



# The Data Privacy Act and the National Privacy Commission: **Building a Regime of Trust**

Raymund E. Liboro

Privacy Commissioner and Chairman

National Privacy Commission



What the law is  
all about



How it will affect  
YOU

# — KEY TAKEAWAYS —

1

Introduction to  
Data Privacy  
and the Data  
Privacy Act

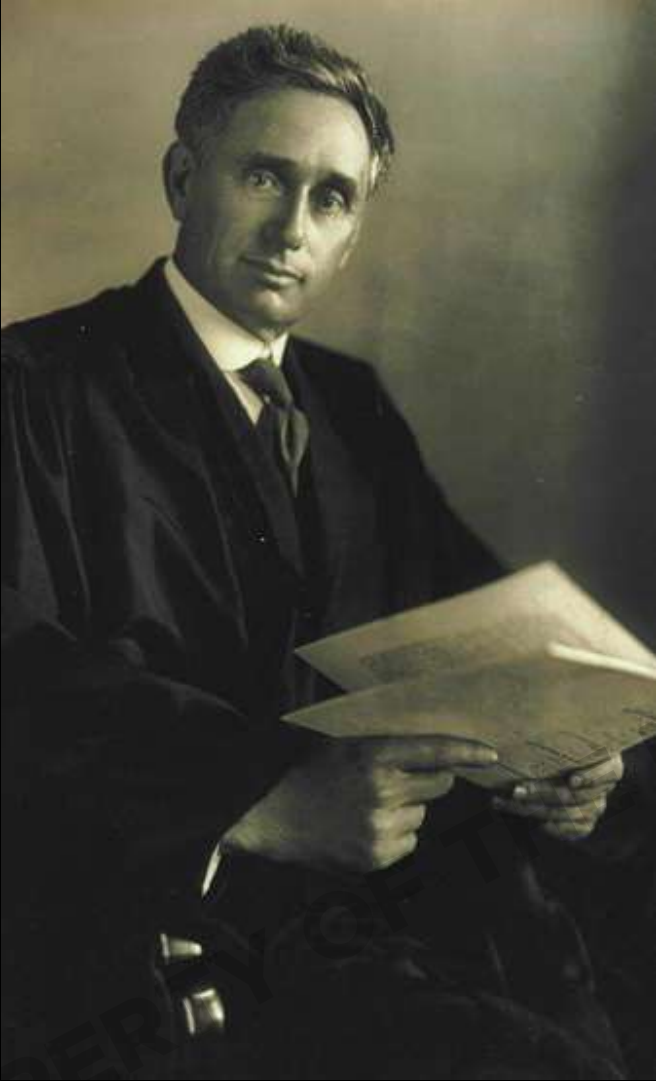
2

DPA Principles &  
The Information  
Life Cycle

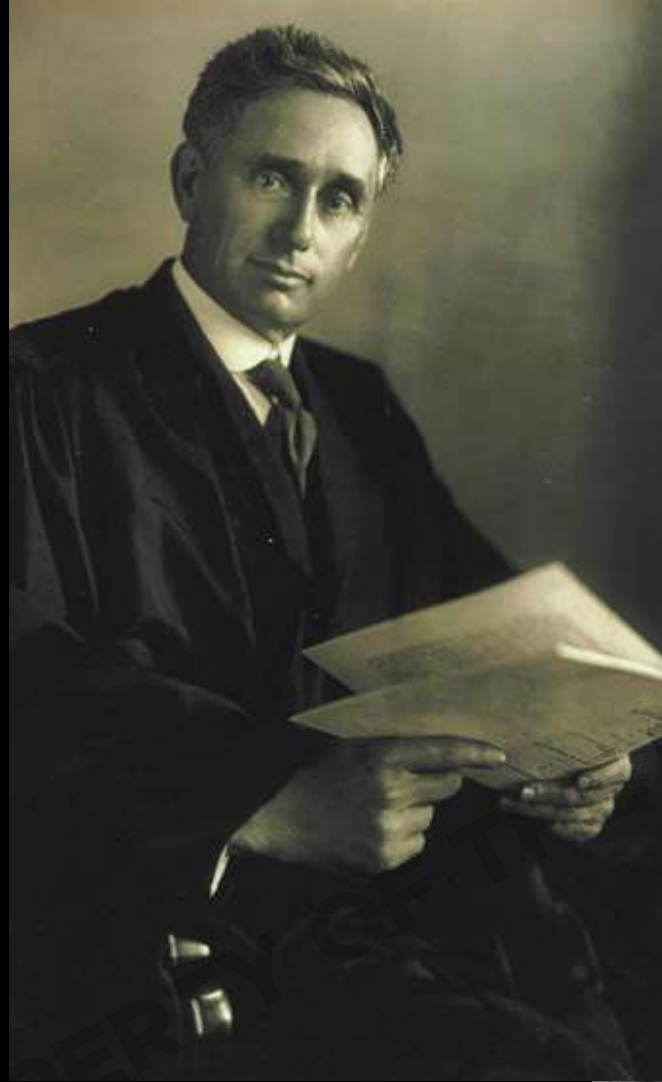
3

HOW NOT TO  
GET IN TROUBLE  
WITH THE DPA

PROPERTY OF THE NATIONAL PRIVACY COMMISSION



<https://timeline.com/how-the-first-mass-market-camera-led-to-the-right-to-privacy-and-roe-v-wade-4fb4cd87d7a>



# RIGHT TO PRIVACY

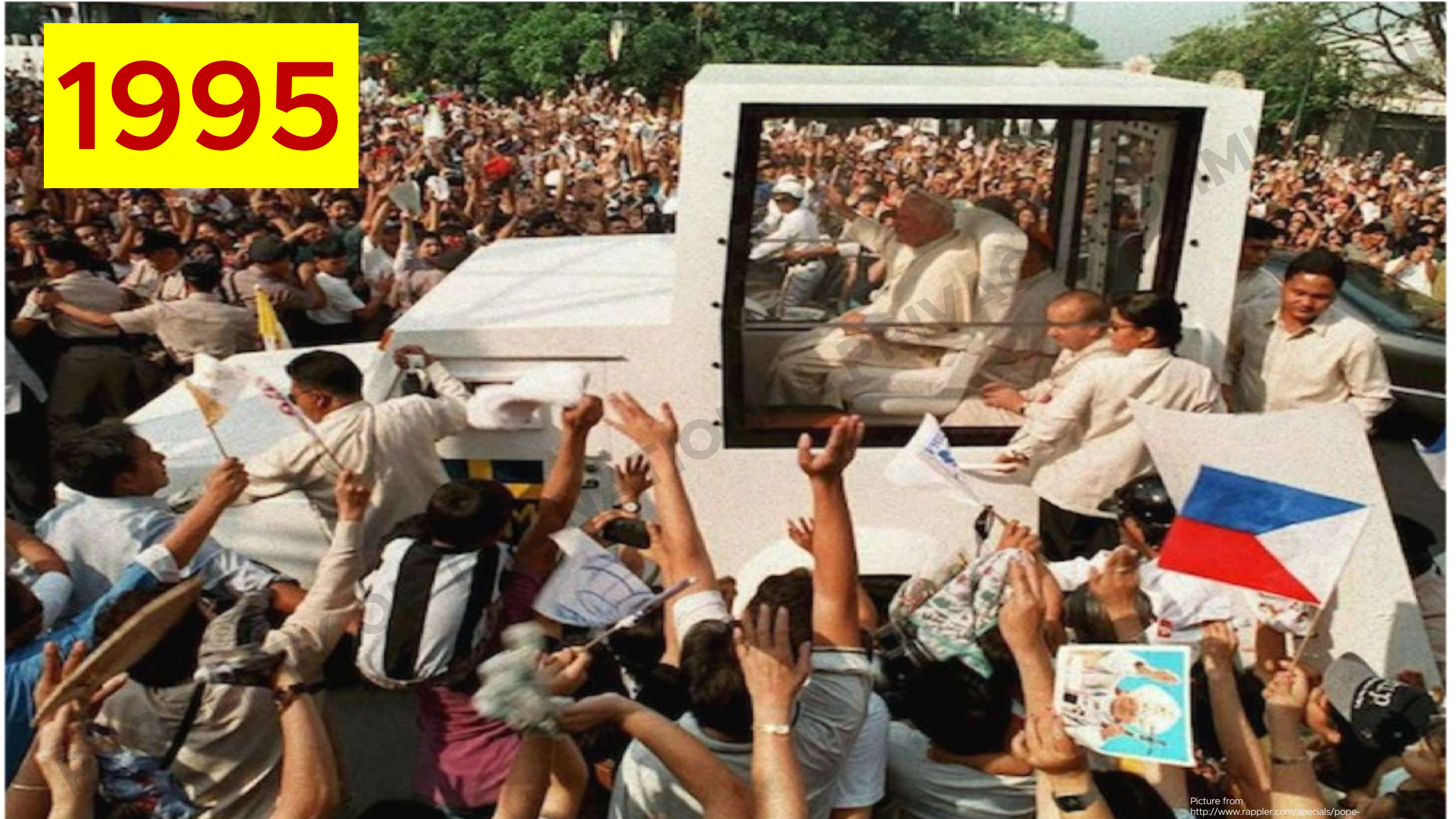
---



“the right to be let alone -  
the most comprehensive of  
rights and the right most  
valued by civilized men”

[Brandeis J, dissenting in *Olmstead v. United States*, 277 U.S. 438 (1928)].

