LEGAL, ETHICAL and PROFESSIONAL ISSUES in INFORMATION SECURITY

Learning Objectives

At the end of this learning activity, you should be able to:

1. Use this chapter as a guide for future reference on laws, regulations, and professional organizations
2. Differentiate between laws and ethics
3. Identify major national laws that relate to the practice of information security
4. Understand the role of culture as it applies to ethics in information security.

Law and Ethics in Information Security

Terminologies:

- *Cultural mores*: fixed morals or customs of a group of people, form the basis of ethics
- *Ethics*: Rules that define socially acceptable behavior, not necessarily criminal, not enforced (via authority/courts)
- *Laws*: Rules that mandate or prohibit behavior, enforced by governing authority (courts)
  - Laws carry sanctions of governing authority, ethics do not

Law and Ethics in Information Security

Terminologies:

- *Policy*: "Organizational laws"
  - Expectations that define acceptable workplace behavior
  - General and broad, not aimed at specific technologies or procedures
  - To be enforceable, policy must be distributed, readily available, easily understood, and
  - acknowledged by employees.
- *Standards, guidelines, best practices*: define what must be done to comply with policy and how to do so.
- *Jurisdiction*: a court's right to hear a case if a wrong was committed in its territory or against its citizens

Law and Ethics in Information Security

Terminologies:

- *Long-arm jurisdiction:* court's ability to "reach far" and apply the law (another state, country)
- *Case law:* documentation about the application of law in various cases
- *Liability*: legal obligation beyond what's required by law, increased if you fail to take due care.
- *Due care*: This is taken when employees know what is/isn't acceptable and what the consequences are.
- *Due diligence*: sustained efforts to protect others.

Law and Ethics in Information Security

Types of Law:

- *Civil:* laws governing nation or state
- *Criminal*: harmful actions to society, prosecuted by the state
- *Tort*: individual lawsuits as recourse for “wrongs”, prosecuted by individual attorneys
- *Private*: includes family, commercial, and labor law
- *Public*: includes criminal, administrative, and constitutional law

Law and Ethics in Information Security

Types of Law:

In practice, you can be sued for almost anything; there is no "absolute" protection against litigation.

Information security practices can:

– Reduce the likelihood that incidents result in lawsuits
– Reduce the likelihood that you lose (by showing due care and due diligence)
– Minimize damages/awards
– Help you respond effectively to incidents

Employment Issues and Employees Rights on Personal Data

The Cybercrime Prevention Act of 2012 (CPA) defines the following as cybercrimes:

- Offenses against the confidentiality, integrity, and availability of computer data and systems (illegal access, illegal interception, data interference, system interference, misuse of devices, and cybersquatting);
- Computer-related offenses (computer-related forgery, computer-related fraud, and computer-related identity theft); and
- Content-related offenses (cybersex, child pornography, unsolicited commercial communications, and libel).

Roles of Government Agencies under CPA:

- *National Bureau of Investigation (NBI) and Philippine National Police (PNP)*
  - Enforcement authorities
  - Regulates their access to computer data
  - Creation of the *Cybercrime Investigation and Coordinating Center (CICC)* as an inter-agency body for policy coordination and enforcement of the national cybersecurity plan;
  - Creation of the *Office of Cybercrime within the Department of Justice (DOJ-OC)* for international mutual assistance and extradition

Roles of Government Agencies under CPA:

- *Supreme Court's Rule on Cybercrime Warrants (AM No. 17-11-03-SC)*
  - Governs the application and grant of court warrants and related orders involving the preservation, disclosure, interception, search, seizure or examination;
  - Custody and destruction of computer data, as provided under the CPA.

