Interaction between Ethics and Technology

Javad Shakib
College of Engineering and Information Science
DeVry University
Pomona, CA 91006
jshakib@devry.edu

David Layton
College of Liberal Arts and Sciences
DeVry University
Pomona, CA 91006
dlayton@devry.edu

Abstract—**At first glance ethics and technology seem to have no interaction. However, we see the influence of ethics on technology both from the profession and the public. For example the "code of professional ethics" has changed the procedures in different parts of science, engineering and technology, and has given a particular direction to the types of projects done, their scope, and implementations. The sensitivity of consumers to choose moral values has also resulted in the change of direction for many technologies. Public participation in science and technology and the legal channels are the other factors that shape the influence of ethics on technology.**

More controversially on the other side we see the impact of technology on ethics. One can argue how and why some of the most abstract ideas like normative ethical theories or Kantian ethics have been reactions to the advancements in science and technology. Additionally, the effects of technological change have greatly influenced modern relativistic ethics. Technology has provided new possibilities for human life and created new ethical questions too. In a sense, "applied ethics" is the product of technological development.

A different view of the ethics of science and technology is discussed and analyzed in this paper.

Keywords— Applied Ethics, Computer Ethics, Normative and Kantian Ethics, Democratic Science, Social Responsibility, Software Engineering, and cyber-crime.

I. INTRODUCTION

At first glance it seems that there is no interaction between ethics and technology. In what is often considered a definitive reflection on the topic, the historian Melvin Kranzberg famously wrote in the first of his six laws of technology: "Technology is neither good nor bad; nor is it neutral."[1]

Evolving information formats and needs require continual reconsideration of ethical principles and how these codes are applied. Considerations regarding information ethics influence "personal decisions, professional practice, and public policy" [2]. Therefore, ethical analysis must provide a framework to take into consideration "many, diverse domains" regarding how information is distributed.

978-1-4799-4992-2/14/$31.00 ©2014 IEEE

This paper will discuss and analyze a different view of the ethics of science and technology. The aim of normative ethics of science is to develop an ethical theory to determine which scientific activities should be regarded as ethically questionable. Apart from general moral and legal considerations, to this end the "aim of science" should be taken into account. Our justification for judging the conduct of some science as unethical is not a conflict between science and general moral or legal obligations, but the conflict between this or that proposed aim of science and ethical justification of a scientific aim.

Normative means conforming to a standard or ideal. Thus, scientific method can be normative whenever an action or proposition is said to conform or not to conform to scientific method. In ethics, normative statements come in the form of "should" or "ought." Normative claims are non-scientific in themselves in that empirical evidence alone rarely justifies an ethical judgment. Much of the action of ethical judgment is purely logical. Because what ought to be done is the result of a logical process using empirical evidence, but may not itself be empirical, one must separate "ought" from "is."

In ethics, empirical evidence provides *grounds*, but is not the origin of an ethical decision. A typical normative ethical statement in electrical engineering might be "The power consumption should not be designed in a way that damages the environment," with environmental preservation being the ideal that the engineer should obtain. Thus, normative ethical statements assume the *value* of the ideal as grounds for ethical behavior. In the example statement, there is an assumed value in environmental preservation that is higher or more important than providing power to the project is in itself.

In the second part of the paper, however, it will be argued that there is a subtler connection between ethics and science. The main part or case study is to stress the importance of ethics in the field of software engineering and certain areas that should be of concern in software engineering. As a result, given the threats of cyber-crime, plus the morality and ethical approaches that a Software Engineer can take to prevent and possibly counteract software malpractices, we will depict and demonstrate what decisions an Engineer must make, and the ability to differentiate between the good and evil of software applications.

The first ground for normative ethics is *morality*, or what is commonly understood to be right and proper within a given culture. In this sense, *culture* refers not just to national or ethnic identity, but to any self-identified group with rules and laws for proper conduct within that group. Thus, an engineer might refer the ethics of a matter to the ideals and laws of the United States, but also might refer to the common practices, rules, and guidelines used by the society of electrical engineers.

Given that morality may not provide clear answers in all cases requiring an ethical decision, and that morality may fail to work in novel situations, one may refer to other normative principles for clarity. The Principle of Utility can effectively answer many questions left ambiguous by common morality. The fundamental question of utility is "whom does this action benefit and/or harm?" Fundamentally, an action is ethical by utilitarian standards when it either spreads benefits or mitigates harm. The software engineer embarking upon a new program can start by trying to determine the benefits of the program. Whom does it help? Whom does it harm? What are the benefits? What are the harms? Are the benefits greater than the harms? A program may halt cybercrime dead, but if the cost of doing so is complete surrender of personal privacy for all users of the internet, would the program's benefits be greater than the harm?

