CSCI 2070 Introduction to Ethics/Cyber Security

Amar Rasheed
Course Information

Course Objectives:

- Introduce students to cyberethics: concepts, perspectives, and methodological Frameworks
- Present ethical concepts and ethical theories
- Address the required tools for evaluating cyberethics issues
- Introduce the students to professional ethics, codes of conduct, and moral responsibility
- Introduce students to the fundamental knowledge of computer security
Course Information

Learning Objectives

- Students will be able to learn a variety of ethical frameworks and relate them to arising ethical issues in Cyberspace
- Students will be able to address issues involving free speech, privacy, and intelligence property in Cyberspace
- Students will be able to address system security issues and their impact on individuals, organizations, and society
- Demonstrate written communication skills
- Students will learn the basic concepts in computer security including software vulnerability analysis and defense, and applied cryptography
Course Information

Prerequisites:
- ENG1102 and either CSCI 1301 or ITEC 1310

Recommended Text Books:

Recommended Reading:
Course Contents

Course Content:

- **Part I- Introduction to Information Security, Law & Ethics**
  - Introduction to Cyberethics: Concepts, Perspectives, and Methodological Frameworks
  - Ethical Concepts and Ethical Theories
  - Tools for Evaluating Cyberethics issues
  - Professional Ethics, Codes of Conduct, and Moral Responsibility
  - Security in Cyberspace
  - Cybercrime and Cyber-Related Crimes
  - Intellectual Property Disputes in Cyberspace
  - Privacy and Cyberspace

- **Part II- Introduction to Applied Crypto Cryptography**
  - Introduction to Applied Crypto
  - Classic Cryptography
  - Symmetric Key Cryptography
  - Public Key Cryptography

- **Access Control**
  - Authentication
Homeworks and Late Policy

Homeworks & quizzes
Homeworks will be announced via Email and will be given at least a week before the due date. Quizzes will be announced in advanced. There will be a total of three homeworks and 8 quizzes during this course.

Late Policy:
The deadline for any assignment can be extended with a 20% penalty per day. No deadline can be extended by more than 24 hours. All Assignments, quizzes, exams, and term paper have to be submitted through eclassroom. Any email submission will NOT be accepted.
Introduction to Cyberethics: Concepts, Perspectives, and Methodological Frameworks

- Introduce some foundational concepts and methodological frameworks for the analysis of Cyberethics issues.

- We will define two keys terms:
  - Cyberethics
  - CyberTechnology
Introduction to Cyberethics: Concepts, Perspectives, and Methodological Frameworks

- Four development phases in cyberTechnology:
  - Phase I (1950s and 1960s)
  - Phase II (1970s and 1980s)
  - Phase III (1990s-present)
  - Phase IV (Present-near future)

- Uniqueness of cyberethics?
- Three different Perspectives for approaching and identifying cyberethics issues

  - Professional Ethics
  - Philosophical Ethics
  - Sociological/Descriptive Ethics
Scenario 1: “The Washingtonienne Blogger”

Jessica Culter, a former staff assistant to U.S. Senator Michael DeWine (R-Ohio), authored an online diary (on blogger.com) under the Pseudonym “The Washingtonienne.” In May 2004 she was fired when the contents of her diary appeared in the Wonkette: The DC Gossip, a popular blog in the Washington D.C. area. Until her diary was discovered and published in Wonkette, Culter assumed that it had been viewed by only a few of her fellow “staffers” who were interested in reading about the details of her romantic relationships and sexual encounters. In her diary, Culter disclosed that she earned an annual salary of only $25,000 as a staffer and that most of her living expenses were thankfully subsidized by few generous older gentlemen. She also described some details of her sexual relationships with these men, one of whom was married and an official in the Bush administration.
In January 2003, a United States district court in the District of Columbia ruled that Verizon (an internet service provider or ISP) must comply with a subpoena by the Recording Industry Association of America (RIAA)—an organization that represents the interests of the recording industry. The RIAA, in an effort to stop the unauthorized sharing of music online, requested from Verizon the names of two of its subscribers who allegedly made available more than 600 copyrighted music files on the Internet. Although many ISPs, such as Comcast, and many Universities complied with similar subpoenas issued on behalf of RIAA, Verizon refused to release the names of any of its subscribers. Verizon argued that doing so would violate the privacy rights of its subscribers and would violate specific articles of the U.S. Constitution.
Scenario 3: “A Cyberstalking Incident”

In October 1999, Twenty-year-old Amy Boyer was murdered by a young man who had stalked her via the Internet. The stalker, Lim Youens, was able to carry out most of the stalking activities that eventually led to Boyer’s death by using a variety of and resources tools generally available to any internet user. Via standard online search facilities, for example, Youens, was able to gathered personal information about Boyer. And after paying a small fee to Docusearch.com, an online information company, Youens was able to find out where Boyer lived, where she worked, and so forth. Youens was also able to use another online tool, available to Internet users, to construct two Web sites, both dedicated to his intended victim. On one site, he posted personal information about Boyer as well as photograph of her. On the other Web site, Youens described, in explicit detail, his plan to murder Boyer.
Jessica Culter, a former staff assistant to U.S. Senator Michael DeWine (R-Ohio), authored an online diary (on blogger.com) under the Pseudonym “The Washingtonienne.” In May 2004 she was fired when the contents of her diary appeared in the Wonkette: The DC Gossip, a popular blog in the Washington D.C. area. Until her diary was discovered and published in Wonkette, Culter assumed that it had been viewed by only a few of her fellow “staffers” who were interested in reading about the details of her romantic relationships and sexual encounters. In her diary, Culter disclosed that she earned an annual salary of only $25,000 as a staffer and that most of her living expenses were thankfully subsidized by few generous older gentlemen. She also described some details of her sexual relationships with these men, one of whom was married and an official in the Bush administration.
A wide range of ethical issues was arise in the Verizon and recording industry:

- Privacy and Surveillance
- Anonymity and civil liberties
- Property and ownership

In January 2003, a United States district court in the District of Columbia ruled that Verizon (an internet service provider or ISP) must comply with a subpoena by the Recording Industry Association of America (RIAA)- an organization that represents the interests of the recording industry. The RIAA, in an effort to stop the unauthorized sharing of music online, requested from Verizon the names of two of its subscribers who allegedly made available more than 600 copyrighted music files on the Internet. Although many ISPs, such Comcast, and many Universities complied with similar subpoenas issued on behalf of RIAA, Verizon refused to release the names of any of its subscribers. Verizon argued that doing so would violate the privacy rights of its subscribers and would violate specific articles of the U.S. Constitution.
Ethical Issues in “A Cyberstalking Incident”

- A wide range of ethical issues was arise in the cyberstalking Incident:
  - Privacy and security
  - Free speech
  - Moral responsibility and legal liability

In October 1999, Twenty-year-old Amy Boyer was murdered by a young man who had stalked her via the Internet. The stalker, Lim Youens, was able to carry out most of the stalking activities that eventually led to Boyer’s death by using a variety of and resources tools generally available to any internet user. Via standard online search facilities, for example, Youens, was able to gathered personal information about Boyer. And after paying a small fee to Docusearch.com, an online information company, Youens was able to find out where Boyer lived, where she worked, and so forth. Younes was also able to use another online tool, available to Internet users, to construct two Web sites, both dedicated to his intended victim. On one site, he posted personal information about Boyer as well as photograph of her. On the other Web site, Youens described, in explicit detail, his plan to murder Boyer.
What Is Cyberethics?

- Cyberethics is the study of moral, legal, and social issues involving cybertechnology.
- It examines the impact that cybertechnology has for our social, legal, and moral systems.
- It also evaluates the social policies and laws that have been framed in response to issues generated by the development and use of cybertechnology.
What Is Cybertechnology?

- *Cybertechnology* 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.

- Hand-held devices (such as Palm Pilots, tablets), personal computers (desktops and laptops), mainframe computers, and so forth.
Cybertechnology (Continued)

- Networked devices can be connected directly to the Internet.
- They also can be connected to other devices through one or more privately owned computer networks.
- Privately owned networks include both Local Area Networks (LANs) and Wide Area Networks (WANs).
Why the term Cyberethics?

- Example of key terms that examine moral, legal and social ethical issues associated with cyber technology:
  - Computer Ethics
  - Information Ethics
  - Internet Ethics
  - Cyberethics

- *Cyberethics* is a more accurate label than *computer ethics*, which might suggest the study of ethical issues limited to computing machines, or to computing professionals.
Why the term Cyberethics?

- **Information ethics**: Refer to the study of ethical concerns regarding the flow of information that is restricted computer technology.
  - Ambiguous: It can mean a specific methodological framework (IE)
  - Study ethical concerns that is restricted to professionals in the field of Library science and Information science
- It is more accurate than *Internet ethics*, which is limited only to ethical issues affecting computer networks.
Development Phases of Cyber Technology

- Phase 1 (1950s and 1960s) consisted mainly of:
  - Mainframe computer

- Ethical issues:
  - The impact of computing machine as “giant Brain”
  - Privacy threats and the “big Brother”
Development Phases of Cyber Technology

- Phase 2 (1970s and 1980s) consisted mainly of:
  - Computing machine and Communication devices

- Ethical issues:
  - Personal Privacy
    - Example: electronic records stored large government and commercial database
  - Intellectual property
    - Software copying
  - Computer Crimes
    - Computer terminals that can be used to hack into the computer system of large organization
Phase 3 (1990s - present) consisted mainly of:
  - Internet era

Ethical issues:
  - Free speech
  - Jurisdiction
    - No geographical boundaries in cyberspace
  - Trust
    - E-commerce
  - Public vs. Private
    - Personal information included on social networking media (e.g. Facebook)
Development Phases of Cyber Technology

- Phase 4 (present – Near future) consisted mainly of:
  - Convergence of information and Communication technologies, biotechnology and nanotechnology

- Ethical issues:
  - Concerns about AI and decision-making capabilities
# Table 1-1: Summary of Four Phases of Cyberethics

<table>
<thead>
<tr>
<th>Phase</th>
<th>Time Period</th>
<th>Technological Features</th>
<th>Associated Issues</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1950s-1960s</td>
<td>Stand-alone machines (large mainframe computers)</td>
<td>Artificial intelligence (AI), database privacy (&quot;Big Brother&quot;)</td>
</tr>
<tr>
<td>2</td>
<td>1970s-1980s</td>
<td>Minicomputers and PCs interconnected via privately owned networks</td>
<td>Issues from Phase 1 plus concerns involving intellectual property and software piracy, computer crime, privacy and the exchange of records.</td>
</tr>
<tr>
<td>3</td>
<td>1990s-Present</td>
<td>Internet and World Wide Web</td>
<td>Issues from Phases 1 and 2 plus concerns about free speech, anonymity, legal jurisdiction, virtual communities, etc.</td>
</tr>
<tr>
<td>4</td>
<td>Present to Near Future</td>
<td>Convergence of information and communication technologies with nanotechnology research and genetic and genomic research, etc.</td>
<td>Issues from Phases 1-3 plus concerns about artificial electronic agents (&quot;bots&quot;) with decision-making capabilities, implantable chips,</td>
</tr>
</tbody>
</table>