The Electronic Commerce Act of 2000 (ECA)

- Provides for the legal recognition of electronic documents, messages, and signatures for commerce, transactions in government, and evidence in legal proceedings;
- Custody and destruction of computer data, as provided under the CPA;
- Penalizes hacking and piracy of protected material, electronic signature, or copyrighted works, limits the liability of service providers that merely provide access, and prohibits persons who obtain access to any electronic key, document, or information from sharing them;
- Allows parties to choose their type or level of electronic data security and suitable technological methods, subject to the *Department of Trade and Industry* guidelines

The Access Devices Regulation Act of 1998 (ADRA)

- Penalizes various acts of access device fraud such as using counterfeit access devices;
- An **access device** is any card, plate, code, account number, electronic serial number, personal identification number or other telecommunications service, equipment or instrumental identifier, or other means of account access that can be used to obtain money, goods, services or any other thing of value, or to initiate a transfer of funds.
- *Banks*, financing companies and other financial institutions issuing access devices must submit annual reports of access device frauds to the *Credit Card Association of the Philippines*, which forwards the reports to the NBI.

Employment Issues and Employees Rights on Personal Data

The Data Privacy Act of 2012 (DPA)

- Regulates the collection and processing of personal information in the Philippines and of Filipinos, including sensitive personal information in government;
- Creates the **National Privacy Commission (NPC)** as a regulatory authority;
- Requires personal information controllers to implement reasonable and appropriate measures to protect personal information and notify the NPC and affected data subjects of breaches;
- Penalizes unauthorized processing, access due to negligence, improper disposal, processing for unauthorized purposes, unauthorized access or intentional breach, concealment of security breaches, and malicious or unauthorized disclosure in connection with personal information

The Functions of the National Privacy Commission

1. Ensure compliance of personal information controllers to this Act.
2. Receive complaints, institute investigations, facilitate or enable settlements of complaints
3. Issue cease and desist orders.
4. Compel or petition any entity, government agency or instrumentality to abide by its orders or take action on a matter affecting data privacy.
5. Monitor the compliance of other government agencies or instrumentalities on their measures and technical measures.
6. Coordinate with other government agencies and the private sector on the efforts to formulate and implement plans and policies to strengthen the protection of personal information in the country.

The Functions of the National Privacy Commission

7. Public on a regular basis a guide to all laws relating to data protection.
8. Publish a compilation of agency system of records and notices.
9. Recommend to the Department of Justice the prosecution and imposition of penalties.
10. Review, approve, reject or require modification of privacy codes voluntarily adhered to by personal information controllers.
11. Provide assistance on matters relating to privacy or data protection.
12. Comment on the implication on data privacy of proposed national or local statutes.
13. Propose legislation, amendment, or modifications to Philippine laws on privacy or data protection as may be necessary.

The Functions of the National Privacy Commission

14. Ensure proper and effective coordination with data privacy regulators.
15. Negotiate and contract with other data privacy authorities of other countries.
16. Assist Philippine companies doing business abroad to respond to foreign privacy or data protection laws and regulations.
17. Generally perform such acts as may be necessary to facilitate cross-border enforcement of data privacy protection.

A full discussion of the Commission's functions can be found here:

https://www.privacy.gov.ph/data-privacyact/#7

Employment Issues and Employees Rights on Personal Data

According to RA 10173, a personal information controller refers to

"a person or organization who controls the collection, holding, processing or use of personal information, including a person or organization who instructs another person or organization to collect, hold, process, use, transfer or disclose personal information on his or her behalf."

AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR

Employment Issues and Employees Rights on Personal Data

A personal information controller must be aware that the employee, of whom the organization has data of is subject to the following protections:

- The right to know about the existence of their right as enumerated below. (Sec. 16(b))
- The right to be informed of the collection and processing of data relating to the employee. (Sec. 16(a) and Sec 16(c))
- The right to be furnished of a copy of the data of the employee which is processed by the employer. (Sec. 16(b))
- The right to data portability (the right to have their data forwarded and transferred) to subsequent employers to the extent lawfully allowed. (Sec. 18)
- The right to correct, amend or remove inaccurate data from the employee's record. (Sec. 16(d) and Sec. 16(e))
- The right to know how long and for what purposes an employee's data is to be maintained. (Sec. 16(b))
- What and how the personal information is processed and stored in the human resource system (HRIS). (Sec. 16(b) and Sec. 16(c))
- The right to have appropriate physical, technical and administrative safeguards in relation to the system where data is being stored pertaining to the employee by the employer. (Sec. 20)

