DATA PRIVACY AND DIGITAL ARCHIVES:
ETHICAL CONSIDERATIONS, POLICIES, AND GUIDELINES

ATTY. ROMULO R. UBAY, JR.

7th ASLP National Congress
9-11 October 2019, Dumaguete City

OBJECTIVES

1. To discuss issues on **data privacy** in relation to **access** and retrieval of materials in **digital archives**;

2. To inform the participants of ethical and **legal implications** of **digitization** and distribution of digital materials; and,

3. To provide practical examples and advice on how to successfully build digital archives without infringing any **copyright** laws and **intellectual property rights**.

Privacy: Three Interrelated Concepts

1. **Privacy as a civil liberty**: safeguarding the privacy of individuals

2. **Data protection**: safeguarding the confidentiality of information about individuals

   **Confidentiality* – is preserving authorized restriction on information access and disclosure, including means of protecting personal privacy and proprietary information. (*US Department of Commerce, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) ")*

3. **Security**: safeguarding the infrastructure (i.e., the systems and networks – that hold and transport electronic data and communications)

(See: Kent Wada. "The Right to Be Let Alone". EDUCAUSE Review, vol. 45, no.1. (January/February 2010): 56-57.)

ASSOCIATION OF SPECIAL LIBRARIES OF THE PHILIPPINES

Right to Privacy

- "the right to be free from unwarranted exploitation of one's person or from intrusion into one's private activities in such a way as to cause humiliation to a person's ordinary sensibilities." (*Social Justice Society v. Dangerous Drugs Board, G.R. 157870*, Nov 3, 2008, 570 SCRA 410, 431)

- Right of an individual "to be free from unwarranted publicity, or to live without unwarranted interference by the public in matters in which the public is not necessarily concerned." *(Spouses Hing vs. Choachuy, et al. (G.R. No. 179736, June 26, 2013)*

- "The right to be let alone is indeed the beginning of all freedom." – Dissenting Opinion of Justice Douglas (*Public Utilities Commission v. Pollak, 343 U.S. 451*, 467 (1952).

RIGHT TO PRIVACY

"Fundamental Right to Be Let Alone"

ASSOCIATION OF SPECIAL LIBRARIES OF THE PHILIPPINES
1954

Categories of Right to Privacy

- ***Decisional Privacy*** (independence in making certain important decisions)
- ***Informational Privacy*** (interest in avoiding disclosure of personal matters)
- ***Locational or situational privacy***

ASSOCIATION OF SPECIAL LIBRARIES OF THE PHILIPPINES 1954

Right to Privacy: Constitutional basis

Article III, Section 3(1) of the 1987 Philippine Constitution

"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."

ASSOCIATION OF SPECIAL LIBRARIES OF THE PHILIPPINES

What is **Data Privacy**?

- The right of an individual not to have private information about himself disclosed, and to live freely from surveillance and intrusion.

(Source: NPC, 2019)

Data privacy v. Free flow of information

PH State Policy (Sec. 2, RA 10173)

It is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth.

The State recognizes the vital role of information and communications technology in nation-building and its inherent obligation to ensure that personal information in information an communications systems in the government and in the private sector are secured and protected.

Privacy v. Free flow of information

"The individual's desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives in."

-- Alan Westin, *Privacy and Freedom* (1967)

Republic Act 10173 - Data Privacy Act of 2012

"AN ACT PROTECTING INDIVIDUAL PERSONAL INFORMATION IN INFORMATION AND COMMUNICATIONS SYSTEMS IN THE GOVERNMENT AND THE PRIVATE SECTOR, CREATING FOR THIS PURPOSE A NATIONAL PRIVACY COMMISSION, AND FOR OTHER PURPOSES"

Data Privacy Act of 2012: Scope

"Apply to the processing of personal data by any natural and juridical person in the government or private sector"

"Personal data" -- refers to all types of personal information

- 1. information in which the individual is identified

- 2. information in which an individual, while not identified, is described in a way that makes it possible to find out who the data subject is by conducting further research.