# 1995



Picture from  
[http://www.rappler.com/specials/pope-  
assassination-plot](http://www.rappler.com/specials/pope-john-paul-ii-1981-1985-1986-1987-1988-1989-1990-1991-1992-1993-1994-1995-1996-1997-1998-1999-2000-2001-2002-2003-2004-2005-2006-2007-2008-2009-2010-2011-2012-2013-2014-2015-2016-2017-2018-2019-2020-2021-2022-2023-2024-2025)

1995









**UBER**

The world's largest taxi company, **owns no vehicles.**



**FACEBOOK**

The world's most popular media owner, creates **no content.**



**ALIBABA**

The world's most valuable retailer, has **no inventory.**



**AIRBNB**

The world's largest accommodation provider, owns **no real estate.**

The  
Economist

MAY 6TH-12TH 2017

Crunch time in France

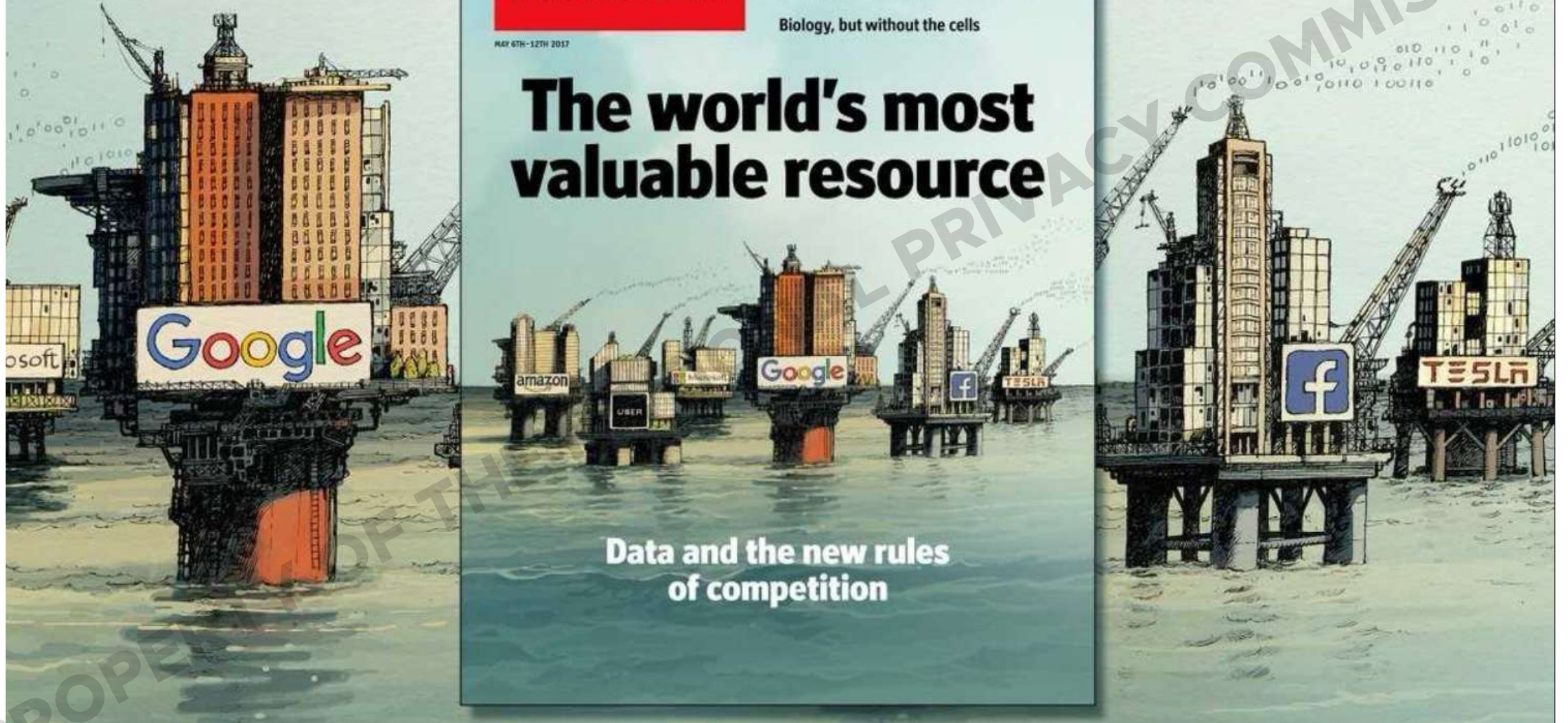
Ten years on: banking after the crisis

South Korea's unfinished revolution

Biology, but without the cells

# The world's most valuable resource

Data and the new rules  
of competition

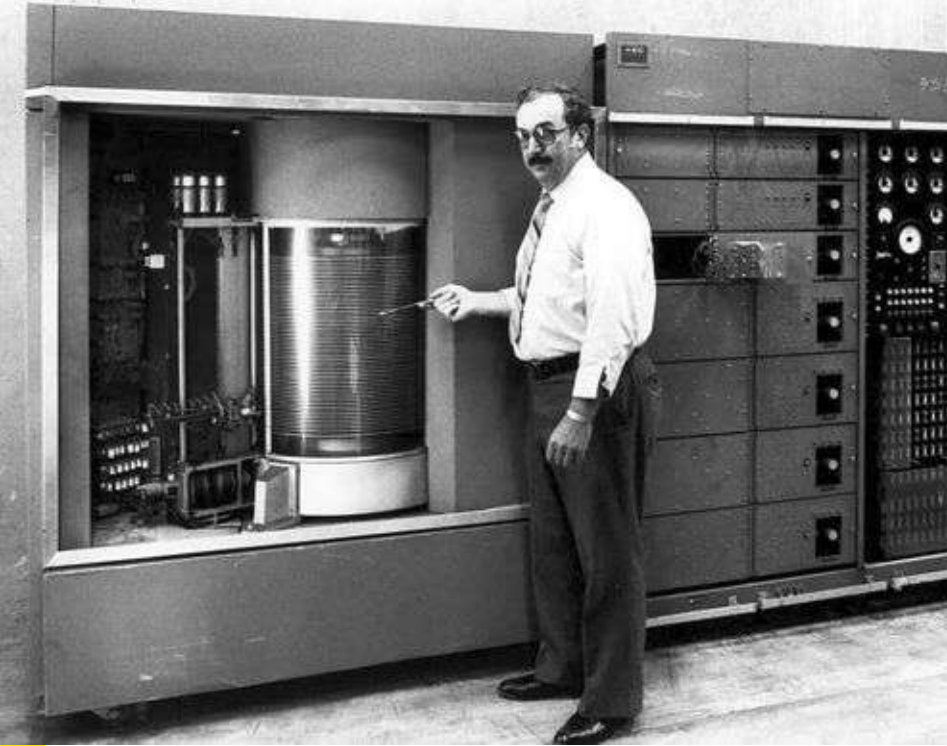


# DISRUPTION

the displacement of established technology by being replaced with a new one

PROPERTY OF THE NATIONAL PRIVACY COMMISSION



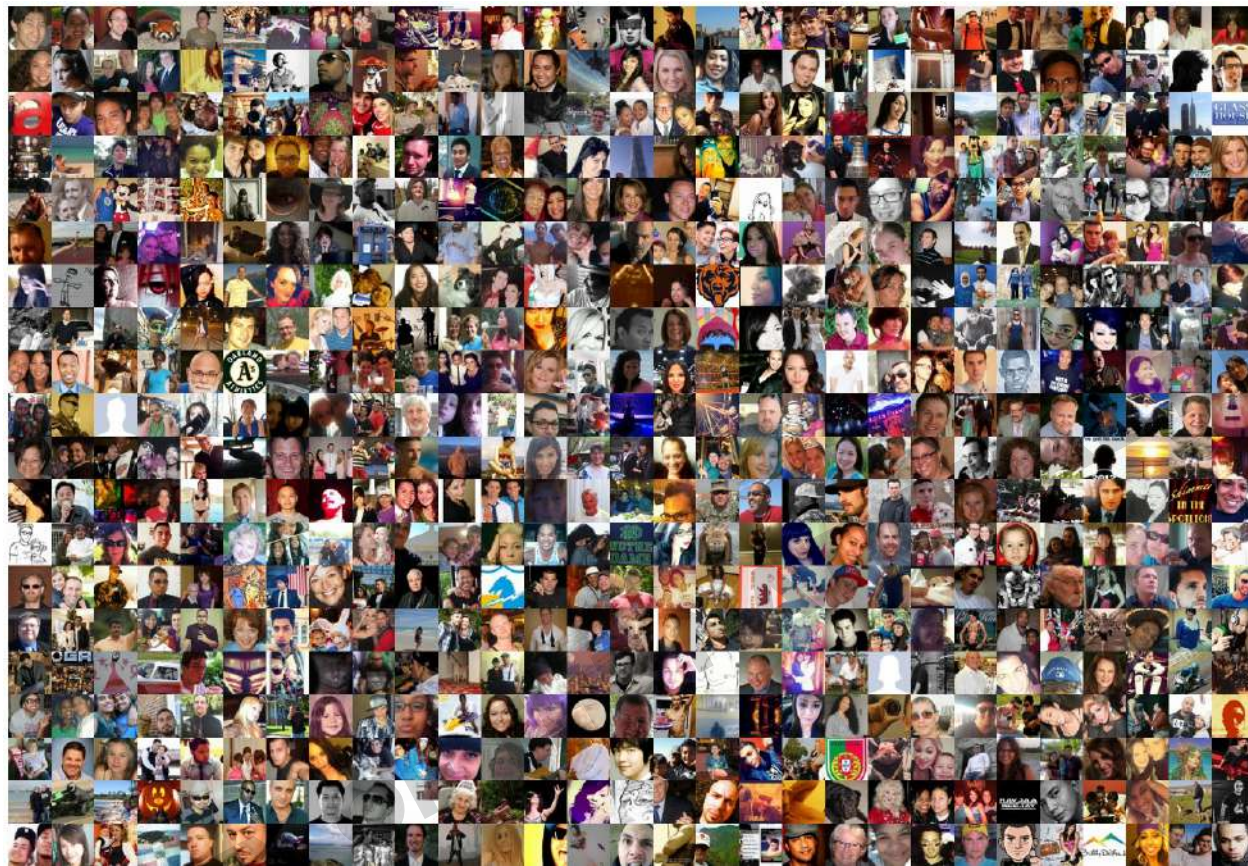


1956

**Model 350 RAMAC** unit  
stored the equivalent of  
5 megabytes

1  
megabyte = 1  
million dollars \$

Cross-Border Data Flow has grown **astronomically**



..To 210  
terabytes  
Per second  
in  
**2017**

**That's 1.6 Billion Selfies a Minute**

Reference: Computerworld Magazine as noted by the McKinsey Singapore Office

[http://s17026.pcdn.co/wp-content/uploads/sites/11/2017/08/AdobeStock\\_135873223-634x0-c-default.jpeg](http://s17026.pcdn.co/wp-content/uploads/sites/11/2017/08/AdobeStock_135873223-634x0-c-default.jpeg)

# WHAT IS PERSONAL DATA?

age

name

net worth

internet searches

marital status

email

astrological sign

car owner

voting habits

kids in house

downloads

clicks

political party

criminal record

purchases

average spending

usernames

homeowner

# WHAT IS PERSONAL DATA?

age

name

net worth

internet searches

marital status

email

astrological sign

car owner

voting habits

kids in house

downloads

clicks

political party

criminal record

purchases

average spending

usernames

homeowner



# WHAT IS PERSONAL DATA?



- Full name
- Passport number
- Vehicle license plate number
- Photograph / Video images of an individual
- Mobile telephone number
- Personal email address
- Thumbprint
- DNA profile
- Name and residential address
- Name and residential telephone number



# The Data Privacy Act (“DPA”) of 2012

Data privacy - acknowledging the rights of Data Subjects over their data and enforcing the responsibilities of entities who process them



# ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select ▼

[See Your Matches »](#)

Over **37,565,000** anonymous members!



**As seen on:** Hannity, Howard Stern, TIME, BusinessWeek, Sports Illustrated, Maxim, USA Today

**Ashley Madison** is the world's leading married dating service for **discreet** encounters



Trusted Security Award



SSL Secure Site

Over **39,470,000** anonymous members!

# ASHLEY MADISON®

Life is short. Have an affair.®

Get started by telling us your relationship status:

Please Select

See your Match

Over 37,65,000 anonymous members!

HACKED!

# DISCRIMINATION

People are discriminated because of their race, color or ethnic origin

## Stigmatization



# Unfair Decision-Making

## Based on Profiling

Personal information such as **marital status, religious or political affiliations** affects the decision-making of companies in various cases.

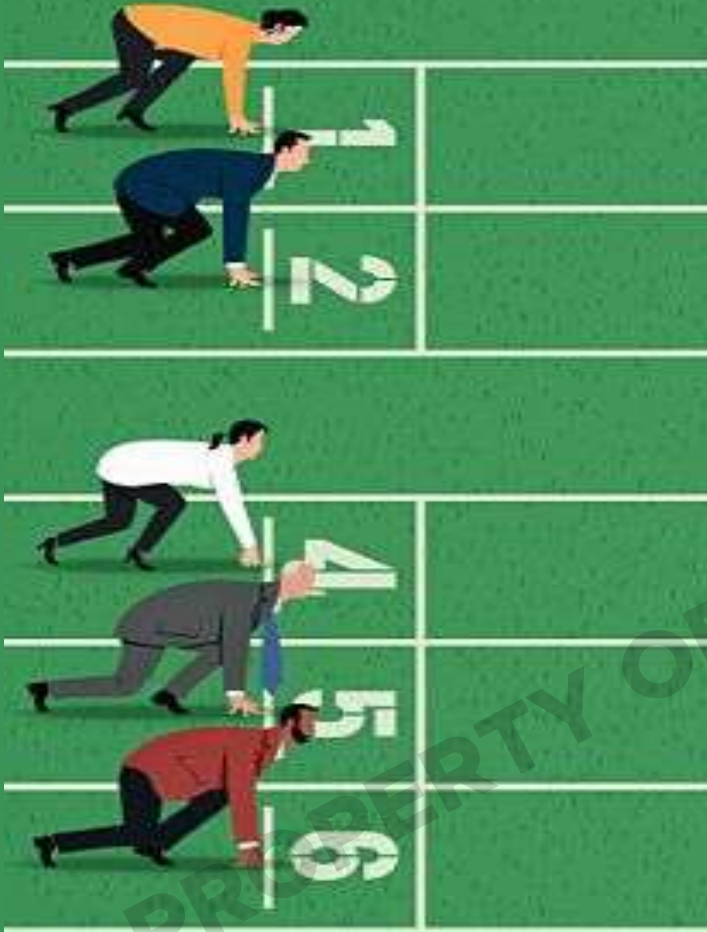
In employment, some experience difficulties in getting hired while others are unfairly dismissed.



# Sources of Data used in Profiling

## | Types of data used in profiling:

- Internet search and browsing history
- Education and professional data
- Data derived from existing customer relationships
- Data collected for credit-worthiness assessments;
- Financial and payment data;
- Consumer complaints or queries
- Driving and location data
- Property ownership data
- Information from store cards and credit cards
- Consumer buying habits
- Wearable tech, such as fitness trackers
- Lifestyle and behavior data gathered from mobile
- Social network information
- Video surveillance systems
- Internet of things
- telematics



# Identity Theft



Access to personal information such as name, date of birth, address, or email address can result to fraudsters victimizing individuals.





1004



30



2



0

## Public school teacher in debt because of identity theft

Published February 26, 2016 10:48pm

A public school teacher may be a victim of identity theft as he owes three banks P800,000 for loans he did not apply for, according to a report by John Consulta on GMA-7's "24 Oras" on Friday.

~~Mark Joseph Lontok~~ said he received notifications from three banks saying that he borrowed a total of P800,000 in salary loans. He denied applying for the loans.

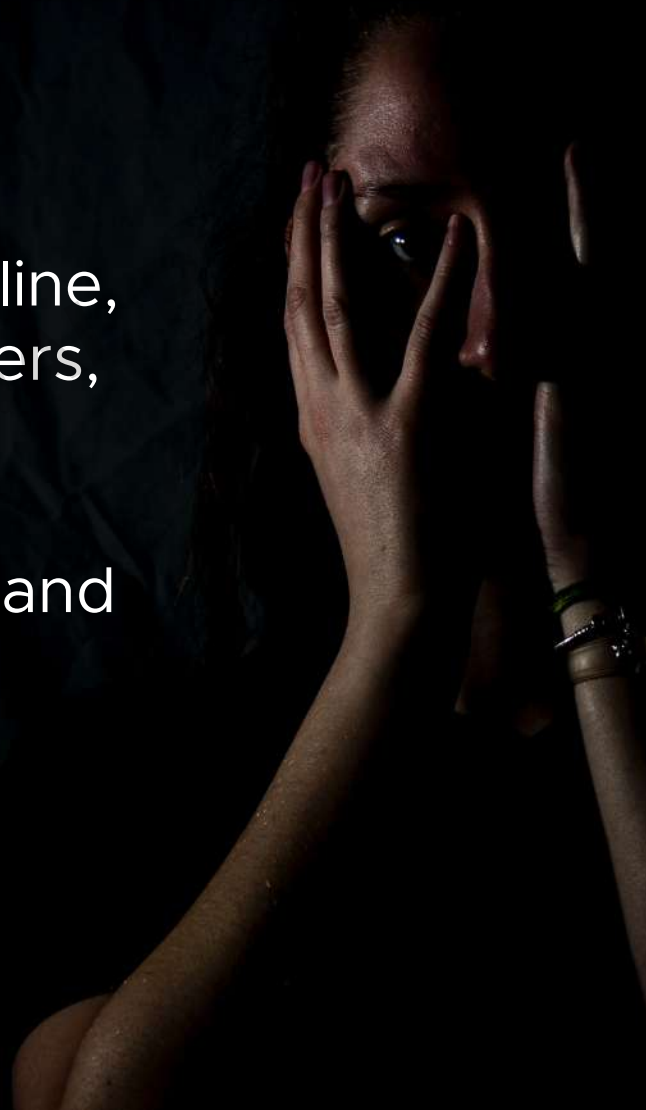
However, ~~Lontok~~ remembered posting a photo of his Professional Regulation Commission (PRC) ID online.

ako. I saka pagpasok ko po sa public (school), pagbigay ng papel ko, pinost din po sa FB (Facebook) sa sobrang tuwa ko po," he said.

