
More Quick Notes, Telegram: @campus_handout / https://t.me/campus_handout

Chapter 6: ETHICS AND PROFESSIONALISM OF EMERGING TECHNOLOGIES

6.1. Technology and ethics

- As with many technological advances, however, the Internet has not been without negative aspects
 - ✓ it has created new concerns about privacy
 - ✓ It has been hampered by spam and viruses
 - ✓ it threatens to cut off people who lack access to it
- Technology can serve to promote or restrict human rights
- Information Society should foster the use of emerging technologies in such a way as to maximize the benefits that they provide while minimizing the harms
- 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

➤ professional behavior

- emergence of new technologies raises some new challenges for the profession to address

6.2. New ethical questions

- increasing use of big data, algorithmic decision-making, and artificial intelligence strengths can potentially have a darker side too
- outputs can be based on biased data, which could lead to discriminatory outcomes
- there is a significant risk that those systems simply recreate the past and subsequently build in errors or systemic biases
- Closely linked to discrimination is personalization, and the impact of tailoring decisions very specifically to individuals, based on preferences, activities and other features
 - ✓ this can be beneficial for many, others can lose out, and outcomes can again seem unfair or unethical
- Whatever the power of the machine, humans will still need to be involved, so that people
 - can be held accountable, or
 - explain the reasons behind a decision
- A central problem of the ethics of technology is that it tends to arrive too late
 - ✓ Ethics can then become a tool to clean up a mess that might have been avoidable

- ✓ Indeed, there are ethical theories and approaches that explicitly aim at an early integration of ethics into the technology life cycle
 - One central problem of this type of approach is that **the future is unknown**
 - Ethics has traditionally not been well equipped to deal with issues of uncertainty and, in particular, future uncertainty

6.2.1. 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**

6.2.2. 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 risks
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 usably secure

6.2.3. 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
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

6.3. Digital privacy

- is **protection of personally identifiable or business identifiable information**
 - ✓ information is collected from respondents through information collection activities or from other sources
- encompasses three sub-related categories
 - **information privacy**
 - **communication privacy**
 - **individual privacy**
- It is often used in contexts that promote advocacy on behalf of individual and consumer privacy rights in digital spheres
 - ✓ typically used in opposition to the business practices of many e-marketers/companies to collect and use such information and data

6.3.1. Information Privacy

- is the notion that **individuals should have the freedom, or right, to determine how their digital information mainly that pertaining to personally identifiable information, is collected and used**
- Every country has various laws that dictate how information may be collected and used by companies
 - ✓ Some of those laws are written to give agency to the preferences of individuals/consumers in how their data is used

6.3.2. Communication Privacy

- is the notion that **individuals should have the freedom, or right, to communicate information digitally with the expectation that their communications are secure**

- ✓ messages and communications will only be accessible to the sender's original intended recipient
- communications can be intercepted or delivered to other recipients without the sender's knowledge, in a multitude of ways
 - intercepted directly through various hacking methods
 - Communications can also be delivered to recipients unbeknownst to the sender due to false assumptions made regarding the platform or medium which was used to send information
 - companies frequently have been known to lack transparency in how they use information, this can be both intentional and unintentional

6.3.3. 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
 - ✓ unwanted information should not interrupt them
 - An example of a digital breach of individual privacy would be an internet user receiving unwanted ads and emails/spam, or a computer virus that forces the user to take actions they otherwise wouldn't

6.3.4. Some digital privacy principles

➤ Data Minimization

- ✓ collect the minimal amount of information necessary from individuals and businesses consistent with the Department's mission and legal requirements

➤ Transparency

- ✓ Information collected will not be used for any other purpose **unless authorized or mandated by law**

➤ **Accuracy**

- ✓ Information collected will be maintained in a **sufficiently accurate, timely, and complete manner** to ensure that the interests of the individuals and businesses are protected

➤ **Security**

- ✓ physical and IT security measures will be implemented to ensure that the collection, use, and maintenance of identifiable **information are properly safeguarded and the information is promptly destroyed in accordance with approved records control schedules.**

6.4. Accountability and trust

- **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
- the very solutions that can be used to better manage risk, increase transparency and build confidence are often themselves the source of new risks, which may go unnoticed
- **There's a danger that the use of technology will degrade people's willingness to judge and intervene** because they feel that they are less personally

connected to consumers and consumer outcomes – the logic of the machine has taken over from individual responsibility

- The obligation of an individual or organization to account for its activities, accept responsibility for them, and to disclose the results in a transparent manner

6.5. Treats and challenges

6.5.1. Ethical and regulatory challenges

- With Technology moving at a fast pace it is always been a **challenge for Security**
- 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
- Emerging technologies are also changing how we approach, plan, and integrate security operations
- Emerging technologies are making an impact include:
 - Counter-terrorism and law enforcement informatics
 - Real-time horizon scanning and data mining
 - Automated cybersecurity and information assurance
 - Enhanced Surveillance
 - Simulation and augmented reality technologies
 - Safety and security equipment
 - Advanced forensics
 - Situational awareness capabilities via GPS

- Biometrics: assured identity security screening solutions by bio-signature
- Robotic Policing

6.5.1.1. Challenges in using Artificial Intelligence

- AI is only as good as the data it is exposed to
 - ✓ How a business teaches and develops its AI will be the major factor in its usefulness
 - ✓ Humans could be the weak link here, as people are unlikely to want to input masses of data into a system
- AI has potential to replace human workers
 - ✓ replace experts in higher-level jobs
 - ✓ Alternatively, AI also has the potential to take the burden of laborious and time-consuming tasks from these people, freeing up their time and brainpower for other things

6.5.1.2. Challenges in using Robotics in manufacturing

- 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

6.5.1.3. Challenges in using the Internet of Things

- As result of more connected devices the amount of data being generated is increasing

- Companies will have to plan carefully how this will affect the customer-facing application and how to best utilize the masses of data being produced
- There are also severe security implications of mass connectivity that need to be addressed

6.5.1.4. 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

6.5.2. Treats

- New and emerging technologies also pose risks
- Some **risks of emerging technology** are:
 - Driverless car
 - ✓ claims related to **bodily injury and property damage**
 - Wearables
 - ✓ 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

- ✓ 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