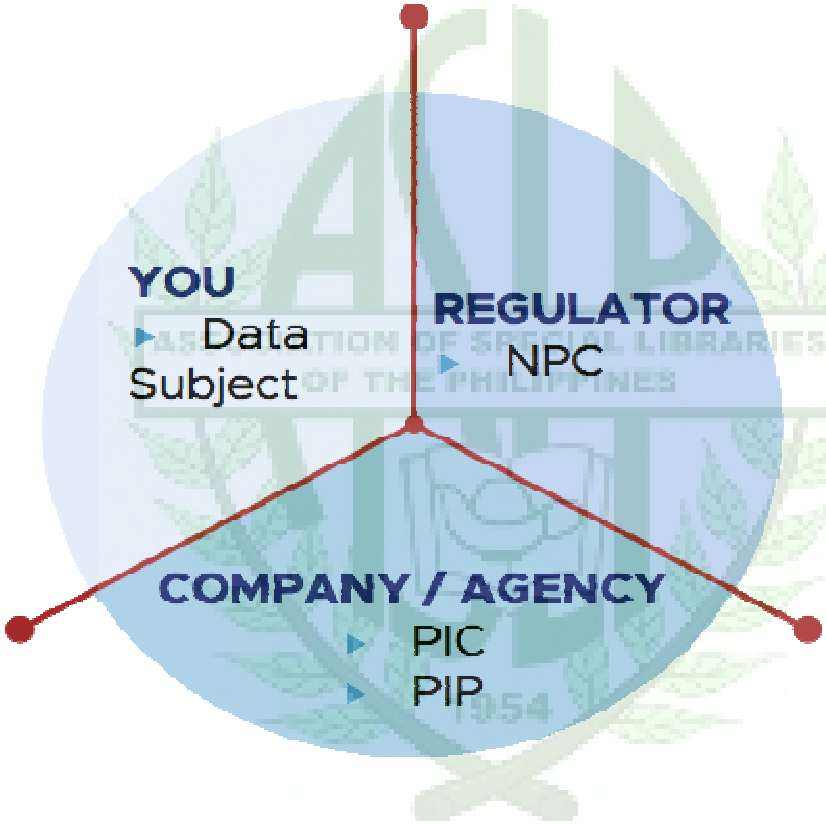
ASSOCIATION OF SPECIAL LIBRARIES OF THE PHILIPPINES 1954

"Processing"

- "any operation or any set of operations performed upon personal data including, but not limited to,
  - collection
  - recording
  - Organization
  - Storage
  - Updating
  - Modification
  - Retrieval
  - Consultation
  - Use
  - Consolidation
  - Blocking
  - Erasure
  - Destruction
- refers primarily to automated systems of data processing but the Data Privacy Act also envisions manual processing in structured filing systems.

KEY ROLES IN THE DATA PRIVACY ACT

- **Data Subjects**
  - Refers to an individual whose personal data is processed
- **Personal Information Controller (PIC)**
  - A natural or juridical person, or any other body who controls the processing of personal data
- **Personal Information Processor (PIP)**
  - A natural or juridical person, or any other body to whom a PIC may outsource or instruct the processing of personal data
- **Data Protection Officer (DPO)**
  - Responsible for the overall management of compliance to DPA
- **National Privacy Commission**
  - Independent body mandated to administer and implement the DPA and to monitor and ensure compliance of the country with international standards set for personal data protection



(NPC, 2019)

Personal Information

"any information whether recorded in a material form or not, from which the identity of an individual is apparent or can be reasonably and directly ascertained by the entity holding the information, or when put together with other information would directly and certainly identify an individual."

PERSONAL INFORMATION : Examples

- Name
- Address
- Place of Work
- Telephone Number
- Gender
- Location of an individual at a particular time
- IP Address
- Birth date
- Birth Place
- Country of Citizenship
- Payroll and Benefits Information
- Contact Information

CRITERIA FOR LAWFUL PROCESSING OF PERSONAL INFORMATION

- Consent
- Necessary for fulfilment of a contract
- Protection of the vital interests of the data subject (Life/health)
- Necessary for compliance of a legal obligation
- Responding to National emergency /
- Compliance with requirements of public order and safety
- Necessary for fulfilment of constitutional or statutory mandate of a public authority
- Legitimate interests of the PIC or third parties to whom data was disclosed