Employment Issues and Employees Rights on Personal Data

A personal information controller must be aware that the employee, of whom the organization has data of is subject to the following protections:

- Who are other 3rd parties, outside the organization that such information pertaining to the employee is shared with including why and how is such information shared. (Sec. 16(c))
- The right to file a complaint with the National Privacy Commission and order the removal, blocking or destruction of data against the organization for misuse, mishandling and unauthorized disclosure of data. (Sec 16(b))
- The right to damages for inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of employee data by the employer. (Sec. 16(f))
- If the employer is collecting data of more than 250 individuals, they need to have their processing system registered with the National Privacy Commission. (NPC Circular 17-01)

Intellectual Property Rights

Republic Act 8942

- Otherwise known as the Intellectual Property Code of the Philippines;
- A governing law that adhered to:
  - The Paris Convention for the Protection of Industrial Property Rights,
  - The Berne Convention for the Protection of Literary and Artistic Works,
  - The Patent Cooperation Treaty, the TRIPS Agreement, and the WIPO Copyright Treaty, among others
- Ensures the protection of intellectual property such as copyright, trademark, patent, utility model, and industrial design;
- All registration of applications for such rights is filed with the **Philippine Intellectual Property Office (IPO)** except copyright;
- Copyright applications are deposited with the IPO pursuant to an agreement with the **Philippine National Library**

Intellectual Property Rights

Common terms that are identified with intellectual property rights

- **Trademark**. It is a type of intellectual property consisting of recognizable signs, designs, or expressions that identify products or services of a particular source from those of others.
- **Patent**. It is a form of intellectual property that gives its owner the legal right to exclude others from making, using, or selling an invention for a limited period of years in exchange for publishing and enabling public disclosure of the invention.
- **Utility Model**. It is an intellectual property right to protect inventions. It is very similar to a patent but usually has a shorter term, shorter grant lag, and less stringent patentability requirements. Utility models can be described as second-class patents.

Intellectual Property Rights

Common terms that are identified with intellectual property rights

- **Industrial Design**. It is an intellectual property right that protects the visual design of objects that are not purely utilitarian. An industrial design consists of the creation of a shape, configuration or composition of pattern or color, or combination of pattern and color in three-dimensional form containing aesthetic value. It can be a two- or three- dimensional pattern used to produce a product, industrial commodity or handicraft.
- **Copyright**. It is at type of intellectual property that gives its owner the exclusive right to make copies of a creative work, usually for a limited time. The creative work may be in a literary, artistic, educational, or musical form. Copyright is intended to protect the original expression of an idea in the form of a creative work, but not the idea itself.

Intellectual Property Rights

Claims of convention priority or priority dates are acknowledged and respected, provided that they are claimed within *twelve (12) months* from the date of the earliest foreign application (for patents and utility models) or *within six (6) months* from the date of the earliest foreign application (for trademarks and industrial designs).

Intellectual Property Rights

The terms of protection for trademark, patent, utility model, industrial design, and patents are as follows:

- **Trademark**. Ten (10) years and may be renewed for periods of ten (10) years each.
- **Patent**. Twenty (20) years from the filing date of the application.
- **Utility Model**. Seven (7) years from the filing date of the application without renewal.
- **Industrial Design**. Five (5) years from the filing date of the application and may be renewed for not more than two (2) consecutive periods of five (5) years each.
- **Patent under the Patent Cooperation Treaty (PCT)**. Twenty (20) years from the international filing date of the application.

The Data Privacy Law

The National Privacy Commission presented a quick guide for the Data Privacy Act, it can be downloaded here:

https://www.privacy.gov.ph/wp-content/files/quickguide/DPA_QuickGuidefolder_insideonly.pdf

Accordingly, RA 10173 or the Data Privacy Act of 2012's full text can be seen here:

https://www.privacy.gov.ph/data-privacy-act/#16

The Ten Commandments of Computer Ethics

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.

