

Addis Ababa University

School of Commerce

Introduction to Emerging
Technologies

Chapter Six- ETHICS AND
PROFESSIONALISM

Technology and ethics

- Ethics is – integrity, objectivity, competence and due care, confidentiality, and professional behavior.
- Technology can serve to promote or restrict human rights. The 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.
- Establishing the proper legal or regulatory system is important to reduce the effect of abusing technology rather than sharing technological benefits

Ethical questions related emerging technology

Ethics in Big data:

- 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, these strengths can potentially have a darker side too, throwing up questions around the ethical use of these fairly new technologies.
- For example, 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.

Technology and ethics

Ethics in AI:

- 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.
- Ethical issues are only recognized when the technology is already on the market and problems arise during its widespread use. Ethics can then become a tool to clean up a mess that might have been avoidable.

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,
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, and their consequences.

Professional leadership principles

1. Ensure that the public good is the central concern during all professional work.
2. Articulate, encourage acceptance and evaluate fulfillment of social responsibilities
3. Manage personnel and resources to enhance the quality of working life.
4. Create opportunities for members of the organization to grow as professionals.
5. 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.
6. Recognize and take special care of systems that become integrated into the infrastructure of society.

Digital privacy

- It is the protection of personally identifiable or business identifiable information that is collected from respondents through information collection activities or from other sources.
- It encompasses three sub-related categories;
 1. Information privacy,
 2. Communication privacy, and
 3. Individual privacy
- It promotes advocacy on behalf of individual and consumer privacy rights in digital spheres, and is typically used in opposition to the business practices of many e-marketers/businesses/companies to collect and use such information and data.

Information Privacy

- It 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.

Communication Privacy

- It 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.
- However, communications can be intercepted or delivered to other recipients without the sender's knowledge, in a multitude of ways such as hacking.

Individual Privacy

- It 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, 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.

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.
- 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 safeguarded and the information is promptly destroyed in accordance with approved records control schedules.

Accountability and trust

- When emerging technology creates far-reaching and rapid change, it can also bring new risks. 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.
- Emerging technologies can provide improved accuracy, better quality and cost efficiencies for businesses in every sector. They can enhance trust in the organization's operations and financial processes, which is crucial for sustainable success. But this can produce a paradox: 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.

...Accountability and trust

- 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.

Ethical and regulatory challenges

Emerging technologies are already impacting how we live and work. They're also changing how we approach, plan, and integrate security operations which 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

...Ethical and regulatory challenges

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)

Challenges in using Artificial Intelligence

- AI is only as good as the data it is exposed to, which is where certain challenges may present themselves. 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 a potential to replace human workers. As machines become more “intelligent” they could begin to replace experts in higher-level jobs.
- Alternatively, AI also has the potential to take the burden of laborious and time-consuming tasks from people, freeing up their time and brainpower for other things

Challenges in using Robotics in manufacturing

- With automation and robotics moving from production lines out into other areas of work and business, the potential for humans losing jobs is greater.
- 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. 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 without compromising the individual privacy.

Challenges in Big Data

- The huge amount of data being generated on a daily basis 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.

Treats

- New and emerging technologies pose significant opportunities for businesses if they utilize them well and understand their true value early on. They also pose risks and questions not only to business but to society as a whole. Planning for how to deal with these emerging technologies and where value can be derived while assessing potential risks before they become a fully-fledged reality is essential for businesses that want to thrive in the world of AI, Big Data and IoT.

...Treats

Some risks of emerging technology are:

- Driverless car: cars could crash and burn from errors resulted 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.

...Treats

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 to huge liabilities.

END!!