SENSITIVE PERSONAL INFORMATION

- Race
- Ethic Origin
- Marital Status
- Age
- Color
- Religious Affiliation
- Political Affiliation
- Health
- Education
- Genetics
- Sexual Life
- Proceeding for any offense committed, the disposal of such proceedings, the sentence of any court in such proceedings

SENSITIVE PERSONAL INFORMATION

(Based on the IRR)

- Social Security Number
- Licences or its denials, suspension or revocation
- Tax returns
- Other personal information issued by Government agencies
- Bank and credit/debit card numbers
- Websites visited
- Materials downloaded
- Any other information reflecting preferences and behaviors of an individual
- Grievance information
- Discipline information
- Leave of absence reason
- Licenses or its denials, suspension or revocation

PRIVILEGED INFORMATION : Examples

- Data received within the context of a protected relationship:
  - Husband and wife
  - Attorney and client
  - Priest and penitent
  - Doctor and Patient
- National Security Matters
- Trade Secrets
- Banking Transactions/Deposits
- Source of published news

Criteria for Lawful Processing of Sensitive Personal Information

- Consent
- Existing law provisions and regulations
- Protection of Life & Health
- Medical treatment
- Protection of lawful rights and interest in court proceedings/legal claims

What are a PIC or PIP's Primary Obligations?

- Adhere to data privacy principles
- Uphold data subject rights
- Implement security measures

ASSOCIATION OF SPECIAL LIBRARIES OF THE PHILIPPINES

Data Privacy Principles

- Transparency
- Legitimate Purpose
- Proportionality

Principle of Transparency

A data subject must be aware of the nature, purpose, and extent of the processing of his or her personal data, including the risks and safeguards involved, the identity of personal information controller, his or her rights as a data subject, and how these can be exercised.

Any information and communication relating to the processing of personal data should be easy to access and understand, using clear and plain language.

Principle of Legitimate Purpose

The processing of information shall be compatible with a declared and specified purpose, which must not be contrary to law, morals, or public policy.

Principle of Proportionality

The processing of information shall be adequate, relevant, suitable, necessary, and not excessive in relation to a declared and specified purpose.

Personal data shall be processed only if the purpose of the processing could not reasonably be fulfilled by other means.

Upholding the Rights of the Data Subject

- Right to be informed
- Right to object
- Right to access
- Right to data portability
- Right to correct (rectification)
- Right to erasure or blocking
- Right to file a complaint
- Right to damages
- Transmissibility of Rights

Right to be informed

- Personal data should never be collected, processed, and stored by any organization without the explicit consent of the data subject, unless otherwise provided by law.

- Requires personal information controllers (PICs) to notify data subject in a timely manner if his data have been compromised.

Right to object

- The right of the data subject to withhold consent.

- If data subject does not give consent, the PIC should no longer process the personal data, unless the processing is pursuant to a subpoena, for obvious purposes (contract, employer-employee relationship, etc.) or a result of a legal obligation.

Right to access

- Right to find out whether an organization holds any personal data about the data subject and if so, gain "reasonable access" to them .

- Right to be provided with a written description on the purpose for holding the data subject's personal data.

Right to correct (rectification)

- Right to dispute and have corrected any inaccuracy or error in the data a personal information controller (PIC) hold about the data subject.

Right to erasure or blocking

- Right to suspend, withdraw or order the blocking, removal or destruction of personal data

Right to file a complaint

- In case data subject 's personal information has been misused, maliciously disclosed, or improperly disposed, or that any of his data privacy rights have been violated

Right to damages

- Right to claim compensation if data subject suffered damages due to inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data

Right to data portability

- Right that allows data subject to obtain and electronically move, copy or transfer his or her data in a secure manner, for further use.

Transmissibility of Rights

- Right to assign rights as a data subject to a legal assignee or lawful heir.

ASSOCIATION OF SPECIAL LIBRARIES OF THE PHILIPPINES
1954

IMPLEMENTING OF SECURITY MEASURES

- Technical
- Organizational
- Physical

ASSOCIATION OF SPECIAL LIBRARIES OF THE PHILIPPINES 1954

Technical

Encryption

- To what standard? (cost Vs benefit)
- All devices or just some?

Passwords

- Enforced strength and updates?