The Ten Commandments of Computer Ethics

6. Thou shalt not copy or use proprietary software for which you have not paid (without permission).
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 other humans.

Ethical Differences Across Cultures

- Cultural differences create difficulty in determining what is and is not ethical;
- Difficulties arise when one nationality's ethical behavior conflicts with the ethics of another national group
- *Example*: One of the ways in which Asian cultures use computer technology is through software piracy

Ethics and Education

- The overriding factor in leveling ethical perceptions within a small population is education
- Employees must be trained in the expected behaviors of an ethical employee, especially in areas of information security
- Proper ethical training is vital to creating informed, well-prepared, and low-risk system user

Deterrence to Unethical and Illegal Behavior

- Deterrence: best method for preventing an illegal or unethical activity, e.g., laws, policies, technical controls
- Laws and policies only deter if three conditions are present:
  - Fear of penalty
  - The probability of being caught
  - Probability of penalty being administered

Association of Computing Machinery (ACM)

- ACM was established in 1947 as “the world's first educational and scientific computing society”
- Code of ethics contains references to protecting information confidentiality, causing no harm, protecting others’ privacy, and respecting others’ intellectual property

International Information Systems Security Certification Consortium, Inc. (ISC) 2

- Non-profit organization focusing on development and implementation of information security certifications and credentials
- Code primarily designed for information security professionals who have certification from $(ISC)^2$
- Code of ethics focuses on four mandatory canons

System Administration, Networking, and Security Institute (SANS)

- Professional organization with a large membership dedicated to protection of information and systems
- SANS offers set of certifications called Global Information Assurance Certification (GIAC)

Information Systems Audit and Control Association (ISACA)

- Professional association with focus on auditing, control, and security
- Concentrates on providing IT control practices and standards
- ISACA has code of ethics for its professionals

Computer Security Institute (CSI)

- Provides information and training to support computer, networking, and information security professionals
- Though without a code of ethics, has argued for the adoption of ethical behavior among information security professionals

Information Systems Security Association (ISSA)

- Nonprofit society of information security (IS) professionals
- The primary mission to bring together qualified IS practitioners for information exchange and educational development
- Promotes code of ethics similar to (ISC)2, ISACA and ACM

Other Security Organizations

- Internet Society (ISOC): promotes development and implementation of education, standards, policy and education to promote the Internet
- Computer Security Division (CSD): division of National Institute for Standards and Technology (NIST); promotes industry best practices and is important reference for information security professionals
- CERT Coordination Center (CERT/CC): center of Internet security expertise operated by Carnegie Mellon University
- Computer Professionals for Social Responsibility (CPSR): public organization for anyone concerned with impact of computer technology on society

Organizational Liability and the Need for Counsel

- Liability is legal obligation of an entity; includes legal obligation to make restitution for wrongs committed
- Organization increases liability if it refuses to take measures known as due care
- Due diligence requires that an organization make valid effort to protect others and continually maintain that level of effort

Group Activity

1. The following are cybersecurity-related terms:
   - hacking,
   - data breach,
   - intellectual property,
   - cyber fraud,
   - Cyberbullying
2. From the list, you are to research on:
   a) A real-world case where this law was applied
   b) The specific section of the law that addresses the issue
   c) The penalties for violating the law
4. Your group will present your output

Learning Activity (Individual)

Read the following case scenario and answer the guided questions below.

Scenario:

A software engineer working for a tech company discovers that the company has secretly collected user data without explicit consent. The data includes browsing history, location, and personal messages. The engineer is concerned about the ethical and legal implications and considers exposing the company's actions.

Guided Questions:

1. What ethical concerns are present in this scenario?
2. Which laws (Cybercrime Prevention Act, Data Privacy Act, etc.) may be violated?
3. What role do due care and due diligence play in this situation?
4. How might jurisdiction affect the legal consequences if this happened in another country?