

CSE 4201

Ethical Issues and Professional Practice in Computing

University of Guyana
Lecturer: Muriana McPherson
Semester 2: 2018/2019

Some Ethical Issues

- ▶ How do I as a software developer/designer decide what is and what is not ethical professional behaviour?
- ▶ if you write a program, and an error causes an accident - who is liable?
- ▶ Is Internet bringing people together, or they are isolated as they all sit in front of their computers?
- ▶ How is Google built - what's "inside" and how do they make money?
- ▶ What is the difference between security and privacy?
- ▶ Does anonymization protect your data?
- ▶ Should software be free (linux?) or for sale (Microsoft?)
- ▶ What is digital divide?
- ▶ Are future technologies (nanotechnology, robotics) potentially dangerous?

What is Ethics?

- ▶ A set of beliefs about right and wrong behavior within a society (Reynolds)
- ▶ **The story of morality (Tavani)**
- ▶ Ethical behavior conforms to generally accepted norms—many of which are almost universal.
- ▶ **Morality** refers to social conventions about right and wrong that are so widely shared that they become the basis for an established consensus
- ▶ Your moral principles are statements of what you believe to be rules of right conduct.

The Importance of Integrity

- ▶ A person who acts with integrity acts in accordance with a personal code of principles.
- ▶ Acting with integrity is one of the cornerstones of ethical behaviour.
- ▶ Unfortunately, consistency can be difficult to achieve, particularly when you are in a situation that conflicts with your moral standards.
- ▶ Another form of inconsistency emerges if you apply moral standards differently according to the situation or people involved.
- ▶ To be consistent and act with integrity, you must apply the same moral standards in all situations.

Ethical Theories

- ▶ Concerned with establishing logically coherent and consistent criteria in the form of standards and rules for evaluating moral problems.
- ▶ It informs our analysis of moral issues.
- ▶ Consider this question:
 - ▶ Should proprietary information in a digital format e.g. MP3 files, electronic text books, be allowed to be exchanged freely over the Internet?
- ▶ An important consideration for an ethical policy is that it protects the rights of individuals, irrespective of the happiness that might or might not result for the majority of Internet users.

Introduction to Computer Ethics

- ▶ An examination of Moral, Legal and Social issues in Computing (cyber-technology)
- ▶ Applied Ethics examines the impact that cyber-technology has for our social, legal, and moral systems.
- ▶ Evaluates the social policies and laws that we frame in response to issues generated by the development and use of cyber-technology.

What is Cyber-technology?

- ▶ refers to a wide range of computing and communications devices
 - from standalone computers, to "connected" or networked computing and communications technologies, to the Internet itself.
- ▶ include:
 - digital electronic devices;
 - networked computers (including servers, desktops, laptops, etc.);
 - stand-alone computers.

Cyber-Ethics

- ▶ According to Tavani (2013), *Cyber-Ethics* is a more accurate term than *computer ethics*
- ▶ *computer ethics*, suggest the study of ethical issues limited either to:
 - a) computing machines,
 - b) computing professionals.
- ▶ Tavani (2013) also posit that *Internet ethics*, is limited only to ethical issues affecting (only) networked computers and devices. Hence Cyber-ethics is a more accurate term to use.

Evolution of Cyber-technology & Cyber-Ethics - 4 phases

- ▶ Phase 1: (1950s and 1960s) consisted mainly of huge mainframe computers that were unconnected (i.e., stand-alone machines).
- ▶ Ethical/social questions that arose dealt with
 - ▶ the impact of computing machines as “giant brains” and what that meant for being human.
 - ▶ privacy threats and the fear of Big Brother.

Phase 2: (1970s and 1980s),

- ▶ computing machines and communications devices began to converge.
- ▶ Mainframe computers and personal computers could be linked together via privately owned networks, which generated three kinds of ethical/social issues:
 - 1) *privacy* concerns (introduced in Phase 1) were exacerbated because confidential information could easily be exchanged between networked databases.
 - 2) *intellectual property* issues emerged because personal computers could easily be used to duplicate and exchange proprietary software programs.
 - 3) *computer crime* emerged because “hackers” could break into the computers of large organizations.