Sharing data

- Technical solutions – e.g. via email; portals

System testing & maintenance

- Who has access, to what (System Administrators)
- Live or dummy data?
- Firewalls / Anti-virus / Spam filters

Backups

- Secure: encrypted tapes | cloud-provider
- Auditable process

Access control

- Who decides permissions and privileges ('need to know')?

Remote access

- How delivered securely?
- Permit Bring Your Own Device?

Source: R. Lansingan , "Primer on the Data Privacy Act of 2012 (ppt file), 24 November 2017

Organisational – physical security

Secure Office Storage

For removable devices **and** hardcopy information

- Identifying marks?
- Kensington locks?
- Locked print?
- Offsite?

Remote working

Secure both hardcopies and devices when in transit.

Kept out of sight: in transit | at home.

Lockable pedestals | Kensington locks?

Building access control

Secure premises – CCTV | locked windows | perimeter

Locked CCTV room | server room

ID badges, supervised visitors | contractors

Secure disposal

Shredding of hardcopies

Beyond use | Reuse | Resale

Source: R. Lansingan , "Primer on the Data Privacy Act of 2012 (ppt file), 24 November 2017

Organisational – other measures

Policy, procedures, guidance & training

Eliminate ambiguities

Clearly communicated, readily accessible and understood

Human Resources

Explicit roles and responsibilities in Job Descriptions and Terms of Reference

Terms and Conditions: confidentiality clauses

Clear expectations | reporting lines

Disciplinary process

Training records

Procurement (and contracts)

i.e. outsourced services like IT and software

Due diligence

Compliant contract Terms and Conditions:

- Act on your instructions
- Equivalent security

Auditing and monitoring

Source: R. Lansingan , "Primer on the Data Privacy Act of 2012 (ppt file), 24 November 2017

NOT Covered under the Data Privacy Act

- Information about public officials relating to their position and official functions
- Matters of public concern
- Journalistic, artistic, or literary purposes
- Research purposes, intended for public benefit
- Information necessary for performance of law enforcement or regulatory functions of public authority (e.g. Secrecy of Bank Deposits Act, Foreign Currency Deposit Act)
- Banks & financial institutions information (in accordance with the BSP-bank regulations, AMLA, & other applicable laws.

OTHER ISSUES

- **Intellectual Property** (specifically, Copyright)
  (Issue on ownership of any content)

- **Freedom of information**
  (Right of the people to information on matters of public concern; access to official records; "closure period / potential exemptions)

- **Full public disclosure**
  (Policy of full public disclosure of all its transactions involving public interest)

References:

- *R. Lansingan , "Primer on the Data Privacy Act of 2012 (ppt file), 24 November 2017*
- Aguda, HR, Montes, MF, and Tiojanco, BD (2016). *Data Privacy & Cybercrime Prevention in the Philippine Digital Age*. Vibal.
- Wada, K (2010), "The Right to Be Let Alone". EDUCAUSE Review, vol. 45, no.1. (January/February 2010): 56-57.
- *US Department of Commerce, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)*
- National Privacy Commission Website.

PART II : WORKSHOP

WORKSHOP : CASE STUDY

- Jay teaches Math subjects in a public elementary school.
- One day, he posted on Facebook photos showing that he was drinking hard liquor and smoking cigarettes inside a nightclub, beside him are women wearing revealing clothes. In one photo, he was shown touching the breast of one of the women she was with.
- Pedro, Jay's friend on Facebook and co-teacher at the school, reported Jay's photos to the School Principal.
- The following week, Jay took a week leave from work. The School's IT Department conducted a school-wide checking of desktop computers used in the school.
- Three videos were discovered on Jay's computer . Each video shows that he was having sexual intercourse with a woman who is not his wife.

WORKSHOP : CASE STUDY

- After an investigation, the school suspended Jay from work for six months.
- Jay assails the decision of the school to suspend him, contending that his right to privacy was violated, arguing that:

1. The photos that he uploaded on Facebook cannot be used against him since Pedro intruded Jay's privacy by downloading the pictures and then showing them to the School principal.

2. The school invaded his privacy when the IT Department opened his desktop computer without his knowledge and consent.

THANK YOU!