"Wala naman akong ginagawang masama," he added.

# Loss of Reputation

People have experienced stalking or harassment online, trouble with family members, lost a job or educational opportunity because of something posted online, and even as grave as physical danger.





# CANISTER SCANDAL: 90-day suspension of 2 docs, nurse ends



- Helen Flores, Ghio Ong () - September 6, 2008 - 12:00am

<https://www.philstar.com/nation/2008/09/06/398622/canister-scandal-90-day-suspension-2-docs-nurse-ends>

Health Undersecretary Alexander Padilla said yesterday the three medical practitioners who were linked to the “canister scandal” at a Cebu hospital were allowed to go back to work after serving the three-month suspension imposed on them by the Department of Health (DOH).

Dr. Philipps Leo Arias, Dr. Joseph Montecillo and nurse Carmenia Sapio reported for duty at the government-run Vicente Sotto Memorial Medical Center sometime last month.

Padilla said the DOH has already imposed enough sanctions on the three and that the matter is already in the hands of the Ombudsman.

# Loss of Autonomy

ABS-CBN NEWS

## Top Gear sorry for identifying wrong suspect in road rage


MANILA - The editor of Top Gear Philippines has **apologized** for posting on its Facebook page a link to the social media account of the wrong person being linked to a **fatal road rage incident** in Quiapo, Manila last Monday.

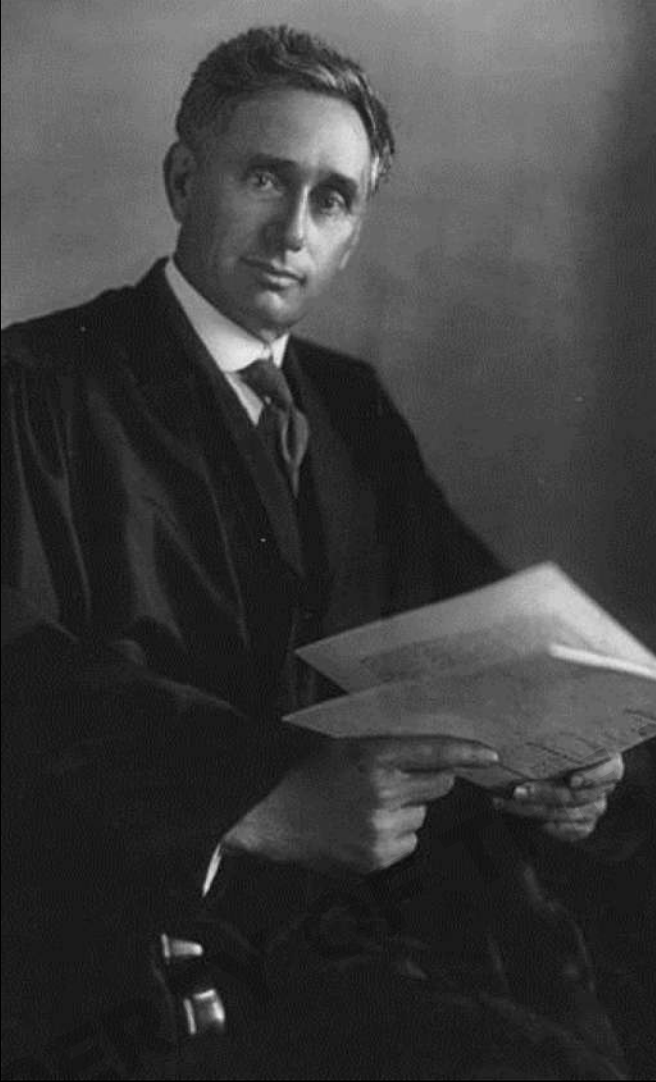
Top Gear editor Vernon Sarne took full responsibility for posting the link to the Facebook profile of Nelson Punzalan, who had been apparently falsely accused as the killer of cyclist Mark Vincent Geralde. Top Gear also posted a photo of Punzalan's car, which was coincidentally a Hyundai Eon model, similar to the car in the incident.

"I was responsible for posting the photo of Mr. Punzalan's vehicle, and I realize now that I shouldn't have done so. I accept full responsibility. This is all on me," Sarne said.

"The buck stops here. This is all my fault," he added.



July 25, 2016 –A jostle in the road between a car driver and cyclist led to a fist fight ended into a gun shooting, leaving the cyclist dead at P. Casal Street in Quiapo, Manila. Suspect left the scene of the crime leaving the dead victim lying on the street.  Nikon Celis, ABS-CBN News





The Data Privacy Act makes it mandatory for all data collectors — whether public or private — to protect the security, integrity and confidentiality of all the personal information they collect. **By doing this, we help usher in a truly knowledge-driven economy.**

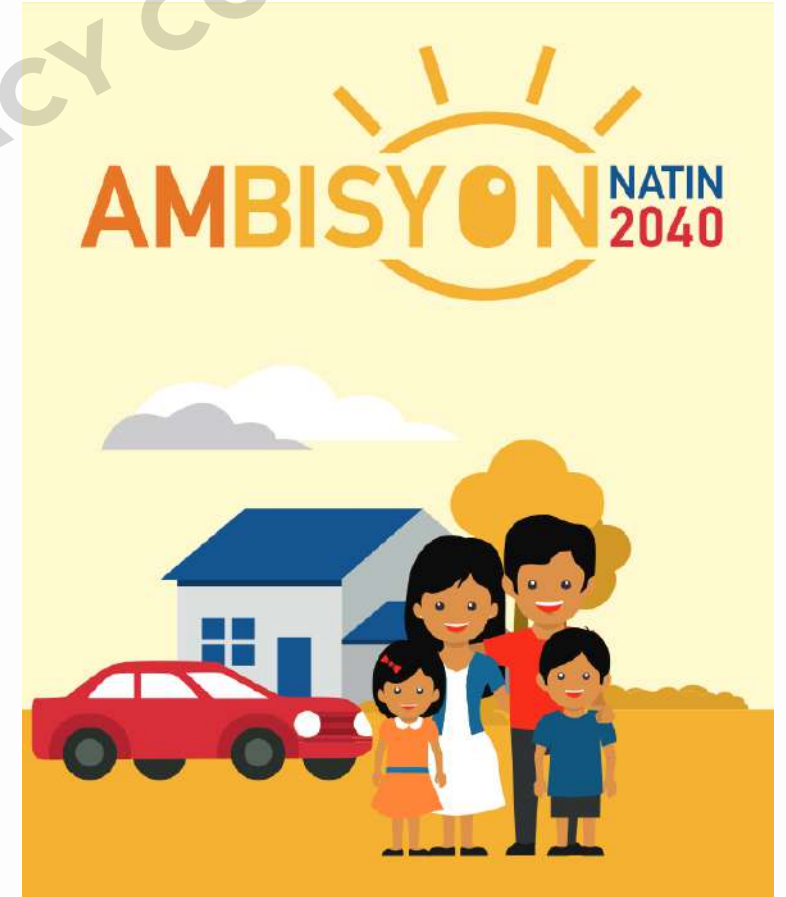
SENATOR EDGARDO ANGARA



# Philippine Development Plan

**By 2040, the Philippines is a prosperous middle class society where no one is poor. People live long and healthy lives and are smart and innovative.**

**The country is a high-trust society where families thrive in vibrant, culturally diverse, and resilient communities.**



# 21<sup>st</sup> Century Hazards and Risks



**Norse – Superior Attack Intelligence**  
 Norse maintains the world's largest dedicated threat intelligence network. With over 60,000 sensors that emulate over six thousand applications – from Apple laptops, to ATM machines, to closed-circuit TV cameras – the Norse Intelligence Network gathers data on what they're after. Norse delivers that data through the Norse Appliance, which pre-emptively monitors for threats, and the Norse Intelligence Service, which provides 24/7 threat monitoring for large networks.

