

CHAPTER 6

Ethics & Professionalism of Emerging Technologies

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.
- ▮ Technology can serve to **promote or restrict human rights**.

▮ Ethics

- Set of **moral principles**.
 - Principles of conduct that guide an **individual** or **group**.
- ✓ **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.**

Con't...

- ▮ However, the emergence of **new technologies** raises some new challenges for the profession to address.
- ▮ **Ethics in technology** is a sub-field of ethics addressing the ethical questions specific to the **Technology**.
- ▮ Therefore, while you involve in different forms of technology you should have to govern based on some sort of **protocol, rule** and **regulation**. unless we lose some thing behind it.
- ▮ **Privacy**: The ability to control information about oneself.

General Ethical Principles

- ❖ 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 **take action** not to discriminate
- ❖ Respect the work required to produce new **ideas**, **inventions**, **creative works**, and **computing artifacts**.
- ❖ Respect **privacy**.
- ❖ Honor **confidentiality**

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.
- ❖ Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
- ❖ Perform work only in areas of competence.
- ❖ Promote 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 useably secure

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.
- ❖ 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**

Con't...

- Top leadership principles
 - ✓ Lead by example.
 - ✓ Leadership is about people.
 - ✓ Focus on change.
 - ✓ Be human and admit mistakes.
 - ✓ Understand the value of listening.
 - ✓ Develop leadership skills.
 - ✓ Promote diversity.
 - ✓ Work together to achieve more.
 - ✓ Have solid values.
 - ✓ Use technology and innovation.
 - ✓ Help to develop future leaders.

Digital Privacy

- **Digital privacy** refers to the **protection of an individual's information** that is used or created while using the **Internet on a computer or personal device**.
- **Digital security** is the protection of this **online identity**. **Criminals** are finding new ways to operate and steal information from digital users for their own personal gain.
- **Digital security** is an all-encompassing term which includes the tools you can use to secure your **identity, assets and technology** in the **online and mobile world**.
- Digital privacy have 3 sub-related categories:
 - ❖ Information privacy
 - ❖ Communication privacy

a. Information Privacy

- **Information privacy**, also known as **data privacy or data protection**, is the relationship between the **collection** and **dissemination** of:
 - ❖ Data
 - ❖ Technology
 - ❖ The public expectation of privacy
 - ❖ Legal and political issues surrounding them
- **Information privacy** is the idea that individuals should have the **freedom or right to determine how their digital information is collected and used.**
- This is particularly relevant for personally identifiable information.

b. 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**.

c. Individual Privacy

- 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.

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.
- ✓ **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

Accountability and Trust

- ✓ Emerging technologies can provide improved accuracy, better quality and cost efficiencies for businesses in every sector.
- ✓ Enhance Accountability and trust in the organization's operations and financial processes, which is crucial for sustainable success.
- ✓ 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.

Treats and Challenges

Ethical and regulatory challenges

- ✓ **Technology** moving at a fast pace it is always been a **challenge for Security**.
- ✓ **Emerging technologies** are already impacting how we live and work.
- ✓ They're also changing how we **approach, plan, and integrate security** operations.
- ✓ For **security**, both **physical** and **cyber**, the equation is the same catalyzing many new potential applications for emerging technologies.

Con't...

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
- ✓ Cyber security and information assurance
- ✓ Enhanced Surveillance (chemical and bio-detection sensors, cameras, drones, facial recognition, license plate readers)
- ✓ Simulation and augmented reality technologies for training and

Con't...

- ✓ **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 scenarios**
- ✓ **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

- ✓ Computing power
- ✓ Trust deficit
- ✓ Limited knowledge
- ✓ Human level
- ✓ Data privacy and security
- ✓ The bias problem
- ✓ Data scarcity

Challenges in using IoT

- ✓ Security
- ✓ lack of strong IoT regulations
- ✓ Bandwidth
- ✓ Customer expectations

Challenges in Big Data

- ✓ Insufficient **understanding** and **acceptance** of big data.
- ✓ Confusing variety of **big data** technologies.
- ✓ Paying loads of **money**.
- ✓ Complexity of **managing data quality**.
- ✓ Dangerous **big data security** holes.
- ✓ Tricky process of **converting big data** into valuable insights.
- ✓ Troubles of **up scaling**.

Treats

❖ **Treat** is a potential negative action or event facilitated by a **vulnerability** that results in an unwanted impact to a computer system or application.

Con't...

Some 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



**THANK YOU FOR YOUR CAREFUL
ATTENTION!!!!**