

ETHICS AND PROFESSIONALISM OF EMERGING TECHNOLOGIES

Chapter 6

Introduction

- Emerging technologies driving and shaping our life, that means technology has its definite effects on our lifestyle, and it can also bring new risks.
- In this chapter, the connection of emerging technologies with professional ethics, privacy, accountability, trust, threats, and challenges of emerging technologies will be discussed.
- A proper understanding of the ethics of emerging technology presupposes a proper understanding of what emerging technologies are.

What are Professional Ethics?

- Professional ethics are a code of conduct that govern how members of a profession deal with each other and with third parties
- It is a field of applied ethics concerned with moral issues that impact technology users.
- Professional ethics includes relationships with and responsibilities toward customers, clients, coworkers, employees, employers, others who use one's products and services, and others whom they affect

Professionalism

- A profession means practice or application of such knowledge and skill that are acquired through a systematic study or training for the betterment of the society or people in the form of services.
- A professional has a responsibility to act ethically or bear moral and ethical behavior.
- Many professions have a code of ethics that professionals are expected to abide by
- The content of profession with moral and ethical behaviors is professionalism.

Code of Ethics

- A written set of guidelines issued by an organization to its workers and management to help them conduct their actions in accordance with its primary values and ethical standards.
- A Sample IT code of Ethics from SANS org:
 - I respect privacy and confidentiality.
 - I will not steal property, time or resources.
 - I will reject bribery or kickbacks and will report such illegal activity.

Some Examples

- ACM Code of Ethics and Professional Conduct.
 - <http://www.acm.org/constitution/code.html>
- British Computer Society Code of Conduct
- IEEE-CS/ACM Software Engineering Code of Ethics and Professional Practice
 - <http://www.computer.org/tab/seprof/code.htm>

Why should we have a Professional Code of Ethics?

- Software has the potential to do good or cause harm, or to enable or influence others to do good or cause harm.
- Defines and promotes a standard for external relations with clients and employers.
- Protects the group's interests.
- Codifies members' rights.
- We want to protect our livelihood.

Examples of un-professional behavior

- **Personal Integrity:** Hiding conflict of interest, Disclosing client's confidential information, Inconsistency in saying and doing (hypocrite), Inability to make appropriate judgment in a particular situation.
- **Criminal offense:** Forging document, Falsifying data, Accepting/offering bribes, Abuse/misuse/disuse of authority, Plagiarism.
- **Negligence:** not doing something that a reasonable person would do, or doing something that a reasonable person would not do
- **Professional malpractice:** professionals who breach the duty of care are liable for injuries that their negligence causes

Common Ethical Issues for IT Users

- Software piracy
- Inappropriate use of computing resources
 - Erodes productivity and wastes time
 - Could lead to lawsuits
- Inappropriate sharing of information, including:
 - Every organization stores vast amounts of private or confidential data
 - Private data (employees and customers)
 - Confidential information (company and operations)

Supporting the Ethical Practices of IT Users

- Policies that protect against abuses:
 - Set forth general rights and responsibilities of users
 - Create boundaries of acceptable behavior
 - Enable management to punish violators
- Policy components include:
 - Establishing guidelines for use of company software
 - Defining appropriate use of IT resources
 - Structuring information systems to protect data and information
 - Installing and maintaining a corporate firewall

1. Technology and ethics

- The emergence of new technologies raises some new challenges for the profession to address
- Technology can serve to promote or restrict human rights.
- Technology ethics are increasingly important because the risks associated with inappropriate behavior have grown in number, complexity, likelihood, and significance.
- Ethics is a Set of beliefs about right or wrong behavior
- Ethics is a reasoning process designed to explore and answer questions about a proposed course of action that take the form “Is that a good idea?”

1. Technology and ethics

- Ethics is the study of standards of right and wrong
- Ethics is particularly important for the accountancy profession, with a code for professional ethics based on five basic principles – integrity, objectivity, competence and due care, confidentiality, and professional behavior.
- Eg. doctors know what the ethics of their profession dictate. A doctor will never divulge patient's medical history to anyone other than the patient himself, unless authorized by the later, or required under law to do so.

2. New ethical questions

- The increasing use of big data, algorithmic decision-making, and artificial intelligence can enable more consistent, evidence-based and accurate judgments or decisions, often more quickly and efficiently.
- However, outputs can be based on biased data, which could lead to discriminatory outcomes.
- Systems learn from real-world data, there is a significant risk that those systems simply recreate the past and subsequently build in errors or systemic biases.
 - This can be beneficial for many, others can lose out, and outcomes can again seem unfair or unethical.

