. Elite groups such as Masters of Deception conferred a kind of credibility on their members (Thomas)

Script kiddie

A script kiddie (also known as a skid or skiddie) is a non-expert who breaks into computer systems by using pre-packaged automated tools written by others, usually with little understanding of the underlying concept—hence the term script (i.e. a prearranged plan or set of activities) kiddie (i.e. kid, child—an individual lacking knowledge and experience, immature) (Andress).

Neophyte

A neophyte, "n00b", or "newbie" is someone who is new to hacking or phreaking and has almost no knowledge or experience of the workings of technology, and hacking (Moore).

Hacktivist

A hacktivist is a hacker who utilizes technology to announce a social, ideological, religious, or political message. In general, most hacktivism involves website defacement or denial-of-service attacks.

Organized criminal gangs

Groups of hackers that carry out organized criminal activities for profit (Chabrow).

Intellectual Property

One of the more controversial areas of computer ethics concerns the intellectual property rights connected with software ownership. Some people, like Richard Stallman who started the Free Software Foundation, believe that software ownership should not be allowed at all. He claims that all information should be free, and all programs should be available for copying, studying and modifying by anyone who wishes to do so (Stallman). Others argue that software companies or programmers would not invest weeks and months of work and significant funds in the development of software if they could not get the investment back in the form of license fees or sales (Johnson). Today's software industry is a multibillion dollar part of the economy; and software companies claim to lose billions of dollars per year through illegal copying ("software piracy"). Many people think that software should be own-able, but "casual copying" of personally owned programs for one's friends should also be permitted (Nissenbaum). The software industry claims that millions of dollars in sales are lost because of such copying. Ownership is a complex matter, since there are several different aspects of software that can be owned and three different types of ownership: copyrights, trade secrets, and patents. One can own the following aspects of a program:

1. The "source code" which is written by the programmer(s) in a high-level computer language like Java or C++.
2. The "object code", which is a machine-language translation of the source code.
3. The "algorithm", which is the sequence of machine commands that the source code and object code represent.
4. The "look and feel" of a program, which is the way the program appears on the screen and interfaces with users.

A very controversial issue today is owning a patent on a computer algorithm. A patent provides an exclusive monopoly on the use of the patented item, so the owner of an algorithm can deny others use of the mathematical formulas that are part of the algorithm. Mathematicians and scientists are outraged, claiming that algorithm patents effectively remove parts of mathematics from the public domain, and thereby threaten to cripple science. In addition, running a preliminary "patent search" to make sure that your "new" program does not violate anyone's software patent is a costly and time-consuming process. As a result, only very large companies with big budgets can afford to run such a search. This effectively eliminates many small software companies, stifling competition and decreasing the variety of programs available to the society (The League for Programming Freedom)

Censorship

Accessibility, censorship and filtering bring up many ethical issues that have several branches in cyber ethics. Many questions have arisen which continue to challenge our understanding of privacy, security and our participation in society. Throughout the

centuries mechanisms have been constructed in the name of protection and security. Today the applications are in the form of software that filters domains and content so that they may not be easily accessed or obtained without elaborate circumvention or on a personal and business level through free or content-control software. Internet censorship and filtering are used to control or suppress the publishing or accessing of information. The legal issues are similar to off-line censorship and filtering. The same arguments that apply to offline censorship and filtering apply to online censorship and filtering; whether people are better off with free access to information or should be protected from what is considered by a governing body as harmful, indecent or illicit. The fear of access by minors drives much of the concern and many online advocate groups have sprung up to raise awareness and of controlling the accessibility of minors to the internet.