**ATTACK TARGETS**

| #    | COUNTRY              |
|------|----------------------|
| 1000 | United States        |
| 970  | Australia            |
| 850  | United Arab Emirates |
| 750  | Singapore            |
| 650  | Hong Kong            |
| 550  | Germany              |
| 450  | Italy                |
| 350  | Romania              |
| 250  | France               |
| 150  | Philippines          |

| REGIONS       | ATTACK TYPES | ATTACK TARGETS | LIVE ATTACKS |
|---------------|--------------|----------------|--------------|
| North America | 1200         | 1000           | 100          |
| Europe        | 800          | 700            | 80           |
| Asia          | 600          | 500            | 60           |
| Africa        | 400          | 300            | 40           |
| Oceania       | 200          | 100            | 20           |

**LIVE ATTACKS**

| Timestamp    | Attacker                                   | Attacker IP    | Attacker Geo   | Target Geo   | Attack Type | Port |
|--------------|--|----------------|----------------|--------------|-------------|------|
| 14:56:21.719 | Microsoft Corporation                      | 207.46.100.252 | Redmond, US    | De Kalb      | smtp        | 25   |
| 14:56:20.770 | Philippine Long Distance Telephone Company | 122.3.47.120   | Paranaque, PH  | Lynnwood, US | telnet      | 23   |
| 14:56:20.770 | Philippine Long Distance Telephone Company | 122.3.47.120   | Paranaque, PH  | Lynnwood, US | telnet      | 23   |
| 14:56:20.580 | Microsoft Corporation                      | 65.55.169.249  | Washington, US | De Kalb      | smtp        | 25   |
| 15:05:41.557 | Philippine Long Distance Telephone Company | 122.54.132.220 | Makati, PH     | Dubai, AE    | telnet      | 23   |
| 14:56:19.784 | Microsoft Corporation                      | 207.46.100.250 | Redmond, US    | De Kalb      | smtp        | 25   |
| 15:04:02.333 | Philippine Long Distance Telephone Company | 122.3.47.120   | Paranaque, PH  | Lynnwood, US | telnet      | 23   |





# The Data Privacy Act of 2012



A 21st Century **Law**

**For 21st Century  
concerns...**



| ATTACK ORIGINS |               |     | ATTACK TYPES       |   | ATTACK TARGETS       |     | LIVE ATTACKS |                       |                          |                |                |                    |                 |        |
|----------------|---------------|-----|--------------------|---|----------------------|-----|--------------|-----------------------|--------------------------|----------------|----------------|--------------------|-----------------|--------|
| #              | COUNTRY       | #   | POSS. SERVICE TYPE | # | COUNTRY              | #   | ATTACKER IP  | ATTACKER OS           | TARGET OS                | ATTACK TYPE    | POINTS         |                    |                 |        |
| 102            | United States | 448 | 23                 | 0 | United States        | 102 | 20-41-22-852 | Chromecast            | Taiwanese Mobile Network | 143,148,19,191 | Hongkong, CN   | Systemdroid, US    | Health-Pharmacy | 1000.4 |
| 23             | China         | 106 | 23                 | 0 | United Arab Emirates | 232 | 20-41-22-858 | Microsoft Corporation | Microsoft Corporation    | 207.46.100.245 | Redmond, US    | De Kuth Jantana... | ...             | 25     |
| 21             | Netherlands   | 100 | 31                 | 0 | Spain                | 68  | 20-41-22-861 | Microsoft Corporation | Microsoft Corporation    | 207.46.100.251 | Redmond, US    | De Kuth Jantana... | ...             | 25     |
| 21             | Ukraine       | 98  | 9189               | 0 | Italy                | 21  | 20-41-22-878 | Microsoft Corporation | Microsoft Corporation    | 207.46.100.244 | Redmond, US    | De Kuth Jantana... | ...             | 25     |
| 24             | South Korea   | 48  | 5900               | 0 | Singapore            | 28  | 20-41-22-882 | Microsoft Corporation | Microsoft Corporation    | 192.168.1.111  | Redmond, US    | De Kuth Jantana... | ...             | 25     |
| 21             | Columbia      | 38  | 443                | 0 | France               | 25  | 20-41-22-891 | Microsoft Corporation | Microsoft Corporation    | 93.55.142.220  | Washington, US | De Kuth Jantana... | ...             | 25     |
| 21             | Southland     | 38  | 52413              | 0 | Belgium              | 15  | 20-41-22-900 | Microsoft Corporation | Microsoft Corporation    | 192.168.1.111  | Redmond, US    | De Kuth Jantana... | ...             | 25     |
| 18             | Turkey        | 32  | 10268              | 0 | Belgium              | 11  | 20-41-22-902 | Microsoft Corporation | Microsoft Corporation    | 128.71.55.53   | Redmond, US    | De Kuth Jantana... | ...             | 25     |
| 12             | Poland        | 25  | 1004               | 0 | Saudi Arabia         | 10  | 20-41-22-904 | Microsoft Corporation | Microsoft Corporation    | 192.168.1.111  | Redmond, US    | De Kuth Jantana... | ...             | 25     |

Photo from Norse Website Real-time Cyber Attacks

# The Data Privacy Act of 2012



## DATA PRIVACY ACT OF 2012

Republic of the Philippines  
Congress of the Philippines  
Metro Manila  
Fifteenth Congress  
Second Regular Session



enacted in Metro Manila, on Monday, the twenty-fifth day of July, two thousand eleven.

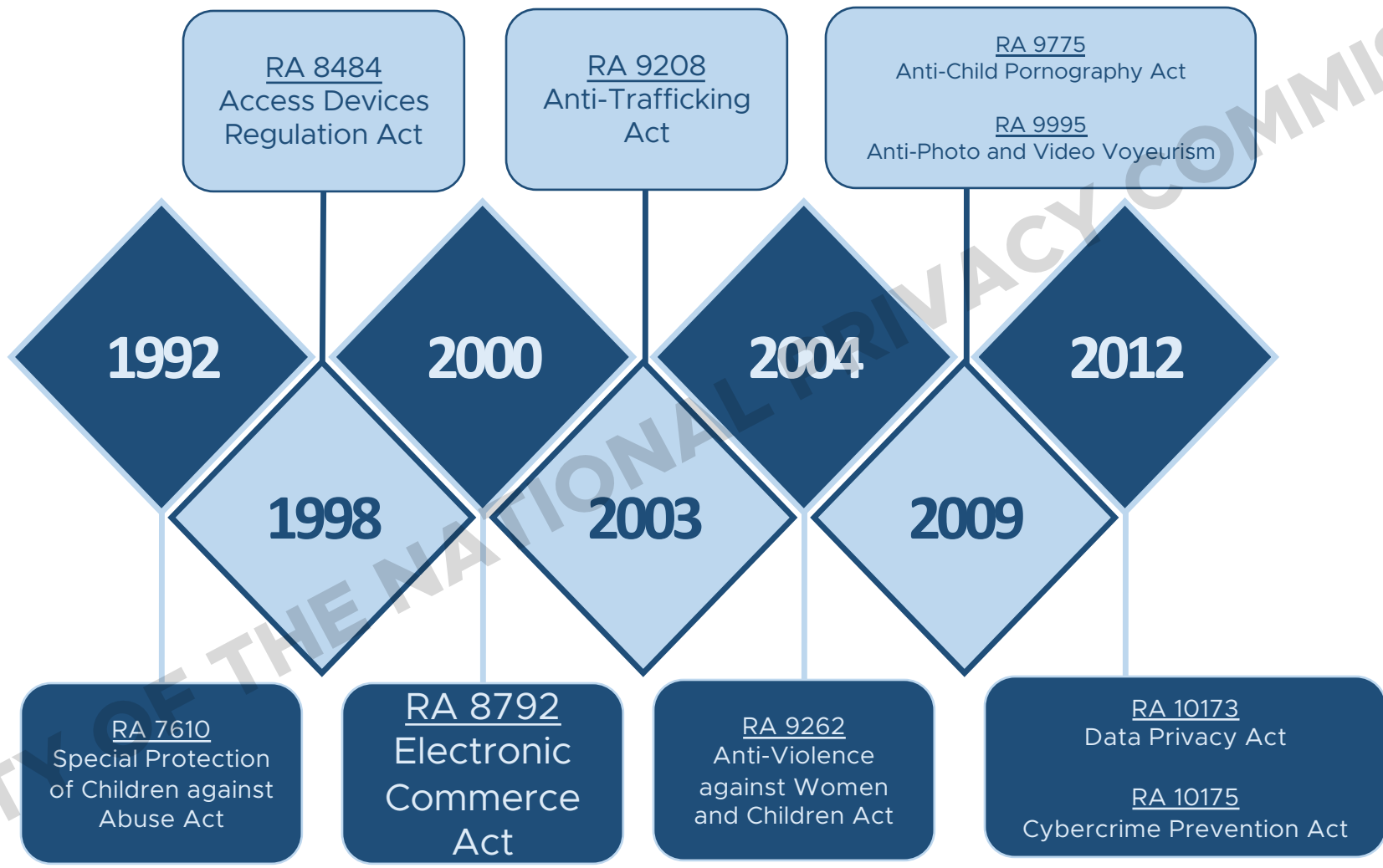
### REPUBLIC ACT NO. 10173

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

*Be it enacted, by the Senate and House of Representatives of the Philippines in Congress assembled:*

# Philippine Constitution: Article 3, Bill of Rights

- Section 2. Right to be secure in their persons, houses, papers, and effects against unreasonable searches
- Section 3. Privacy of communication and correspondence
- Section 5. Free exercise and enjoyment of religious profession and worship
- Section 6. Liberty of abode and the right to travel
- Section 8. Right to information, and access to official records