Phase 3: (1990-present)

- ▶ the availability of Internet access to the general public has increased significantly.
- ▶ This has been facilitated by the phenomenal growth of the World Wide Web.
- ▶ The proliferation of Internet- and Web-based technologies in this phase has raised ethical and social concerns affecting:
 - free speech,
 - anonymity,
 - jurisdiction.

Phase 4: (present to near future),

- ▶ “Web 2.0” has made possible the proliferation of social networking sites (SNSs), such as Facebook and Twitter.
- ▶ As cyber-technology continues to evolve in Phase 4, computers will likely become more and more a part of who or what we are as human beings.
- For example, Moor (2005) notes that computing devices will soon be a part of our clothing, and even our bodies.
- ▶ Computers are already becoming *ubiquitous*, and are beginning to “pervade” both our work and recreational environments.
- ▶ Objects in these environments already exhibit what Brey (2005) calls “ambient intelligence,” which enables “smart objects” to be connected via wireless technology.

Phase 4

- ▶ Computers are becoming *less visible* as distinct entities, as they:
 - a) continue to be miniaturized and integrated into ordinary objects,
 - b) blend unobtrusively into our surroundings.
- ▶ Cyber-technology is also becoming *less distinguishable* from other technologies as boundaries that have previously separated them begin to blur because of convergence.

Evolution of Cyber-technology & Cyber-Ethics

- ▶ Additional ethical/social concerns associated with Phase IV include controversies that are made possible by the following kinds of technologies:
- ▶ autonomous machines and sophisticated robots (used in warfare, transportation, care for the elderly, etc.);
- ▶ nanocomputing and nano-scale devices;
- ▶ artificial agents (including “soft bots”) that act on behalf of humans and corporations;
- ▶ AI-induced bionic chip implants (that can cause us to question what it means to be human vs. cyborg).

Scenario: Are Any Cyber-ethics Issues Unique Ethical Issues?

Megan Meier, a 13-year-old resident of Dardenne Prairie, Missouri, had an account on MySpace where she received a “friend” request from a user named Josh Evans. Evans, who claimed to be a 16-year-old boy, told Meier that he lived near her and was being home-schooled by his parents. At first, Evans sent flattering e-mails to Meier, which also suggested that he might be romantically interested in her. Soon, however, Evans’s remarks turned from compliments to insults, and Evans informed Meier that he was no longer sure that he wanted to be friends with her because he heard that she “wasn’t very nice to her friends.” Next, Meier noticed that some highly derogatory posts about her—e.g., “Megan Meier is a slut” and “Megan Meier is fat”—began to appear on MySpace.

Meier, who was reported to have suffered from low self-esteem and depression, became increasingly distressed by the online harassment (cyberbullying) being directed at her—i.e., from both the insulting MySpace postings and hurtful e-mail messages she continued to receive from Evans. On October 17, 2006, Meier decided to end her life by hanging herself in her bedroom. An investigation of this incident, following Meier’s death, revealed that Josh Evans was not a teenage boy; she was Lori Drew, the 49-year-old mother of a former friend of Meier’s.

Ethical concerns that arise in the cyberbullying scenario.

- ▶ Should Lori Drew, as well as any other MySpace user, have been permitted to open an account on that social networking site (SNS) under an alias or pseudonym that also included a fictitious profile?
- ▶ Should MySpace, or any SNS, tolerate members who deceive, intimidate, or harass other users?
- ▶ Should users who create accounts on SNSs with the intention to deceive or harass others be subject to criminal prosecution?
- ▶ Should MySpace have been held legally liable, at least in some contributory sense, for Meier's death?
- ▶ Do ordinary users of an SNS who discover that someone is being bullied in that online forum have a moral responsibility to inform the SNS?
- ▶ Do they also have a moral responsibility to inform that SNS if they discover that someone has created a fraudulent account on their forum, which could be used to deceive and harass other members?

