SPI 1ST SEM FINALS

Republic Act No. 9995: Anti-Photo and Video Voyeurism Act of 2009

An act defining and penalizing the crime of photo and video voyeurism, prescribing penalties therefor, and for other purposes.

Offenses Against The Confidentiality & Availability of Computer Data & Systems

1. **Illegal Access**
    a. The intentional access to the whole or any part of a computer system without rights
        i. There must be an intentional access in whole or in part of a computer system.
        ii. The person who attempts to, or is accessing, or had already access the data has no right of access to the system.
            1. conduct undertaken without or in excess of authority; or
            2. conduct not covered by established legal defenses, excuses, court orders, justifications, or relevant principles under the law
    b. **Ethical/white-hat hackers** - use hacking tools and techniques similar to those used by criminal hackers but with permission from the target organization.
2. **Illegal Interception**
    a. the unauthorized listening, recording, or monitoring of private, non-public transmissions of computer data. This can include intercepting emails, data from computer systems, or other electronic communications, either by technical means or through the use of spyware or similar tools.
        i. It must be intentional;
        ii. It must be by technical means;
        iii. The person involved is without any right to do the interception;

iv. The transmission of computer data to, from, or within a computer system is non-public.

b. Data interference

i. The intentional or reckless alteration, damaging, deletion or deterioration of computer data, electronic document, or electronic data message, without right, including the introduction or transmission of viruses.

ii. Alteration - the modification or change, in form or substance, of an existing computer data or program.

c. System interference

i. The intentional alteration or reckless hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data message, without right or authority, including the introduction or transmission of viruses.

In data interference, interference is directed against the data itself whilst system interference is directed against the functioning computer system--both data & computer program.

Misuse of Devices

The use, production, sale, procurement, importation, distribution, or otherwise making available, without right, of:

- Device, including a computer program, designed or adapted primarily for the purpose of committing any of the offenses under this Act; or
- A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with intent that it be used for the purpose of committing any of the offenses under this Act:
    - the possession of an item referred to in paragraphs 5(i)(aa) or (bb) above with intent to use said devices for the purpose of committing any of the offenses under this Section.

Cybersquatting

the acquisition of a domain name over the internet in bad faith to profit, mislead, destroy reputation, and deprive others from registering the same, if such a domain name is:

1. similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration:
2. identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and
3. acquired without right or with intellectual property interests in it

Computer-Related Offenses

1. **Computer-Related Fraud**
2. **Computer-Related Forgery**
3. **Computer-Related Identity Theft**

Content-Related Offenses

1. **Cybersex**
    a. Willful engagement of sexuality activity via computer devices--maintenance, control, or operation
2. **Child Pornography**
    a. Republic Act 9775 criminalizes the production, distribution, and possession of child pornography in the Philippines
3. **Unsolicited Commercial Communications**
    a. messages, usually in the form of emails, texts, or calls, that promote products, services, or businesses and are sent without the recipient's prior consent.
    b. Often referred to as "spam" in the context of email, these communications are typically sent in bulk and aim to advertise or market products, services, or events to a broad audience.

Cultural Relativism

the idea that cultural values, beliefs, and behaviors should be understood within the context of the culture that created them, rather than being judged by the standards of another culture. It suggests that all points of view are equally valid, and that truth is relative.

Republic Act No. 10175: Cybercrime Prevention Act of 2012, The Cybercrime Law

completely address crimes committed against and by means of computer system on 12 September 2012. It includes penal substantive rules, procedural rules and also rules on international cooperation.

- Cyber-disaster as the LOVE bug struck the world in the early part of the year 2000
- The so-called "Love-Bug"/"Love Letter" email virus has caused some $10 billion in losses in as many as 20 countries
- Main suspect: Filipino student as the author of the "I love you" virus
- VBS - – a type of interpreted file, most often hidden by default on Windows computers of the time, leading unsuspecting users to think it was a normal text file

Republic Act No. 8792: The Electronic Commerce Act of 2000, The E-Commerce Law

- Signed into law on June 14, 2000
- Prompted by cyber incidents like the "I LOVE YOU" virus attack, the law aims to regulate electronic transactions and address cybercrimes, particularly focusing on electronic evidence, hacking, and copyright violations. It provides a legal framework for internet-based services and electronic commerce, establishing rules for online business transactions and promoting cybersecurity by criminalizing various forms of digital misconduct
- Focuses more on electronic evidence and common online crimes such as hacking and copyright violations
- Section 33 of the Electronic Commerce Act of 2000

Types of E-Commerce Law

- B2B (Business-to-business)
- B2C (Business-to-consumer)
- C2C (Consumer-to-consumer)

Consumer Trends

Increased credit card use, online payments, and exchange of goods/services platforms.

DTI Registration

Improved business name registration—processing now takes only 15-30 minutes online, benefiting small businesses and entrepreneurs

Security

The general security concerns in e-commerce involves:

1. User authorisation
2. Data & transaction security

Available authorization schemes

1. Password encryption
2. Encrypted smart cards
3. Biometrics
4. Firewalls

Penalty

Section 6 of the Cybercrime Prevention Act of 2012

- The penalty for any crime defined in the Revised Penal Code or special laws that is committed using information and communications technologies is one degree higher than the penalty provided for in the Revised Penal Code or special laws.
- Prosecution under the Cybercrime Act does not affect any liability for violating the Revised Penal Code or special laws.

Encryption

a set of secret codes which defends sensitive information that crosses over public channels (such as the Internet). It is a mutation of information in any form (text, video, and graphics) into a form decipherable only with a decryption key.

Kinds of Encryption

- Secret-key encryption
    - Symmetric encryption; a single-key shared between the sender and receiver to encrypt and decrypt messages
- Public/private-key encryption
    - Asymmetric encryption; uses two keys to encrypt the message and a private key to decrypt it

Digital Signature

A cryptographic tool that verifies the sender's identity & ensures message integrity

Under Philippine law, text messages are considered admissible as evidence thanks to the Rules of Court (A.M. No. 01-7-01-SC) issued by the Supreme Court on July 17, 2001. This ruling complements the E-Commerce Act, which first recognized electronic communications, like texts, as valid evidence. In A.M. No. 01-7-01-SC, two important sections are relevant: Section 1(k), Rule 2 defines "ephemeral electronic communication, " which includes text messages. This confirms that texts are a type of digital communication that can be legally examined. Section 2, Rule 11 states that these messages can be used as evidence if a witness, who was either involved or has personal knowledge of the content, can verify them. This rule sets a clear standard for verifying and using text messages in court.

Republic Act No. 10173: Data Privacy Act of 2012

The Data Privacy Act of 2012 (DPA) is a law in the Philippines that protects personal and sensitive information in communication systems:
Purpose: The DPA protects the privacy of individuals while ensuring the free flow of information. It also aims to comply with international standards for data protection.

Scope: The DPA applies to both the public and private sectors. It regulates the collection, storage, use, and destruction of personal data.

Rights: The DPA outlines the rights of data subjects, including:

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

Netiquette is the computer ethics to be followed when using the Internet.
Consequentialism is an ethical theory that judges actions based on their outcomes or consequences.
Conventionalism is the belief that ethical norms are based on social agreements
Trading is the exchange of goods, services, or assets, governed by ethical and legal standards
Ethics is the study of what is morally right or wrong

- Morality is the principles concerning the distinction between right & wrong behaviour

Libel is defamation through written or electronic means
Slander is defamation through spoken words
Cybersecurity is the practice of protecting systems, networks, and data from cyber threats
John Kemeny & Thomas Kurtz are creators of the BASIC programming language