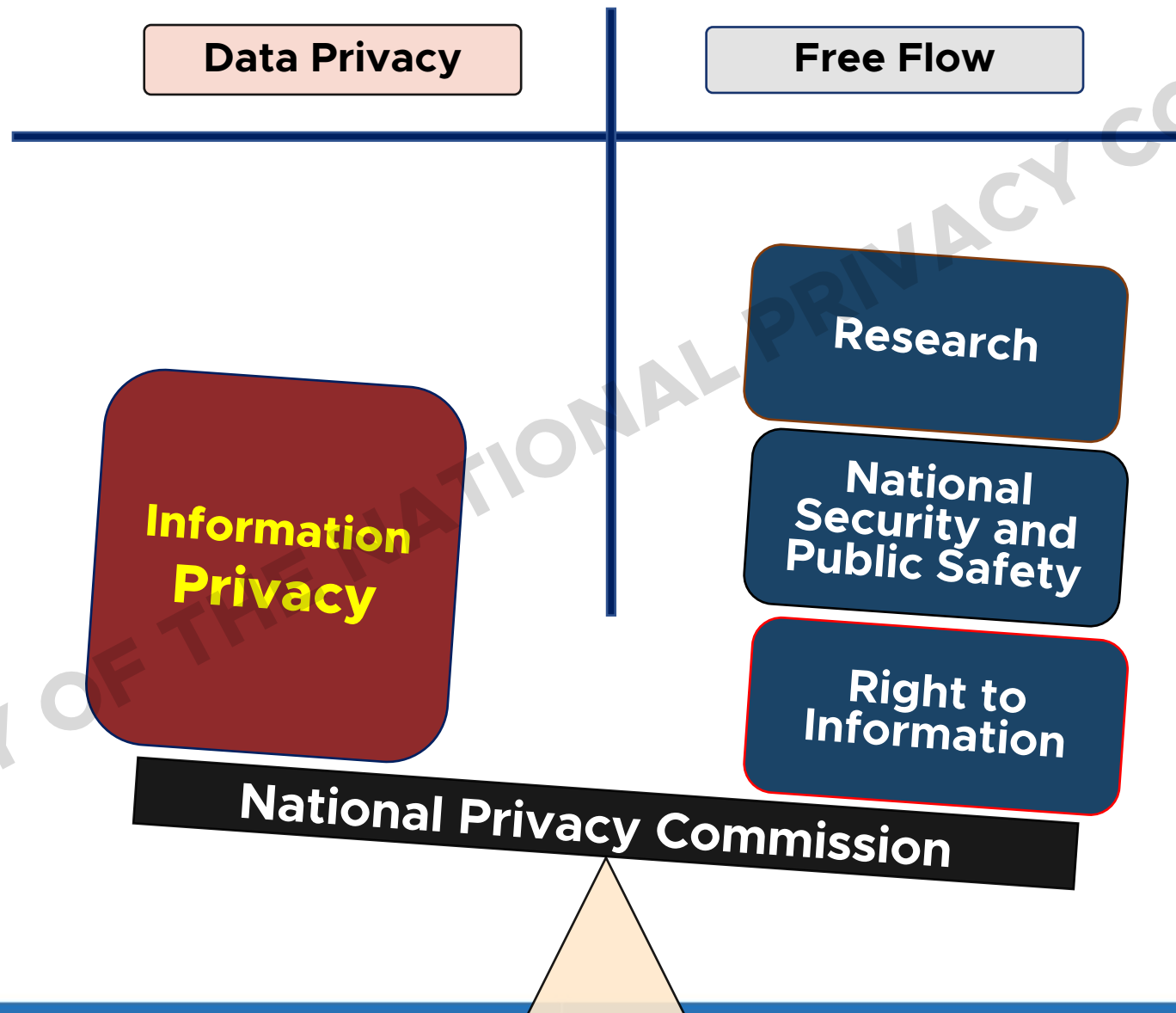
# DATA PRIVACY ACT *of* 2012

# **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**

# Balancing Data Privacy and the Free Flow of Information



# Sections of the DPA



## SECTION 1 - 6

Definitions  
and General  
Provisions



## SECTION 7 - 10

National  
Privacy  
Commission



## SECTION 11 - 21

Rights of Data  
Subjects  
and Obligations  
of Personal  
Information  
Controllers and  
Processors



## SECTION 22 - 24

Provisions  
specific to  
Government



## SECTION 25 - 37

Penalties





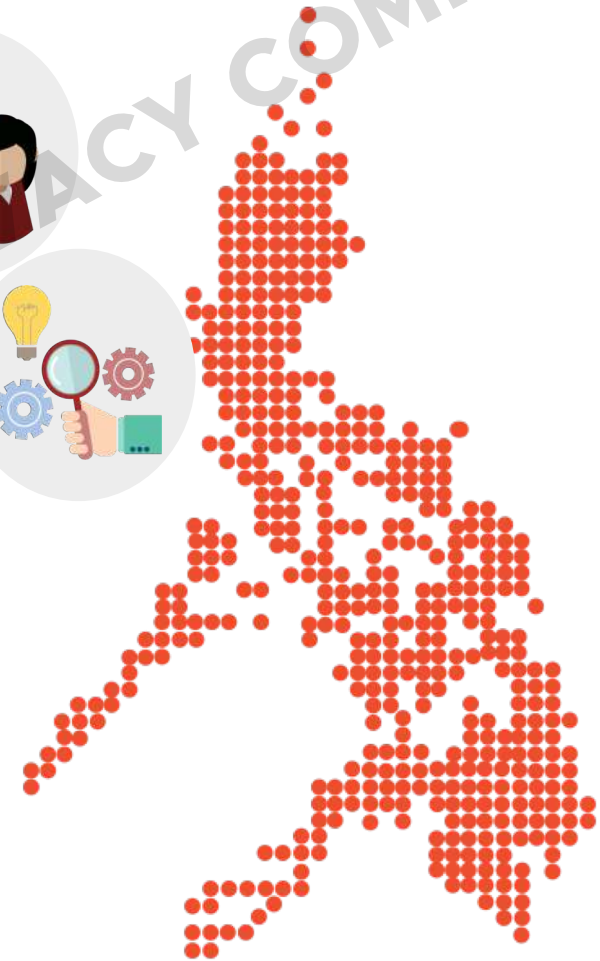
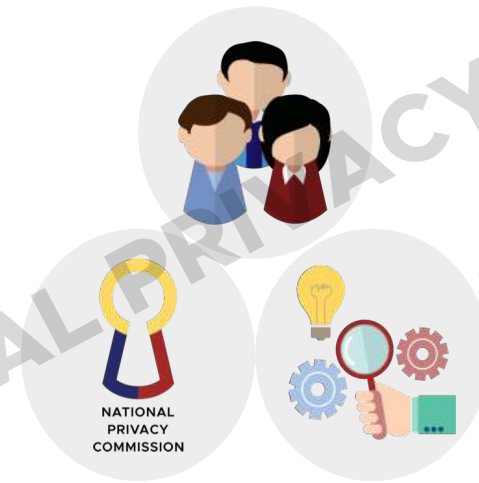
# Scope

of the DPA

PROPERTY OF THE NATIONAL PRIVACY COMMISSION

# Scope

- government and the private sector
- processing of all types of personal information in the Philippines
- extraterritorial application in certain instances



# DPA **APPLIES** TO THE PROCESSING OF PERSONAL DATA



- By any natural & juridical person
- In the government or private sector
- In and outside of the Philippines

# This Act Shall Not Apply to the Following

An officer or employee of a government institution

- **Individual**

is or was an officer or employee of the **government institution**

- **Business contract & employee related information**

The title, business address and office telephone number of the individual

The classification, salary range and responsibilities of the position held by the individual

- **Employment Related Matters in the government** (including those performing service under contract)

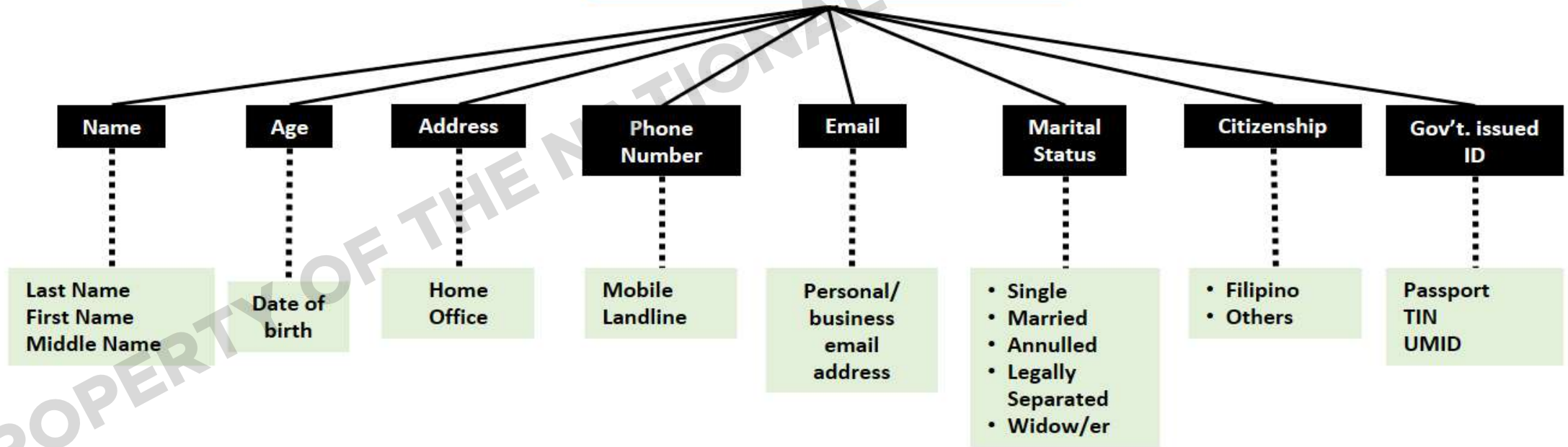
# This Act Shall Not Apply to the Following

- Journalistic, artistic, literary or research purposes
- Information necessary to carry out the functions of public authority
- Personal information originally collected from residents of foreign jurisdictions which is being processed in the Philippines

# KEY TERMS

# Personal Information

- any information from which the identity of an individual is apparent or can be reasonably or directly ascertained by the entity holding the information; or
- when put together with other information would directly and certainly identify an individual.