Uniqueness of Cyber-ethics Issues

- ▶ There are two points of view on whether cyber-technology has generated any new or unique ethical issues:
 1. *Traditionalists* argue that nothing is new - crime is crime, and murder is murder.
 2. *Uniqueness Proponents* argue that cyber-technology has introduced (at least some) new and unique ethical issues that could not have existed before computers.

The Uniqueness Debate

- ▶ Both sides seem correct on some claims, and both seem to be wrong on others.
- ▶ Traditionalists underestimate the role that issues of *scale* and *scope* that apply because of the impact of computer technology.
- For example, cyberbullies can bully multiple victims simultaneously (scale) and globally (because of the scope or reach of the Internet).
- Cyberbullies can also operate without ever having to leave the comfort of their homes.

The Uniqueness Debate

- ▶ Those who defend the Uniqueness thesis tend to overstate the effect that cyber-technology has on ethics per se.
- ▶ Maner (2004) correctly points out that computers are uniquely fast, uniquely malleable, etc.
- ▶ So, there may indeed be some *unique aspects of computer technology*.

The Uniqueness Debate

- ▶ Proponents of the uniqueness thesis tend to confuse *unique features of computer technology* with *unique ethical issues*.
- ▶ Their argument is based on a logical fallacy:
Premise. Cyber-technology has some unique technological features.
Premise. Cyber-technology generates some ethical issues.
Conclusion. (At least some of the) Ethical issues generated by cyber-technology must be unique.

The Uniqueness Debate

- ▶ Traditionalists and uniqueness advocates are each partly correct.
- ▶ Traditionalists correctly point out that *no new ethical issues* have been introduced by computers.
- ▶ Uniqueness proponents are correct in that cyber-technology has complicated our analysis of traditional ethical issues.

The Uniqueness Debate

- ▶ So, in analyzing the issues involved in this debate, it is useful to distinguish between any:
 - unique technological features;
 - (alleged) unique ethical issues.

Scenario: Developing the Code for a Computerized Weapon System

Sally Bright, a recent graduate from Technical University, has accepted a position as a software engineer for a company called CyberDefense, Inc. This company has a contract with the U.S. Defense Department to develop and deliver applications for the U.S. military. When Sally reports to work on her first day, she is assigned to a controversial project that is developing the software for a computer system designed to deliver chemical weapons to and from remote locations. Sally is conflicted about whether she can, given her personal values, agree to work on this kind of weapon delivery system, which would not have been possible without computer technology.

- ▶ Is the conflict that Sally faces in this particular scenario one that is new or unique because of computers and cyber-technology?
- ▶ Consider that long before computing technologies were available, engineers were confronted with ethical choices involving whether or not to participate in the design and development of certain kinds of controversial technological systems.
- ▶ Is the fact that certain technological systems happen to include the use of computer software or computer hardware components morally relevant in this scenario?
- ▶ Have any new or unique ethical issues, in a nontrivial sense of “unique,” been generated here?

Discussion Question

- a) computer professionals responsible for designing the software code for a controversial computer system;
 - b) ordinary users making unauthorized copies of proprietary software.
- Are any of the ethical issues that arise in either scenario unique ethical issues?

Alternative Strategy for Analyzing the Uniqueness Issue

- ▶ Moor (2000) argues that computer technology generates “new possibilities for human action” because computers are *logically malleable*.
- ▶ Logical malleability in computers means that they can be molded in ways that allow for many different kinds of uses.
- ▶ Some of the unanticipated uses of computers have introduced *policy vacuums*.

Policy Vacuums and Conceptual Muddles

- ▶ Policy vacuums are “voids” or gaps in our laws and policies.
- ▶ One solution might seem simply to fill the voids with new or revised policies.
- ▶ Some policy vacuums cannot easily be filled because of *conceptual muddles*.
- ▶ In these cases, conceptual muddles first need to be elucidated before clear policies can be formulated and justified.

