MOD 1: Common Ethical Theories

Ethics

- called **moral philosophy**
- the discipline concerned with what is morally good and bad and morally right and wrong.
- study of ethics dates back to ancient Greek times through the philosopher Socrates

Ethical Theories

I. Relativism

Relativism is the theory that there is no universal moral norm of right and wrong. According to this theory different individuals or groups of people can have completely opposite views or moral problem, and both can be right.

a) Subjective Relativism
- person decides right and wrong for himself/herself.
- "What's right for you may not right for me."
- e.g. Reproductive Health Bill

b) Cultural Relativism
- "right" and "wrong" rests with a society's actual moral guidelines.
- Action may be wrong in a society at one time and wrong in another society or in another time
- e.g. Capital punishment

II. Divine Command Theory

The divine command theory is based on the idea that good actions are those aligned with the will of God and bad actions are those contrary to the will of God. Since the Holy Book contains God's directions, we can use the Holy Book as moral decision-making guides.

III. Consequentialism

"The end will justify the means." In consequentialism, the consequence of an action justifies the moral acceptability of the means taken to reach that end. It is the consequence of an action which determines whether or not the action is moral. Thus rightness or wrongness of actions is definable in terms of the goodness or badness of the result.

a) Ethical egoism
- person should focus exclusively on his or her self interest.
- Action that will provide that person with the maximum long-term benefit.
- assisting another is the right thing to do if and only if it is the helper's own long-term best interest.

b) Utilitarianism
- right action is the one that produces the most intrinsic good for everyone affected.
- "the greatest happiness for the greatest number"

IV. Kantianism

Kantianism or Deontology is an obligation-based theory whose chief author was Immanuel Kant, who lived in the 18th century. This theory emphasizes the type of action rather than the consequences of that action. Deontologists believe that moral decisions should be made based on one's duties and the rights of others.

MOD2: Critical Reasoning and Moral Theory

Ethics vs Morals

- relate to “right” and “wrong” conduct.
- ethics refer to rules provided by an external source, e.g., codes of conduct in workplaces or principles in religions.
- Morals refer to an individual’s own principles regarding right and wrong.

Morality

1. descriptively to refer to certain codes of conduct put forward by a society or a group (such as a religion), or accepted by an individual for her own behavior,
2. normatively to refer to a code of conduct that, given specified conditions, would be put forward by all rational persons

Law

law tries to create a basic, enforceable standard of behavior necessary in order for a community to succeed and in which all people are treated equally. Law is narrower in focus than ethics or morality. So long as we’re fulfilling our legal obligations we can consider ourselves ‘ethical

- There are some matters the law will be agnostic on but which ethics and morality have a lot to say
  - Example: law will be useless to you if you’re trying to decide whether to tell your competitor their new client has a reputation for not paying their invoices, but our ideas about what’s good and right will still guide our judgement here.
- First, the law outlines a basic standard of behavior necessary for our social institutions to keep functioning
  - Example: it protects basic consumer rights. However, in certain situations the right thing to in solving a dispute with a customer might require us to go beyond our legal obligations.
- Secondly, there may be times when obeying the law would require us to act against our ethics or morality.
  - Example: A doctor might be obligated to perform a procedure they believe is unethical

Ethical Reasoning

Ethical reasoning is how to think about issues of right or wrong. No matter how knowledgeable one is about their profession, if the knowledge is not backed by ethical reasoning, long-term success in the career is likely to be severely compromised.

1) Recognize that there is an event to which to react.
   - Observe the situation
2) Define the event as having an ethical dimension.
   - Check if there is an ethical violation
3) Decide that the ethical dimension is significant.
   - Decide if you will intervene to the action
4) Take personal responsibility for generating an ethical solution to the problem.
   - Apply it to other’s POV to create possible solution
5) Figure out what abstract ethical rule(s) might apply to the problem (including any codes of ethics relevant to the situation).
   - Law/Rules and Regulations that is violated
6) Decide how these abstract ethical rules actually apply to the problem so as to suggest a concrete solution.
   - Apply the Law/Rules and Regulations to propose a concrete solution
7) Prepare to counteract contextual forces that might lead one not to act in an ethical manner.
   - Prepare for any consequences
8) Act
   - Take Action. In the end, what matters is not how one thinks, but rather what one does.