General ethical principles

1. Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
2. Avoid harm.
3. Be honest and trustworthy.
4. Be fair and take action not to discriminate
5. Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.
6. Respect privacy.
7. Honor confidentiality

Professional responsibilities

1. Strive to achieve high quality in both the processes and products of professional work.
2. Maintain high standards of professional competence, conduct, and ethical practice.
3. Know and respect existing rules pertaining to professional work.
4. Accept and provide appropriate professional review.
5. Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risk

Professional responsibilities

6. Perform work only in areas of competence.

7. Foster public awareness and understanding of computing,

related technologies, and their consequences.

8. Access computing and communication resources only when authorized or when compelled by the public good.

9. Design and implement systems that are robustly and useably secure

Professional leadership principles

1. Ensure that the public good is the central concern during all professional computing work.
2. Articulate, encourage acceptance of and evaluate fulfillment of social responsibilities by members of the organization or group.
3. Manage personnel and resources to enhance the quality of working life.
4. Articulate, apply, and support policies and processes that reflect the principles of the Code.

Professional leadership principles

5. Create opportunities for members of the organization or group to grow as professionals.
6. Use care when modifying or retiring systems. Interface changes, the removal of features, and even software updates have an impact on the productivity of users and the quality of their work.
7. Recognize and take special care of systems that become integrated into the infrastructure of society.

3. Digital privacy

- Digital Privacy is the protection of personally identifiable or business identifiable information that is collected from respondents through information collection activities or from other sources.
- The protection of the information of private citizens who use digital mediums.
- It is a collective definition that encompasses three sub-related categories;
 - information privacy, communication privacy, and individual privacy

Information Privacy

- **Information privacy** is the protection of customers or individuals and their personal information.
- Many companies collect employee and customer information as a part of their business procedures.
 - financial, family, credit, and educational information,...
- Due to the access of this sensitive information, the public and congress have implemented information privacy laws.
 - Organizations must have a purpose for the information that is collected, get rid of information that is no longer needed.
 - Companies can't share information with third parties unless consent is given, information has to be accurate and customers must have the ability to review the information that is discovered

Communication Privacy

- Electronic communication: Is a transfer of signs, signals, writing, images, sounds, data or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo-electric, or photo-optical system that affects interstate .
- **Illegal for any “person” to “intentionally intercept” the “content” of any “wire . . . or electronic communication” and to disclose or use any illegally intercepted communication**
- Private right of action also possible—damages, punitive damages, attorney fees
- No exclusionary rule for illegally intercepted electronic communication

Individual Privacy

- Individual privacy is the notion that individuals have a right to exist freely on the internet,
 - They can choose what types of information they are exposed to, and unwanted information should not interrupt them like receiving unwanted ads and emails/spam, or a computer virus that forces the user to take actions they otherwise wouldn't.
 - In such cases the individual, during that moment, doesn't exist digitally without interruption from unwanted information; thus, their individual privacy has been infringed upon.

Some digital privacy principles

- The Privacy Task Force considered international regulatory privacy requirements and industry best practices to develop the privacy guidance.
- Generally Accepted Privacy Principles (GAPP). The GAPP consists of ten privacy principles. The privacy principles are listed and summarized below:
 - **Management.** The entity defines, documents, communicates, and assigns accountability for its privacy policies and procedures.
 - **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained, and disclosed.

Some digital privacy principles

- The privacy principles are listed and summarized below:
 - **Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use, and disclosure of personal information.
 - **Collection.** The entity collects personal information only for the purposes identified in the notice.
 - **Use, retention, and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent.
 - **Access.** The entity provides individuals with access to their personal information for review and update.

Some digital privacy principles

- The privacy principles are listed and summarized below:
 - **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.
 - **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).
 - **Quality.** The entity maintains accurate, complete, and relevant personal information for the purposes identified in the notice.
 - **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy related complaints and disputes.

4. Accountability and trust

- Understanding and mitigating them will help to build confidence.
- Often legal and regulatory frameworks haven't kept pace with digital transformation, and organizations are seeking guidance.
- This challenge is exacerbated by the speed at which technological change is occurring and the breadth of its adoption – which is introducing new risks that demand new responses

5. Threats and challenges

- While we enjoy the conveniences brought by new emerging technologies, there are also challenges and threats ahead such as security concerns, governance dilemmas
- As security professionals, we need to keep pace with ever-changing technology and be aware of the AI, IoT, Big Data, Machine Learning, etc.

