EmTc1012

CHAPTER 6

ETHICS AND PROFESSIONALISM OF EMERGING TECHNOLOGIES

Outline

The following topics will be covered

- Introduction
- Technology and ethics
- New ethical questions
- Digital privacy
- Accountability and trust
- Threats and challenges

Objectives

After accomplishing this chapter, Students will be able to:

- Distinguish the link between ethics and technology.
- Understand general, professional and leadership ethical questions.
- Explain what digital privacy is, its components and why it is important.
- know the importance of accountability and trust in emerging technologies.
- Identify the threats and challenges we face in developing

Technology and Ethics

Technology and ethics

- The Internet boom has provided many benefits for society, allowing the creation of new tools and new ways for people to interact.
- 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.*

✓ *Moreover, even as it serves as a medium for communication across the globe, it threatens to cut off people who lack access to it.*

Technology and ethics

Con't ...

- 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.

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

General Ethical principles

Ethical rules:

- Contribute to ***society*** and to ***human well-being***, acknowledging that all people are stakeholders in computing.
- ***Avoid harm.***
- ***Be honest and trustworthy.***
- ***Be fair and act not to discriminate.***
- Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.
- ***Respect privacy.***
- ***Honor confidentiality***

General ethical principles

Professional responsibilities:

- ***Strive*** to achieve high quality in both the processes and products of professional work.
- ***Maintain*** high standards of professional competence, conduct, and ethical practice.
- ***Know*** and ***respect*** existing rules pertaining to professional work.
- ***Accept*** and ***provide*** appropriate professional review.

General ethical principles

Professional responsibilities.

- Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
- Perform work only in areas of competence.
- Foster public awareness and understanding of computing, related technologies, and their consequences.
- Access computing and communication resources only when authorized or when compelled by the public good.
- Design and implement systems that are robustly and usably secure

General ethical principles

Professional leadership principles.

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

General ethical principles

Professional leadership principles.

- Create opportunities for members of the organization or group to grow as professionals.
- 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.
- Recognize and take special care of systems that become integrated into the infrastructure of society.

Digital privacy

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.

It Contains:

- *Information privacy,*
- *Communication privacy, and*
- *Individual privacy*

Information privacy

Information privacy,

- 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.

Communicatio n Privacy

Communication privacy

Communication privacy: 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.

- ✓ meaning that messages and communications will only be accessible to the sender's original intended recipient.

Individual Privacy

Individual privacy

Individual privacy : individual privacy is the notion that individuals have a right to exist freely on the internet, in that they can choose what types of information they are exposed to, and more importantly that 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,

Digital privacy

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:*** Notice covering the purpose of the collection and use of identifiable information will be provided in a clear manner.

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

Digital privacy

Some digital privacy principles

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

Accountability and trust

Con’t …

- 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. It also includes the responsibility for money or other entrusted property.

Threats and challenges

- With Technology moving at a fast pace it is always been a challenge for Security.
- As security professionals, we need to keep pace with ever-changing technology and be aware of the AI, IoT, Big Data, Machine Learning, etc.

- **Emerging technologies are making an impact include:**
  - Counter-terrorism and law enforcement informatics via predictive analytics and artificial intelligence.
  - Real-time horizon scanning and data mining for threats and information sharing
  - Automated cybersecurity and information

Threats and challenges

an impact include: Cont...

- Enhanced Surveillance (chemical and bio-detection sensors, cameras, drones, facial recognition, license plate readers)
- Simulation and augmented reality technologies for training and modeling.
- Safety and security equipment (including bullet and bomb proof) made with lighter and stronger materials.
- Advanced forensics enabled by enhanced computing capabilities (including future quantum computing)
- Situational awareness capabilities via GPS for disaster response and crisis response

Threats and challenges

Emerging technologies are making an impact include: Con’t …

- 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)
- Robotic Policing (already happening in Dubai!)

Threats and challenges

Challenges in using Artificial Intelligence (AI)

- With automation and robotics moving from production lines out into other areas of work and business, 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.

Threats and challenges

Challenges in using the Internet of Things (IoT)

- 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.

- 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.

Threats and challenges

Challenges in Big Data

- Almost all the technologies mentioned above have some relation to Big Data.

- The huge amount of data being generated daily has the potential to provide businesses with better insight into their customers as well as their own business operations.

- 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. AI will play a role here.

Threats of ET

Threats

As they have benefits ET also have some risks.

- **Some risks of emerging technology are:**
  - Driverless car: while a compelling option for future fleer 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.

Threats of ET

Con’t …

- **Some risks of emerging technology are:**
  - 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

END OF CH-6