MOD3: Professional Code of Ethics

Professional Code of Ethics

A professional code of ethics is a set of principles designed to help professionals distinguish right from wrong in order to govern their decision-making.

Why is it important?
A professional code of ethics is designed to ensure employees are behaving in a manner that is socially acceptable and respectful of one another.

Some of these advantages are:
1. Ethical Decision Making
2. High Standards of Practice and Ethical Behavior
3. Trust and Respect from the General Public
4. Evaluation Benchmark

Examples of Code of Ethics in the IT Profession

A. The Association for Computing Machinery (ACM)
ACM brings together computing educators, researchers, and professionals to inspire dialogue, share resources, and address the field's challenges. ACM supports the professional growth of its members by providing opportunities for life-long learning, career development, and professional networking.

Guiding Members with a Framework of Ethical Conduct
The ACM Code of Ethics identifies the elements of every member's commitment to ethical professional conduct. It outlines fundamental considerations that contribute to society and human well-being and those that specifically relate to professional responsibilities, organizational imperatives, and compliance with the code.

1. GENERAL ETHICAL PRINCIPLES.

A computing professional should...
1.1 Contribute to society and to human well-being, acknowledging that all people are stakeholders in computing.
1.2 Avoid harm.
1.3 Be honest and trustworthy.
1.4 Be fair and take action not to discriminate.
1.5 Respect the work required to produce new ideas, inventions, creative works, and computing artifacts.
1.6 Respect privacy.
1.7 Honor confidentiality.

2. PROFESSIONAL RESPONSIBILITIES.

A computing professional should...
2.1 Strive to achieve high quality in both the processes and products of professional work.
2.2 Maintain high standards of professional competence, conduct, and ethical practice.
2.3 Know and respect existing rules pertaining to professional work.
2.4 Accept and provide appropriate professional review.
2.5 Give comprehensive and thorough evaluations of computer systems and their impacts, including analysis of possible risks.
2.6 Perform work only in areas of competence.
2.7 Foster public awareness and understanding of computing, related technologies, and their consequences.
2.8 Access computing and communication resources only when authorized or when compelled by the public good.
2.9 Design and implement systems that are robustly and usably secure.

3. PROFESSIONAL LEADERSHIP PRINCIPLES.

A computing professional, especially one acting as a leader, should...
3.1 Ensure that the public good is the central concern during all professional computing work.
3.2 Articulate, encourage acceptance of, and evaluate fulfillment of social responsibilities by members of the organization or group.
3.3 Manage personnel and resources to enhance the quality of working life.

3.4 Articulate, apply, and support policies and processes that reflect the principles of the Code.
3.5 Create opportunities for members of the organization or group to grow as professionals.
3.6 Use care when modifying or retiring systems.
3.7 Recognize and take special care of systems that become integrated into the infrastructure of society.

4. COMPLIANCE WITH THE CODE.

A computing professional should...
4.1 Uphold, promote, and respect the principles of the Code.
4.2 Treat violations of the Code as inconsistent with membership in the ACM.

B. The Philippine Computer Society (PCS)

The Philippine Computer Society (PCS) is the longest-existing professional association of computing and information technology professionals in the country. From its special interest groups (SIGs) have spun off today's more specialized computing and IT-related organizations, many of which have evolved into national organizations themselves.

Code of Ethics of the Filipino Computing and Information Technology Professional

PREAMBLE:

I. I will use my special knowledge and skills for the benefit of the public. I will serve employers and clients with integrity, subject to an overriding responsibility to the public interest, and I will strive to enhance the competence and prestige of the professional. By these, I mean:
II. I will promote public knowledge, understanding and appreciation of information technology;
III. I will consider the general welfare and public good in the performance of my work;
IV. I will advertise goods or professional services in a clear and truthful manner;
V. I will comply and strictly abide by the intellectual property laws, patent laws and other related laws in respect of information technology;
VI. I will accept full responsibility for the work undertaken and will utilize my skills with competence and professionalism;
VII. I will make truthful statements on my areas of competence as well as the capabilities and qualities of my products and services;
VIII. I will not disclose or use any confidential information obtained in the course of professional duties without the consent of the parties concerned, except when required by law;
IX. I will try to attain the highest quality in both the products and services I offer;
X. I will not knowingly participate in the development of Information Technology Systems that will promote the commission of fraud and other unlawful acts;
XI. I will uphold and improve the IT professional standards through continuing professional development in order to enhance the IT profession.