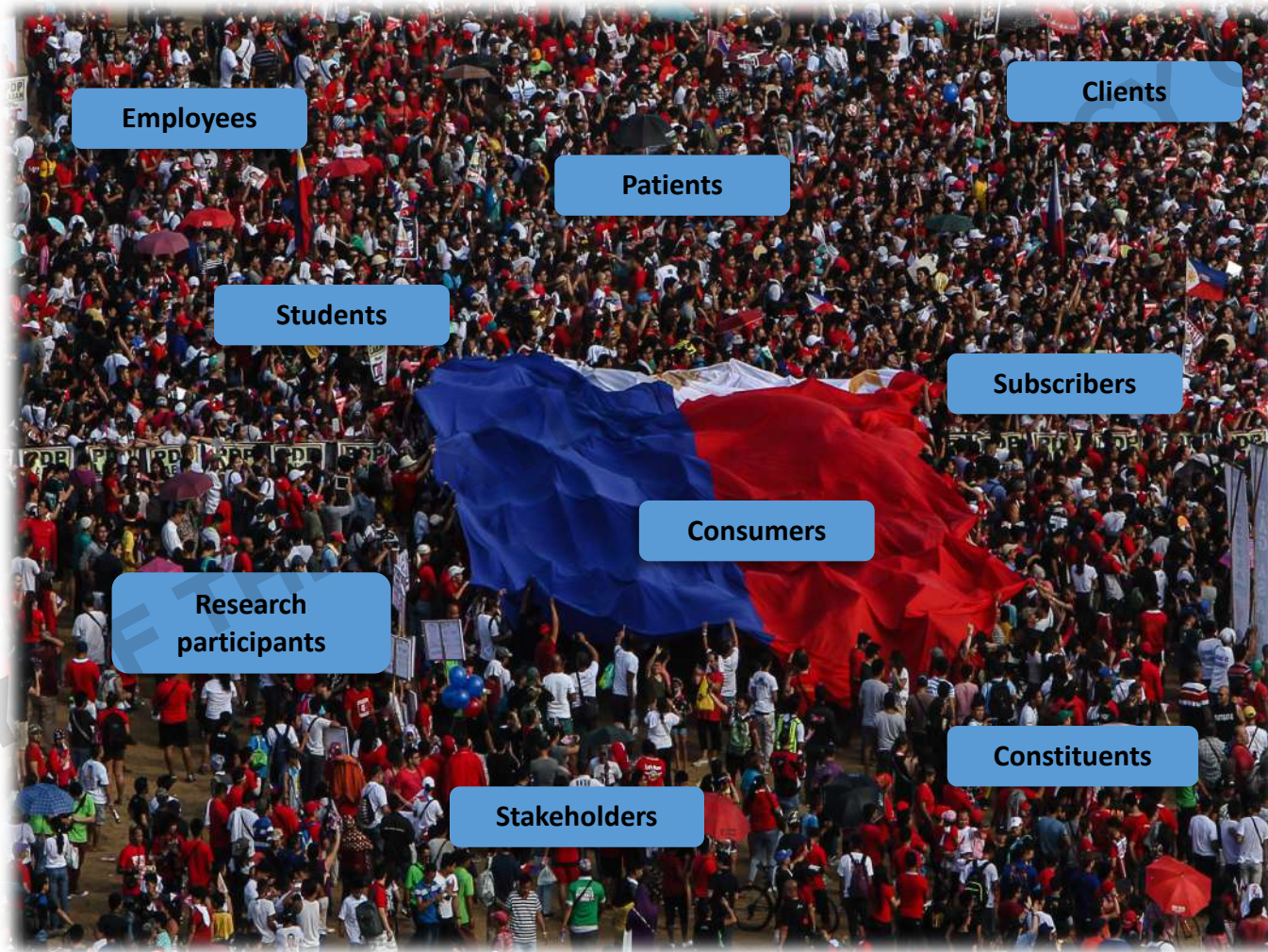




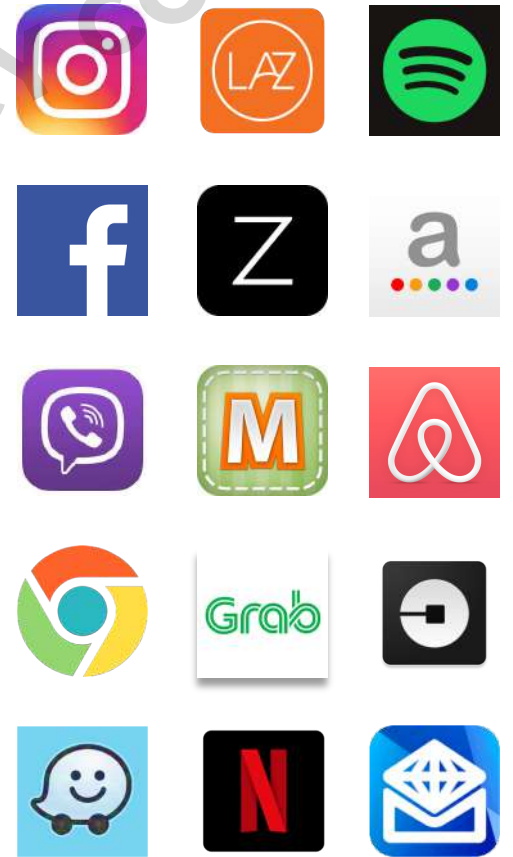
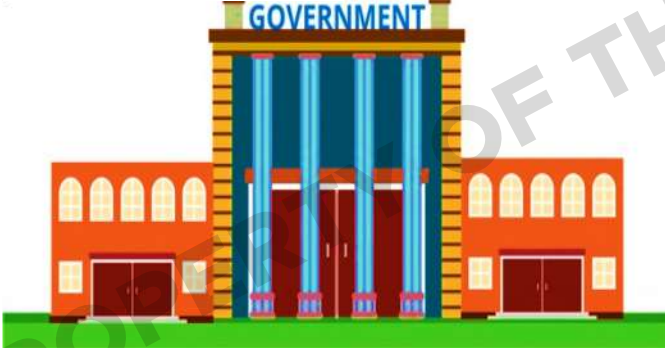
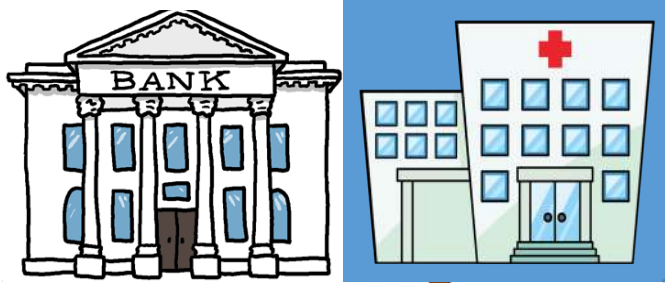
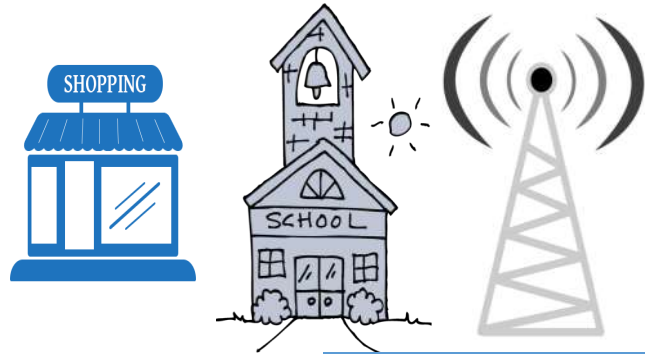
# Sensitive Personal Information

- race, ethnic origin, marital status, age, color and religious, philosophical, political affiliations
- health, education, genetic or sexual life, or to any proceeding for any offense committed or alleged to have been committed by the individual
- issued by government agencies peculiar to an individual (i.e. TIN, SSS Number, etc.)
- specifically established by law to be kept classified (i.e. Top Secret, Secret, Confidential, Restricted)

# Data Subject



# Personal Information Controller



# Personal Information Processor

Refers to any natural or juridical person or any other body to whom a PIC may **OUTSOURCE** or **INSTRUCT** the processing of personal data