Ethical and regulatory challenges

- With Growing needs Cyber & Data Security is getting prominence that requires security practitioners to focus on the business need for securing data, understanding security and risk from a business perspective by extensively interacting with the business community in understanding their requirements or what they want.
- The most prevalent ethics concerns overall were related to informed consent, privacy and confidentiality, and data sharing.

Emerging technologies impact include:

1. Counter-terrorism and law enforcement informatics via predictive analytics and artificial intelligence.
2. Real-time horizon scanning and data mining for threats and information sharing
3. Automated cybersecurity and information assurance
4. Enhanced Surveillance (chemical and bio-detection sensors, cameras, drones, facial recognition, license plate readers)
5. Simulation and augmented reality technologies for training and modeling

Emerging technologies impact include:

6. Safety and security equipment (including bullet and bomb proof) made with lighter and stronger materials
7. Advanced forensics enabled by enhanced computing capabilities (including future quantum computing)
8. Situational awareness capabilities via GPS for disaster response and crisis response scenarios
9. Biometrics: assured identity security screening solutions by bio-signature: (every aspect of your physiology can be used as a bio-signature. Measure unique heart/pulse rates, electrocardiogram sensor, blood oximetry, skin temperature)
10. Robotic Policing (already happening in Dubai!)

Challenges in using Artificial Intelligence

- As machines become more “intelligent” they could begin to replace experts in higher-level jobs.
- Building Trust
- AI Human Interface
- Investment: it is expensive that not every business man invest money
- Software Malfunction:
- AI Can't Replace Every Task
- Higher Expectations
- Not all people support
- Data Privacy and security
- Algorithm bias

Challenges in using Robotics in manufacturing

- The potential for humans losing jobs is great here too
- As automation technologies become more advanced, there will be a greater capability for automation to take over more and more complex jobs.
- As robots learn to teach each other and themselves, there is the potential for much greater productivity but this also raises ethical and cybersecurity concerns

Challenges in using the Internet of Things

- As more and more connected devices (such as smartwatches and fitness trackers) join the Internet of Things (IoT) the amount of data being generated is increasing.
- There are also severe security implications of mass connectivity that need to be addressed.
- Security
- Privacy
- Reliability
- Resource Consumption

Challenges in Big Data

- Although data can be incredibly useful for spotting trends and analyzing impacts, surfacing all this data to humans in a way that they can understand can be challenging.
- Insufficient understanding and acceptance of big data
- Variety of big data technologies
- Complexity of managing data quality
- Big data security holes
- process of converting big data into valuable insights

Threats

- New and emerging technologies pose significant threats and questions not only to business but to society as a whole.
 1. Threat to Sustainable Development
 2. Threats from Health-related Technologies
 3. Surrogate Mother Technique and Threat to Kinship Norms
 4. High Efficiency Weaponry and Threat to Life
 5. Threats from Agricultural Technologies
 6. Threats from Genetically Modified Food
 7. Biotechnology and Threat to Human Society
 8. Science and Ethics
 9. Technology's Disruptive Potential

Risks of emerging technology are:

- Driverless car: while a compelling option for future fleet cars, companies could crash and burn from claims related to bodily injury and property damage.
- Wearables: Google glass, Fitbit and other wearables can expose companies to the invasion of privacy claims that may not be covered by general liability or personal injury claims that weren't foreseen.
- Drones: Turbulence is in the offing for manufacturers and organizations that fail to protect themselves for property damage and bodily injury, as well as errors and omissions.
- Internet of things: The proliferation of sensors and cross-platform integration creates potential exposure from privacy invasion, bodily injury and property damage that may connect an organization to huge liabilities.

Threats to Online Privacy

- More Widespread Tracking
 - Companies like Facebook running the internet's largest advertising networks use tracking to collect user data. The more smart devices you use, the more ways these companies have to collect your information.
- Government Surveillance
 - Authoritarian governments around the world are some of the worst offenders for tracking their citizen's internet activity. If these governments are able to continue their privacy-invasive tracking, privacy on a global scale may remain a distant reality.

How To Stay More Private on The Internet

- Use A Private Search Engine
- Use Search Encrypts Private Search Engine
- Use Privacy Based Extensions
 - **Privacy Badger**
 - **Ghostery**
 - **Blur**
 - **Privacy Cleaner**
 - **Search Encrypt**
- Use VPNs

END