Computer Ethics

In the mid 1940s, **Computer Ethics** became a new branch of ethics also known as Information Ethics. Norbert Wiener, a professor of mathematics and engineering at MIT pioneered a new branch of applied science known as Cybernetics and identified the social and ethical implications of computers.

He predicted that:

- after war, the world would undergo a second industrial revolution
- automatic age with enormous potential for good and evil
- staggering number of new ethical challenges & opportunities
- effects on information technology on key human values such as life, health, happiness, abilities, knowledge, freedom, security, and opportunities

Problem in Computer Ethics

- A typical problem in Computer Ethics arises because there is a policy vacuum about how computer technology should be used. Some of these concerns are rooted in the uniqueness of Computer Ethics due to the properties of computers that raises unique issues.

Computers Special Case

I. Logical Malleability

Computers can be shaped and molded to perform any activity that can be characterized in terms of inputs, outputs and connecting logical operations.

II. Impact on Society

The extensive impact of computerization on society is clear. Naturally, in 1985, when Moor wrote his paper, relatively few could foresee the extent of that impact, nor did anyone envisage the Internet and the World Wide Web. Moor did, however, foresee the changing workplace, and the nature of work.

III. Invisibility Factor

An important fact about computers is that most of the time, and under most conditions, computer operations are invisible. Moor identifies three kinds of invisibility that can have ethical significance:

1. Invisible Abuse: the intentional use of the invisible operations of a computer to engage in unethical conduct
2. Invisible Programming Values: these are values which are embedded into a computer program.
3. Invisible Complex Calculation: Computers today perform calculations which are too complex for human inspection and understanding.

The Three Levels of Computer Ethics

a) Pop

- overall goal
- Newspapers, magazines and TV news programs have engaged increasingly in computer ethics of this sort.

b) Para

- second "level" of computer ethics
- Someone who takes a special interest in computer ethics cases, collect examples, clarifies them, looks for similarities and differences, reads related works, attends relevant events, and so on,

c) Theoretical

- third level of computer ethics
- applies scholarly theories to computer ethics cases and concepts
- not only to identify, clarify, compare and contrast computer ethics cases; she or he could also apply theories and tools from philosophy, social science or law in order to deepen our understanding of the issues.

Ten Commandments of Computer Ethics

The Ten Commandments of Computer Ethics have been a highly effective code of ethics for the proper use of information technology.

1. Thou shalt not use a computer to harm other people.

2.Thou shalt not interfere with other people's computer work.

3.Thou shalt not snoop around in other people's computer files.

4.Thou shalt not use a computer to steal.

5.Thou shalt not use a computer to bear false witness.

6.Thou shalt not copy or use proprietary software for which you have not paid.

7.Thou shalt not use other people's computer resources without authorization or proper compensation.

8.Thou shalt not appropriate other people's intellectual output.

9.Thou shalt think about the social consequences of the program you are writing or the system you are designing.

10.Thou shalt always use a computer in ways that ensure consideration and respect for your fellow humans.

MOD4: Technologies Impact to Privacy

Privacy is defined by

- Oxford
    - the state or condition of being free from being observed or disturbed by other people, or the state of being free from public attention.
- Merriam-Webster
    - the quality or state of being apart from company or observation and freedom from unauthorized intrusion.

Major reasons for the movement towards comprehensive privacy and data protection laws include:

- to remedy past injustices
- to promote electronic commerce

Threats to Privacy

The increasing sophistication of information technology with its capacity to collect, analyze and disseminate information on individuals has introduced a sense of urgency to the demand for legislation. Furthermore, new developments in medical research and care, telecommunications, advanced transportation systems and financial transfers have dramatically increased the level of information generated by each individual.