In scientific and technological endeavors, the standards for scientific reasoning, the so-called "scientific method," also provides a normative value for determining the ethicality of a scientific aim. Using the standards of scientific reasoning is not merely a methodological choice, but also an ethical one. Admittedly, normativity of scientific objectivity, unlike scientific honesty, cannot be justified on the basis of general moral or legal obligations. Nevertheless, when used appropriately, scientific reasoning clarifies the aims of any scientific or technological process.

One can argue to the contrary, that if the "anything goes" slogan is the guiding principle of methodology, then defining ethics of science, in the above-mentioned sense, is impossible. However, true scientific methodology is never an "anything goes" proposition. In practice, scientific reasoning reduces egocentric thinking, the source of many bad decisions that would occur if "anything goes" were the norm. Scientific reasoning determines that the aim of the project has a clear scientific justification and/or useful application separate from the personal desires and needs of the experimenter or engineer and thus operates as an ethically normative value.

II. What is Computer Ethics?

Although it is easy to discuss ethics in philosophy and sociology, it is not completely clear what the content should be for the computer science profession. A computer scientist does not develop theories of ethics or study the ways that people deal with values. Indeed ethics and values aren't the subjects which are normally addressed by computer science; nevertheless, they form an area in which we evaluate and interpret our professional actions.

James H. Moore, who defined Computer Ethics for the first time, has defined it as the analysis of the social impact of computer technology and formulation of its ethical policies [3]. However, it is believed that this term was first coined by Dr. Walter Maner, a professor at Bowling Green State University [4].

Differentiating between terms such as ethics, morals, and values is not necessarily required while we are exposing computer ethics to discussion. The important issue is that considering ethics for the field of Computer Professionals is not an inconsequential component, but instead should be viewed as a critical part of computer vocation.

The emphasis should basically be on the social aspect of ethical affairs, since social and human discourse is actually the root of action assessment that provides a distinction between ethical and unethical decision making in each science and technology profession including computer fields.

Although an individual facet of ethics is also required in addition to its social aspect for choosing the right and ethical option between different alternatives, it is essential to provide a public moral background for people via teaching methods and patterns in order to make computer engineers ethical professionals.

III. Assessments of our Professional Actions

There is a variety of assessment communities in which the actions of every scope of science would be compared, evaluated and judged via a numerous standards and measures. Now to assess computer profession from the ethics point of view, we also need specific standards. According to Bynum et al. [5], the vision of the NCCV conference was: "To integrate computer technology and human values in such a way that the technology advances and protects those values rather than doing damage to them." This could be a good measure of a success in ethics facet of computer science. Actions are assessed in terms of being ethical, independent of the actor via pre developed standards.

IV. Scope of Ethical Action

We should consider what actions have both concerns simultaneously, the technological advancement and the ethical facet. On one hand, from an ethical standpoint, technological advancement should protect human values while improving computer technology. Everyone understands that there are things that are right and things that are wrong to do, and normally each person can independently choose between them. Everyone also accepts that we should do the right thing even when we might not want to. Another problem is that although everyone understands the distinction between right

and wrong actions, there is no absolute and general agreement on just what actions belong to which classification.

Numerous disputes and controversies have occurred over the years on this issue among various ethnic, cultural, religious or political groups of people, which has led to wars and conflicts in history. On common points there is public agreement between them in trivial right actions like helping others. However, computer technology has now entered a phase when just about any development should be seen as no longer having just trivial consequences.

For years, many hard efforts have been done to produce a standard code of ethics, but there is no universal ethics that could be generalized to all. Indeed, ethics is a relative subject not a definite one.

V. Measures and standards

Being a right action is not enough to make an action ethical, so it is not a good measurement. In fact, ethics becomes meaningful for right actin in the social and public domain, not necessarily in the personal domain. For example, we do not consider an unhealthy diet as unethical, even though it is an unjust act towards one's body. Ethics is related to others' rights and others' interests. Subjects such as privacy, security, ownership and fair access fall under the domain of ethics because these issues are amongst people of concern in the public domain.

Consequences of actions are often ignored. Ethical obliviousness could be a key sign of bad behavior. For example, the social efficacies of the programs we write mustn't be relinquished. But, social efficacy alone would not be a good measurement. For example, the harmful consequences of computer technology wrongly applied to agriculture are definitely not unethical where the computer programmer is concerned because nobody is responsible for the scope which is outside of his viewable area.

