Joran Beasley
CS 383
Ethics Paper

Ethical Issues in Software Engineering

In this paper I will explore ethical issues that we as software developers face. I will base the bulk of the paper on the code of ethics set forth by the ACM (Association for Computing Machinery), as I believe that it is a fairly broad set of standards that covers most ethical dilemmas that we may end up encountering. I will attempt to add depth to some of the more relevant sections by relating them to contemporary events and people. I argue largely that there is no black or white with ethics, but varying shades of grey.

Section one of the ACM code of ethics covers general ethical guidelines the things I would consider largely common sense, however a large number of corporate entities violate these guidelines to varying degrees. Contribute to society and human well-being, the first of this section, is actually rather vague as it is a sliding scale that differs largely from person to person, as a person I would consider weapons R & D to go against this principle however a great many corporations do weapons systems and weapon R & D. I would consider much of the monitored police state to also be contrary to this, however there again are many companies that do research into eavesdropping techniques and technologies. However the concept that these activities are harmful to society at large is almost entirely subjective, a person at the opposite end of the political spectrum would likely view these activities as falling well within the scope of article 1.1. The second article in this section reads Avoid Harm to others, which is similar to article 1.1, but slightly different. When a large corporation like Microsoft drives a smaller corporation like Go out of business I would argue that causes pain to others, and I would say that this article is less ambiguous than article 1.1 , as I doubt anyone could argue that a large corporation driving out a smaller one does not harm others. We can skip honest and trustworthy as those are fairly black and white concepts. Be fair and take action not to discriminate is also fairly straight forward and no company does this, or if they do its behind closed doors. Honor property rights including copyrights and patents, the fifth article is a valid statement, however I have heard convincing arguments that people typically pirate software that they would not buy, regardless of the ability to pirate said software, these pirates end up working for companies and suggesting company licensing for said software because they are more familiar with that technology than other similar technologies, thus driving sales. Im not sure how well that argument holds up but it sounded credible enough to me at the time. To give credit for intellectual property is important it encourages people to contribute to the open software movement.

The last two articles merit their own paragraph. Respecting the privacy of others , the seventh article is a very interesting topic, especially with the new laws enacted by the patriot act. It goes hand in hand with honoring confidentiality. In the last 6 months the United States has requested data on 4287 users, and has asked for the partial or complete removal of content

128 times. Mexico and Canada asked for fewer than 10 removals each. An average person in London appears on CCTV approximately 300 times PER DAY (in 2006, its probably more now). China has blocked large swaths of the internet, including youTube , facebook, vimeo, photobucket, and many more**.** All these are in conflict with both of these last two issues.

Section two largely deals with ethics specifically related to us as developers and designers. Strive to achieve the highest quality, effectiveness and dignity in both the process and products of professional work, the first article in section two is fairly straightforward , basically don't do a half-assed job, and don't trade your dignity for a few bucks. The second article, acquire and maintain professional competence, to me means that you must work at knowledge, and even when you have it , well then you have to throw it away(well maybe file it away is a better phrase) and learn a new skill for the changing market. Unfortunately, I see a lot of people ignore this and I see students who would rather cheat than learn, professionals who would rather stagnate in a dying language than learn a new one. Know and respect existing laws pertaining to professional work, the third article is fairly straight forward, don't do illegal stuff, if it seems marginal check it out and make sure it won't get you into to get in hot water. This article does come with the get out of jail free card of "unless you have compelling ethical cause to do so", such as the case with reporters in Burma that reported on the riots (by illegally broadcasting and smuggling footage out of the country.) To accept and provide appropriate professional review mean to tell someone if you think you know a way to improve upon they're code or concept, and likewise to always strive to learn new things from others by accepting critical review. To give thorough evaluations to computers systems including analysis of possible risks, is kinda like thinking before you act, just think about possible ramifications or problems that could arise. To Honor contracts and assigned responsibilities is just what it sounds like do what you say and say what you'll do. To improve public understanding of computing and its consequences , encourages openness and dialog both with peers and the public. It is our responsibility as forerunners to teach others about computing, and how to protect themselves as well as how to utilize the technology to improve their lives. The final article in section two, Access computing and communication resources only when authorized to do so, is directly related to hacking. I agree to an extent, I think white hat hackers who access the system without authorization just to see if they can, and then notify said sysadmin that they have vulnerabilities and inform them of how they got access is a perfectly acceptable practice (although if caught a white hat has just as much to fear punitively as a black hat.) I think the proper response to white hat hackers is to hire them.

The third section deals mostly with organizational and leadership qualities , and ethical imperatives. Articulate social responsibilities of members of an organizational unit and encourage full acceptance of those responsibilities, is the first. This encourages management and individuals that lead teams to encourage civic responsibility and community building, and to try and get your team on board as well. Manage personal and resources to design and build systems that enhance the quality of working life, is fairly common sense and states that our projects should not make life more difficult for users/workers, and should in fact facilitate at least aspects of their work. Acknowledge and support proper and authorized uses of an organizations computing and communication resources. This article should have few rules and great subjectivity, however in a leadership position it is your job to ensure that other team

members or outside entities are not misusing the available computing resources, whether posting racial slurs on 4chan or installing trojans(even unintentionally) to grant unauthorized access, there are a multitude of monitoring and reporting tools to help facilitate this. Ensure that users and those that will be affected by a system have their needs clearly articulated during the assessment and design of requirements; later the system must be validated against said requirements. Often as designers we are given incomplete product specs, it is up to us, as designers/developers to clarify any ambiguities that may exist in the specification, and to do that we must have a dialog with the customer. And once the job is complete we should have a fairly quantifiable way to judge how complete or to spec the project was. Articulate and support policies that protect the dignity of users and others affected by a computing system. Don't sign up for jobs that you don't agree with ethically, and in this position of power, wield your power to implement policies that reinforce good ethics. Create opportunities for members of the organization to learn principles and limitations of computer systems. An employee or contractor with access to the system, but lacking the knowledge of its principles and limitations is like a bull in a coffee shop. This type of user presents a huge security hole (the largest probably) and the only way to close it is to ensure that all members with access to company systems become knowledgeable on the subject of principals/limitations/threats within a given system.

As Ive explored many of the issues directly related to the ACM code of ethics (http://www.acm.org/about/code-of-ethics), I hope it is clear to the reader that many of these points are subjective and open to interpretation, others appear almost contradictory in nature. I would expect that many of these "rules" are mostly common sense, and so I doubt knowing the wording of them would change a users behavior. However they do provide a good guideline, so that even if we don't share the same set of ethics we can all stick by ours. If we get into a questionable situation we can think back to this list and see how many tenets we break and judge the worthiness of the job from an ethical standpoint to help us decide whether or not to take it.

Interesting Ethical Links

Google Transparency Report

http://www.google.com/transparencyreport

This Shows government requests for data or to have content removed(the US is surprisingly high on the list) as well as internet traffic patterns to various google services , where a sharp drop can often signify disruptions in service whether by government intervention or maybe a cable is accidently cut.

CPSR -Computer Professionals for Social Responsibility

http://cpsr.org/

A Whole slew of interesting ethics discussions including the 10 commandments of computer ethics (http://cpsr.org/issues/ethics/cei/).

Electronic Privacy Information Center (EPIC)

http://epic.org/

Discussions and articles on privacy issues and policy.