The extent of privacy invasion -- or certainly the potential to invade privacy -- increases correspondingly. Beyond these obvious aspects of capacity and cost, there are a number of important trends that contribute to privacy invasion :

- **Globalization** removes geographical limitations to the flow of data. The development of the Internet is perhaps the best known example of a global technology.
- **Convergence** is leading to the elimination of technological barriers between systems. Modern information systems are increasingly interoperable with other systems, and can mutually exchange and process different forms of data.
- **Multimedia** fuses many forms of transmission and expression of data and images so that information gathered in a certain form can be easily translated into other forms.

Technology transfer and policy convergence

New initiatives technologies will require a bold, forward looking legislative framework. Whether governments can deliver this framework will depend on their willingness to listen to the pulse of the emerging global digital economy and to recognize the need for strong protection of privacy.

privacy protection is frequently seen as a way of drawing the line at how far society can intrude into a person's affairs. It can be divided into the following facets :

- **Information Privacy**, which involves the establishment of rules governing the collection and handling of personal data such as credit information and medical records;
- **Bodily privacy**, which concerns the protection of people's physical selves against invasive procedures such as drug testing and cavity searches;
- **Privacy of communications**, which covers the security and privacy of mail, telephones, email and other forms of communication; and
- **Territorial privacy**, which concerns the setting of limits on intrusion into the domestic and other environments such as the workplace or public space.

The Technologies of Privacy Invasion

- **Identity Systems**
  - Identity Cards - linked to national registration systems
  - Biometrics - process of collecting, processing and storing details of a personís physical characteristics for the purpose of identification and authentication
- **Surveillance of Communications -**
  - Internet and email interception
  - National Security
- **Video Surveillance -** prevalence of the use of CCTV
- **Workplace Surveillance -** tracking employees movement

Privacy and Anonymity Issues

- Data Breaches
  - identity theft incidents can be traced back to data breaches involving large databases of personal information. Data breaches are sometimes caused by hackers breaking into a database, but more often than one might suspect, they are caused by carelessness or failure to follow proper security procedures.
- Electronic Discovery
  - Electronic discovery (e-discovery) is the collection, preparation, review, and production of electronically stored information for use in criminal and civil actions and proceedings.
- Consumer Profiling
  - Companies openly collect personal information about users when they register at Websites, complete surveys, fill out forms, or enter contests online.

- Workplace Monitoring
  - Plenty of data exists to support the conclusion that many workers waste large portions of their work time doing non-work-related activity.
- Advanced Surveillance Technology
  - A number of advances in information technology—such as surveillance cameras and satellite-based systems that can pinpoint a person's physical location—provide amazing new data-gathering capabilities. However, these advances can also di9minish individual privacy and complicate the issue of how much information should be captured about people's private lives:
    - Camera Surveillance
    - Vehicle Event Data Recorders
    - Stalking Apps

The Right to Privacy

Privacy is a fundamental human right, although not absolute, enshrined in numerous international human rights instruments. It is central to the protection of human dignity and forms the basis of any democratic society. It also supports and reinforces other rights, such as freedom of expression, information and association.

The Philippine Constitution: Provision on Privacy

The word privacy was only mentioned once in the 1987 Philippine Constitution, thus

1. The privacy of communication and correspondence shall be inviolable except upon lawful order of the court, or when public safety or order requires otherwise as prescribed by law.
2. Any evidence obtained in violation of this or the preceding section shall be inadmissible for any purpose in any proceeding. (Art. III, Sec. 3)

Given that the constitution does not provide enough information in determining whether privacy is violated or not due to a non-absolute declaration of a citizen's right to privacy. Some questions that may be posted are:

When can we say that the order of the court lawful?

Exception 1. LAWFUL COURT ORDER.

The court order is lawful when the search warrant (court order) is issued by the judge after he personally determines that there is a probable cause which is required by Art. III Section 2 of the Constitution, thus: The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complaint and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.

In what instance that a citizen's right to privacy be invaded because public safety or order requires it?