Scenario: Digital Piracy

Harry Flick is an undergraduate student at Pleasantville State College. In many ways, Harry's interests are similar to those of typical students who attend his college. But Harry is also very fond of classic movies, especially films that were made before 1950.

DVD copies of these movies are difficult to find; those that are available tend to be expensive to purchase, and very few are available for loan at libraries. One day, Harry discovers a Web site that has several classic films (in digital form) freely available for downloading. Since the movies are still protected by copyright, however, Harry has some concerns about whether it would be permissible for him to download any of these films (even if only for private use).

Discussion Question

Is Harry's ethical conflict one that is unique to computers and cyber-technology?

Are the ethical issues surrounding Harry's situation new and thus unique to cyber-technology?

- ▶ In the early 1980s, there were still no clear laws regarding the duplication of software programs, which had been made easy because of the availability of personal computers.
- ▶ Because there were no clear rules for copying programs, a policy vacuum arose.
- ▶ Before the policy vacuum could be filled, a conceptual muddle had to be elucidated: What, exactly, is software?

Cyber-ethics as a Branch of Applied Ethics

- ▶ Three distinct perspectives of applied ethics (as applied to cyber-ethics):
 - Professional Ethics;
 - Philosophical Ethics;
 - Sociological/Descriptive Ethics.

Perspective # 1: Cyber-ethics as a Branch of Professional Ethics

- ▶ According to this view, the purpose of cyber-ethics is to identify and analyze issues of ethical responsibility for computer/information technology (IT) professionals.
- ▶ Consider a computer professional's role in designing, developing, and maintaining computer hardware and software systems.
- ▶ Suppose a programmer discovers that a software product she has been working on is about to be released for sale to the public, even though it is unreliable because it contains “buggy” software.
- ▶ Should she “blow the whistle”?

Professional Ethics

- ▶ Gotterbarn (1995) has suggested that computer ethics issues are *professional ethics* issues.
- ▶ Computer ethics, for Gotterbarn, is similar to medical ethics and legal ethics, which are tied to issues involving specific professions.
- ▶ He notes that computer ethics issues aren't, strictly speaking, about technology per se.
- For example, he point out that we don't have automobile ethics, airplane ethics, etc.

Some Criticisms of the Professional Ethics Perspective

- ▶ Is Gotterbarn's model for computer ethics too narrow for cyber-ethics?
- ▶ Consider that cyber-ethics issues affect not only computer professionals; they effect virtually everyone.
- ▶ Before the widespread use of the Internet, Gotterbarn's professional-ethics model may have been adequate.

Perspective # 2: Philosophical Ethics

- From this perspective, cyber-ethics is a field of philosophical analysis and inquiry that goes beyond professional ethics.
- Moor (2000) defines computer ethics as:
...the analysis of the nature and social impact of computer technology and the corresponding formulation and justification of policies for the ethical use of such technology.

Philosophical Ethics Perspective (continued)

- ▶ Moor argues that automobile and airplane technologies did not affect our social policies and norms in the same kinds of fundamental ways that computer technology has.
- ▶ Automobile and airplane technologies have revolutionized transportation, resulting in our ability to travel faster and farther than was possible in previous eras.
- ▶ But they did not have the same impact on our legal and moral systems as cyber-technology.

Philosophical Ethics: Standard Model of Applied Ethics

- ▶ Brey (2004) describes the “standard methodology” used by philosophers in applied ethics research as having three stages:
 - 1) Identify a particular controversial practice *as* a moral problem.
 - 2) Describe and analyze the problem by clarifying concepts and examining the factual data associated with that problem.
 - 3) Apply moral theories and principles to reach a position about the particular moral issue.

Perspective #3: Cyber-ethics as a Field of Sociological/Descriptive Ethics

- ▶ The professional and philosophical perspectives both illustrate *normative* inquiries into applied ethics issues.
- ▶ Normative inquiries or studies are contrasted with *descriptive* studies.
- ▶ Descriptive (and sociological) investigations report about “What *is* the case.”
- ▶ Normative inquiries evaluate situations from the vantage-point of the question: “What *ought to be* the case?”.