Another view of ethics in a technoscience field such as computer programming would come from the profession itself. According to Gordana Dodig-Crnkovic [7], Professional codes of ethics should be understood as conventions between professionals. Dr. Singh, Dr. Chaudhary and Dr. Panwar stated in their book named Human Values & Professional Ethics that a decisive set of ethical standards has been developed by the Association for Computing Machinery. The body of this code of ethics qualifies behavior of the computer professionals and defines their responsibilities for the effects of computer technologies they are producing and working with. There is also another standard for ethics generated by the British Computer Society that includes both a code of conduct and a code of practice. Another code was conducted by Uniform Computer Information Transactions Act (CITA), in which its ethical measurements are related to legality; however, it does not fully cover computer ethics. [5]

VI. Education

In addition to the need to pre-define standards and codes of ethics in computer professions, there is also the need for having good skills in managing critical situations and making decisions immediately. According to Bynum et al [5], we always find ourselves "thrown" into acting and the evaluations of ethics normally apply to these actions in addition to those actions where we deeply consider and think perfectly.

According to White & Pooch [8] when considering computer ethics, there are two wings: we should pay attention to both those who develop software and those who use it. A general failure in this area is that not enough time in the training of computer and programming engineers goes into considering the relationship between the developer and the user.

A very important ethical issue which educators around the world should deal with in a good manner is the misuse of intellectual property. Jerry Crystal, technology coordinator at Carmen Arace Middle School in Bloomfield, Connecticut, has a good idea in the field of education. He believes that in such cases, the issue must be personally relevant and to do this, students should be asked to work on a web site where they are really its constructors and provide intellectual properties with online access to others. Then, a fruitful discussion would be conducted about how they would feel if somebody violated the copyright law and their work were copied by someone else without their authorization.

Walter Maner illustrates two global main aspects of Computer ethics education and explains six levels of justifications for the study of computer ethics for these two views. [4] He lists them from weaker to stronger as following:

- We should study computer ethics because doing so will make us behave like responsible professionals.
- We should study computer ethics because doing so will teach us how to avoid computer abuse and catastrophes.
- We should study computer ethics because the advance of computing technology will continue to create temporary policy vacuums.
- We should study computer ethics because the use of computing permanently transforms certain ethical issues to the degree that their alterations require independent study.
- We should study computer ethics because the use of computing technology creates, and will continue to create, novel ethical issues that require special study.

- We should study computer ethics because the set of novel and transformed issues is large enough and coherent enough to define a new field.

Further, As Ben-Jacob, M. G. contended, the courses addressing this issue are prevalent on the graduate level and he believes it should be promulgated at the undergraduate level of education. He also presented a beneficial model that could be applied to easily achieve this purpose. [9]

VII. Social Responsibilities of Computer Professionals

All social and moral aspects of each issue must be completely investigated and then the clients must be aware of all these aspects. So as computer experts, we should unconditionally be honest and initially let the client know all detailed ethical components about the product or service that has been provided for them.

Even here there may arise some situations where the action seems ethical but could have a negative repercussion. These marginal subjects must also be covered in the initial interactive meeting with the client.

To have the sense of responsibility of all repercussions of the actions, an individual should get a wide range of understanding of his or her action's outcomes at a large scale. Such growth could be obtained via ethical education and be emphasized through professional organizations that have computer ethical concerns and visions.

Mental or intellectual property (IP) as a product of the mind is a sort of ownership and must be protected as other kinds of properties that are naturally protected, and specialized property right policies applied to it. Computer software resultants and productions are forms of intellectual properties, too, and should be respected as such.

Each action that is included in the immoral act classification should be also categorized as wrong when using a computer to do it. i.e. using a computer to steal, using a computer to damnify people, or using others' computer resources without their permission.

VIII. Examples

Typically an entry level programmer mainly focuses on creating code that can compile and get the job done. They do not tend to emphasize security, performance, and runtime bugs that can have damaging effects on the user's hardware. Normally, a beginner should value the work that has been previously created and all of the discoveries that have led to where we are currently today. It is not a beginner's ethical fault to fail to deliver quality software at first. We should focus on awareness and directly demonstrate the limitless power that Software Engineering contains, especially when it comes to controlling hardware. Anything that is written and uploaded to the internet will be exposed to many users, and professionals should think clearly about the kinds of use to which such material could be put.

How do we control and protect those users? As Software Engineers it is our responsibility to flag and report unstable software. Beginners are somewhat of concern and should be mentored into the right direction.