Exception 2: PUBLIC ORDER OR SAFETY REQUIREMENT

This provision is best explained without regard to technology. In the Philippines, terrorists often carry out their attacks in public places such as LRT/MRT station and shopping malls. Hence, if Pedro carrying his precious wedding gift specially wrapped and sealed for wedding purposes decided to ride at any LRT/MRT station, he could not prevent the security guards to compel him to open the contents of the gift. This is because of the principle that the general welfare of the public is the supreme law. Thus, when one decides to ride in LRT/MRT or to travel by plane, he is temporary surrendering his rights to privacy because public safety requires it.

What are the laws which prescribed the invasion of an individual's privacy?

Exception 3: EXPRESS PROVISION OF THE LAW

There are so many laws, which provide an express provision requiring surrender of one's privacy. For instance, under the Anti Money Laundering Law, when an individual deposits in one transaction an amount of at least Three Hundred Thousand pesos (P300,00) in a bank, the latter is obliged by law to provide the name, as well as the personal information of the depositor, to the Anti Money Laundering council.

The Rational Relationship Test

In relation to the court order being lawful question, the Supreme Court will first determine if the policy has a "reasonable purpose" or "rational basis" for being enacted by the legislature. If the answer is yes, the policy is deemed to be "legitimate." The Supreme Court will then determine if the policy is "reasonably related" to attaining the identified legitimate end. If the answer is yes, the Supreme Court will go on further and the policy will be upheld.

Reasonable Expectation of Privacy

RA 4200, otherwise known as the **Anti-Wiretapping Act**, is a law which allows to some extent that the privacy of individuals may be invaded, provided that some requirements are complied with.

Section 1 and Section 4 of the Anti-Wiretapping Act provides:

- Sec. 1. It shall be unlawful for any person, not being authorized by all the parties to any private communication or spoken word, to tap any wire or cable, or by using any other device or arrangement, to secretly overhear, intercept, or record such communication or spoken work by using a device commonly known as a Dictaphone or dictograph or detectaphone or walkie-talkie or tape recorder, or however otherwise described.
- Sec. 4. Any communication or spoken word, or the existence, contents, substance, purport, effect, or meaning of the same or any part thereof, or any information therein contained, obtained or secured by any person in violation of the preceding sections of this Act shall not be admissible in evidence in any judicial, quasi-judicial, legislative or administrative hearing or investigation.

Areas of Concern in the Philippines

I. Communications Surveillance : the lack of oversight of state surveillance and the increase in the capacity of police and other agencies to conduct intrusive surveillance, pose a significant risk that unlawful surveillance will result not only the violation of individuals' privacy but also in enabling other serious human rights violations.

- Interception of Communication
  - Anti-Wiretapping Law of 1965 (Republic Act No. 4200)
  - Anti-Photo and Video Voyeurism Act of 2009 (Republic Act No. 9995)
  - Cybercrime Prevention Act of 2012 (Republic Act No. 10175)
  - Human Security Act of 2007 (Republic Act No. 9372)
- No implementation of oversight and accountability mechanism for the police
- Regulations of Cybercrime Prevention Act
  - Section 12 (Real-Time Collection of Traffic Data) of the Cybercrime Prevention Act was stricken down as unconstitutional by the Supreme Court.
- Data retention
  - The regime of data retention is outlined in the Implementing Rules and Regulations of the Electronic Commerce Act (2000). The act is intended to provide for the "recognition and use of electronic commercial and non-commercial transactions and documents, penalties for unlawful use thereof and for other purposes".
  -

II. Data Protection

- Massive Breach of the Government's Electoral Commission
- Bills seeking to establish a National ID System

The Data Privacy Law

The Data Privacy Act or Republic Act 10173 regulates the processing of personal information of individuals collected by both public and private entities as a way to protect one's privacy. Under the Data Privacy Law, an individual shall be given the right to control any kind of personal information that is collected from him for further use and disclosure.

It **(1)** protects the privacy of individuals while ensuring free flow of information to promote innovation and growth; **(2)** regulates the collection, recording, organization, storage, updating or modification, retrieval, consultation, use, consolidation, blocking, erasure or destruction of personal data; and **(3)** ensures that the Philippines complies with international standards set for data protection through National Privacy Commission (NPC).

Know Your Data Privacy Rights

1. The right to be informed
2. The right to access
3. The right to object
4. The right to erasure or blocking
5. The right to damages
6. The right to file a complaint
7. The right to rectify
8. The right to data portability