Sociological/Descriptive Ethics Perspective (continued)

- ▶ Suppose that a new technology, *Technology X*, displaces 8,000 workers in Community Y.
- ▶ If we analyze the issues solely in terms of their sociological dimension, including the number of jobs that were gained or lost in that community, our investigation would be essentially descriptive in nature.

Some Benefits of Using the Sociological/Descriptive Approach

- ▶ Huff and Finholt (1994) claim that when we understand the descriptive aspect of social effects of technology, the normative ethical issues become clearer.
- ▶ The descriptive/sociological perspective can prepare us for our subsequent (normative) analysis of the ethical issues that affect our system of policies and laws.

A "Disclosive" Method for Cyber-ethics

- ▶ Brey (2004) believes that because of embedded biases in cyber-technology, the standard applied-ethics methodology is not adequate for identifying cyber-ethics issues.
- For example, Brey notes that we might fail to notice certain features embedded in the *design* of cyber-technology.
- Using the standard model, we might also fail to recognize that certain *practices* involving cyber-technology can have moral implications.

Disclosive Method (Continued)

- ▶ Brey points out that one weakness of the “standard method of applied ethics” is that it tends to focus on *known* moral controversies
- ▶ So, that model fails to identify practices involving cyber-technology which have moral implications but that are not yet known.
- ▶ Brey refers to these practices as having *morally opaque* (or *morally non-transparent*) features, which he contrasts with “morally transparent” features.

A Multi-Disciplinary and Multi-Level Method for Cyber-ethics

- ▶ Brey's disclosive method is *multidisciplinary* because it requires the collaboration of:
 - computer scientists,
 - philosophers,
 - social scientists.
- ▶ Brey's scheme is also *multi-level* because the method for conducting computer ethics research requires three levels of analysis, i.e., a:
 - *disclosure level*,
 - *theoretical level*,
 - *application level*.

A Three-step Strategy for Approaching Cyber-ethics Issues

Step 1. Identify a practice involving cyber-technology, or a feature in that technology, that is controversial from a moral perspective.

1a. Disclose any hidden (or opaque) features or issues that have moral implications

1b. If the ethical issue is descriptive, assess the sociological implications for relevant social institutions and socio-demographic and populations.

1c. If the ethical issue is also normative, determine whether there are any specific guidelines, that is, professional codes that can help you resolve the issue

1d. If the normative ethical issues remain, go to Step 2

Step 2. Analyze the ethical issue by clarifying concepts and situating it in a context.

2a. If a policy vacuum exists, go to Step 2b; otherwise go to Step 3

2b. Clear up any conceptual muddles involving the policy vacuum and go to Step 3.

Step 3. Deliberate on the ethical issue. The deliberation process requires two stages:

3a. Apply one or more ethical theories to the analysis of the moral issue, and then go to step 3b.

3b. Justify the position you reached by evaluating it against the rules for logic/critical thinking

Groups of 5 Discussion Exercise

Below is a list of 6 controversial issues or practices involving cyber-technology that has not yet been identified as an ethical issue, but which might eventually be recognized as one that has moral implications.

- ▶ Data Collection and Privacy: <http://reillytop10.com/previous-lists/2013-list/data-collection-and-privacy/>
 - ▶ Autonomous Systems: <http://reillytop10.com/previous-lists/2013-list/autonomous-systems/>
 - ▶ 3-D Printing: <http://reillytop10.com/previous-lists/2013-list/222-2/>
 - ▶ Driverless Zipcars: <http://reillytop10.com/previous-lists/2013-list/driverless-zipcars/>
 - ▶ Hacking Into Medical Devices: <http://reillytop10.com/previous-lists/2013-list/hacking-into-medical-devices/>
 - ▶ Predictive Policing: <http://reillytop10.com/previous-lists/2014-list/predictive-policing/>
1. Apply Brey's "disclosive method" to see whether you can isolate any embedded values or biases affecting that practice.
 2. Apply the "comprehensive strategy" for approaching cyber-ethics that we examined in the previous slide