Censorship and filtering occurs on small to large scales, whether it be a company restricting their employees' access to cyberspace by blocking certain websites which are deemed as relevant only to personal usage and therefore damaging to productivity or on a larger scale where a government creates large firewalls which censor and filter access to certain information available online frequently from outside their country to their citizens and anyone within their borders. One of the most famous examples of a country controlling access is the Golden Shield Project, also referred to as the Great Firewall of China, a censorship and surveillance project set up and operated by the People's Republic of China. Another instance is the 2000 case of the League Against Racism and Antisemitism (LICRA), French Union of Jewish Students, vs. Yahoo! Inc (USA) and Yahoo! France, where the French Court declared that "access by French Internet users to the auction website containing Nazi objects constituted a contravention of French law and an offense to the 'collective memory' of the country and that the simple act of displaying such objects (e.g. exhibition of uniforms, insignia or emblems resembling those worn or displayed by the Nazis) in France constitutes a violation of the Article R645-1 of the Penal Code and is therefore considered as a threat to internal public order."(Akdeniz) Since the French judicial ruling many websites must abide by the rules of the countries in which they are accessible.

Countries in other regions also practice certain forms of filtering. In the United States state-mandated Internet filtering occurs on some computers in libraries and K-12 schools Content related to Nazism or Holocaust denial is blocked in France and Germany. Child pornography and hate speech are blocked in many countries throughout the world. In fact, many countries throughout the world, including some democracies with long traditions of strong support for freedom of expression and freedom of press, are engaged in some amount of online censorship, often with substantial public support.

Internet censorship in China among the most stringent in the world. The government blocks Web sites that discuss the Dalai Lama the 1989 crackdown on Tiananmen Square protesters, the banned spiritual practice Falun Gong, as well as many general Internet sites. The government requires Internet search firms and state media to censor issues deemed officially “sensitive,” and blocks access to foreign websites including Facebook, Twitter, and YouTube.

Conclusion

There are many views on computer ethics, you have the ethics set forth by the Association of Computing Machinery and you have “ethics” as seen from hackers. Even within the hacker groups you have different views. There are the white hats, who try to stop the black hats from penetrating there computer networks and stealing data. There are the organized criminal gangs who will do what ever is necessary to make a buck on the internet.

There is the fight over intellectual property, with some people believing all software should be free. Mathematicians and scientists don’t think you should be able to patent an algorithm, they think this takes mathematics from the public domain.

There are also the issues of censorship on the internet. With countries like China and North Korea censoring parts of the internet so that their citizens can access and view only the information they see fit to “protect them”. You have companies who limit what you can do on the internet as to not decrease productivity.

There are many views on computer ethics and it varies form one region of the world to the other, form one point of view to the other. Is one particular view right or wrong, no I don’t believe so. I believe you should go with you “gut”, does it feel right? Like many ethical issues in the world today there is a lot of grey area and I think as the profession matures some of the grey areas will become clearer.

Works Cited

Andress, Mandy, Philip Cox, and Ed. Tittel. CIW security professional certification bible. New York: Hungry Minds, 2001. Print.

Chabrow, Eric. "7 Levels of Hackers." 7 Levels of Hackers. N.p., n.d. Web. 12 Nov. 2013. <http://www.govinfosecurity.com/blogs.php?postID=1206&rf=2012-02-27-eg>.

Johnson, Deborah G., and Keith Miller. Computer ethics: analyzing information technology. Upper Saddle River, N.J.: Prentice Hall, 2009. Print.

Levy, Steven. "hacker." Webopedia. N.p., n.d. Web. 15 Oct. 2013. <http://www.webopedia.com/term/h/hacker.html>.

Moore, Robert. Cybercrime: investigating high-technology computer crime. Newark, N.J.: LexisNexis/Matthew Bender, 2005. Print.

Nissenbaum, Helen. "Protecting Privacy in an Information Age: The Problem of Privacy n Publlic." nyu.edu. N.p., n.d. Web. 14 Nov. 2013. <http://www.nyu.edu/projects/nissenbaum/papers/privacy.pdf>.

Thomas, Douglas. Hacker culture. S.l.: Univ Of Minnesota Press, 2003. Print.

Wilhelm, Thomas. Professional penetration testing creating and operating a formal hacking lab. Rockland, Mass.: Syngress Press, 2010. Print.