The skills that come with the territory of software engineering can be beneficial to society as we have seen the powerful applications being built today to make our lives easier. Software is getting more interesting; almost every profession depends on specific applications to carry out their daily functions. For example, a mechanic can run specific software that talks to a car and graphically gives him an overview of what to repair. This can improve the performance of the shop or it can cause it to fail. Given that the repair shop is dependent on this software, it would be too easy for their techs not to know any other troubleshooting methods. Additionally, we can suppose that a healthcare device that uses an interface to alert the caring nurse when a person is not breathing can be of critical value in life and death situations. However, its value extends only to the degree that the healthcare professional can use the device. A clumsy or confusing design in either hardware or software could in such a situation cost a life. It is apparent, then, that software can become a serious issue when it affects health, money, or everyday life.

Money is of great concern and it is very important that product users keep their information safe. Today we are faced with the era of modern technology crooks, who can take credit card information and accounts to steal and commit fraud. According to dailytech.com, hackers use tools such as SQL injections and malware to get into servers and leave backdoors open. This is troubling and can cause people to lose trust both in the internet and using credit cards. [10]

The following corporations were affected by this hacking scheme [10]:

- NASDAQ
- 7-Eleven, Inc.
- Carrefour SA (EPA:CA) (a French clothing retailer)
- J.C. Penney Comp., Inc. (JCP)
- Hannaford Bros. Comp.
- Heartland Payment Systems
- The Wet Seal, Inc. (WTSL)
- Verifone Systems Inc.'s (PAY) Commidea
- Dexia SA (ETR:DXB)
- JetBlue Airways Corp. (JBLU)
- Dow Jones
- Euronet Worldwide, Inc. (EEFT)
- Visa Inc.'s (V) Jordan subsidiary
- Global Payments Inc. (GPN)

- Diners Club Singapore
- Ingenicard U.S. Inc.

These companies above lost an average of $300M USD. The hackers were caught [10]. However, people suffered irreversible damages as they were exposed to the vulnerability of computer information to identity theft. Computer software, scripts, and other routes taken by unethical hackers can become catastrophic if the software community stays quiet and allows for the development of these spying tools that one can easily find on Linux distributions.

Software has proven to be both helpful and dangerous at the same time. It all depends on who is actually employing the right methodologies. Therefore, what exactly should we do in order to prevent misuse and enrich an ethical approach to what we consider to be the right measures? Although it will be nearly impossible to prevent software corruption, unethical practices always tend to drive the legal system into making more laws. Unfortunately, since few in the legal system are experts in computer programming, more laws are not always helpful and can, in fact, make the situation worse. The guidance of the professional community is critical in this endeavor, which is a major reason for development of a clear, intelligible, and practicable set of ethical guidelines. Most of the rules being broken are due to limited regulation. Although the internet is being monitored, there are still many changes we need to make to our practices in software engineering.

ACKNOWLEDGMENT

The first author would like to thank Juan Rodriguez for his contribution.

REFERENCES

[1] M. Kranzberg, Technology and History: “Kranzberg's Laws”, Technology and Culture, Vol. 27, No. 3,1986, pp. 544-560

[2] E. Elrod and M. Smith, “Information Ethics”, in Encyclopedia of Science, Technology, and Ethics, ed. by Carl Mitcham. Vol. 2: D-K , 2005, pp. 1004-1011

[3] J. Moor, “Metaphilosophy 1”, 1985, pp.266-275

[4] Science and Engineering Ethics, volume 2, number 2, April, 1996, pages pp. 137-154.

[5] Terrell Ward Bynum, Walter Maner, and John L. Fodor, “Proceedings of the first National Conference on Computing and Values”, 1991,

[6] P. Singh, R. Chaudhary, P. Human, “Values & Professional Ethics”, First Edition, 2010, Krishna Prakashan Media publication.

[7] Gordana Dodig-Crnkovic, “On the Importance of Teaching Professional Ethics to Computer Science Students”, In Computing and Philosophy, E-CAP 2004, Pavia, Italy, 2005.

[8] Gregory B. White, Udo W. Pooch, , “ECA '94 Proceedings of the conference on Ethics in the computer age”, Texas A&M University, 1994, pp. 170-173

[9] M. G. Ben-Jacob , “Integrating Computer Ethics across the Curriculum: A Case Study, Educational Technology & Society”, 8 (4), 2005, pp. 198-204.

[10] J. Mick, J. (). “Five charged in largest financial hacking case in u.s. history”. Retrieved from http://www.dailytech.com/Five Charged in Largest Financial Hacking Case in US History/article32050.htm , 2013