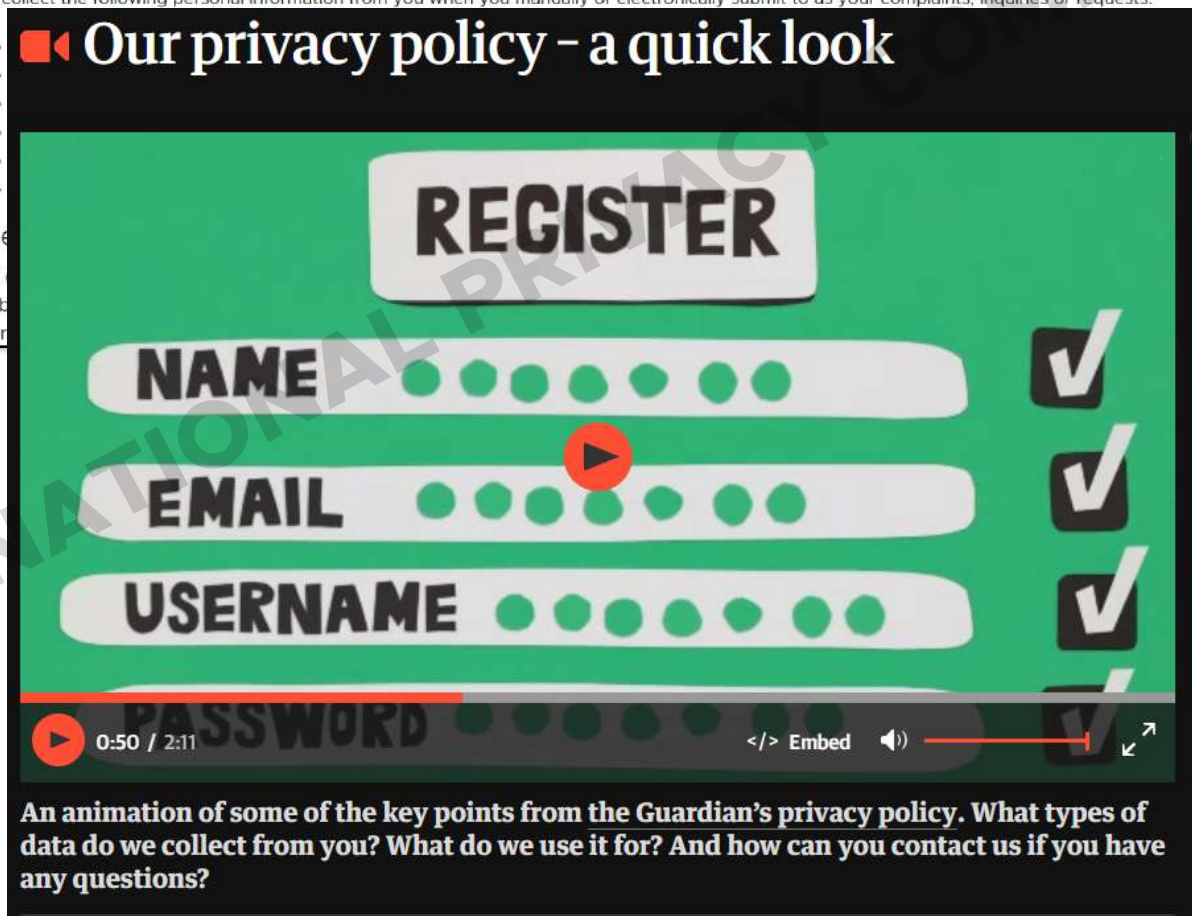
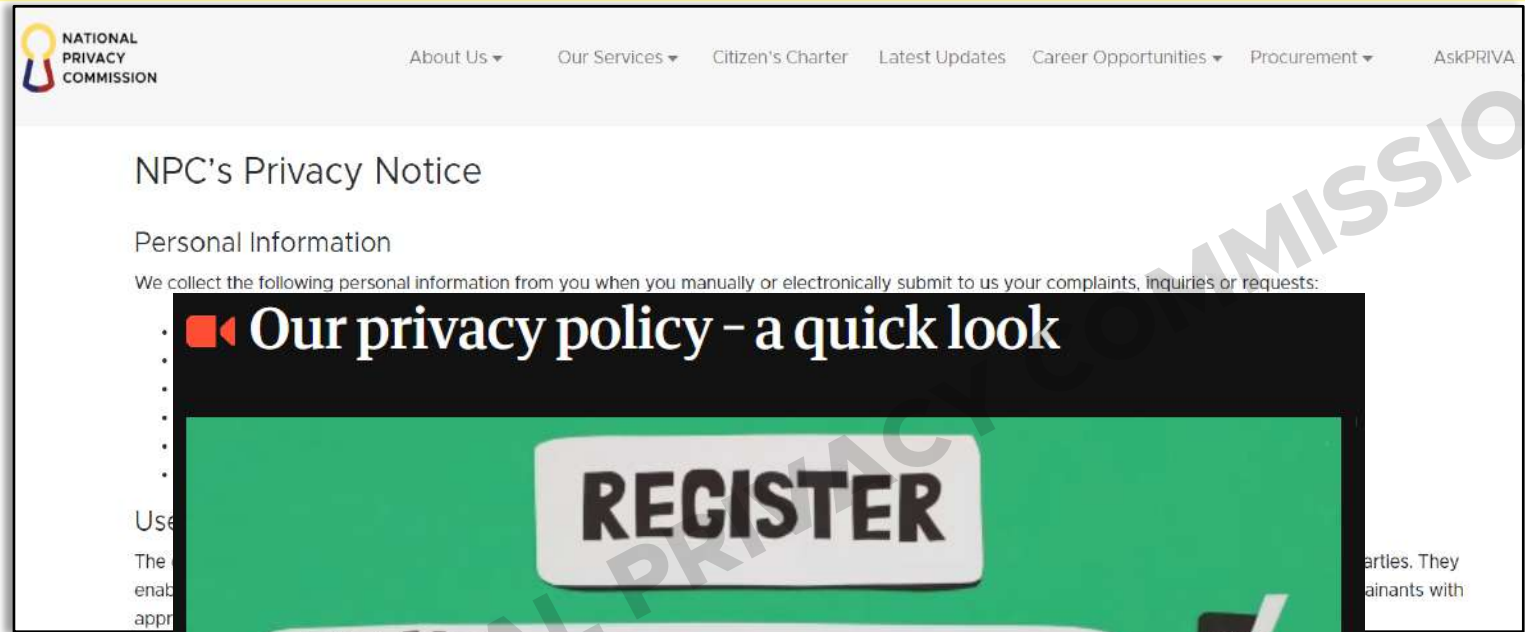
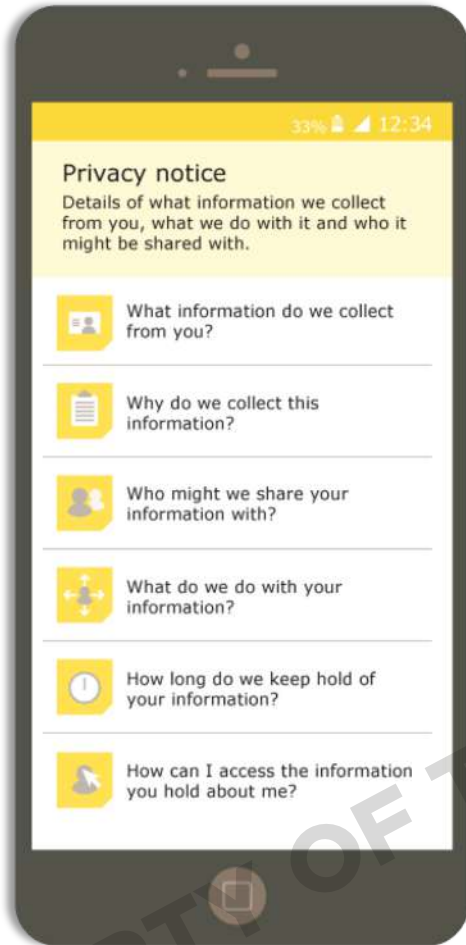


**General  
Data Privacy  
Principle**

explicability  
clarity  
simplicity  
unambiguity  
perceptibility  
manifestness  
**transparency**  
translucence  
openness  
conspicuousness  
clearness  
decipherability

# Right to INFORMATION

| WHAT INFORMATION MUST BE SUPPLIED?   | WHEN SHOULD INFORMATION BE PROVIDED?  |
|--|---|
| 1. Description of the personal data  | <ul style="list-style-type: none"><li>• before the entry of personal data into the processing system<br/>or</li><li>• at the next practical opportunity</li></ul> |
| 2. Purposes for processing; including: direct marketing, profiling, or historical, statistical or scientific purpose |   |
| 3. Basis of processing (legal mandate, contract, etc.)   |   |
| 4. Scope and method of the processing  |   |
| 5. Recipients/classes of recipients to whom the personal data are or may be disclosed                                |   |
| 6. Identity and contact details of the personal information controller   |   |
| 7. Retention period  |   |
| 8. Existence of rights as data subjects.   |   |



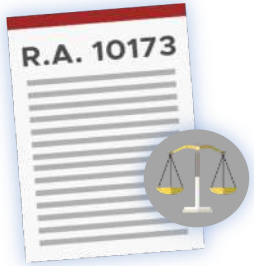


# Rights

of the data subject

PROPERTY OF THE NATIONAL PRIVACY COMMISSION





# The Rights of the Data Subject

- ✓ **Right to be informed - Why are you processing my data?**
- ✓ **Right to object - I don't want to do this survey anymore?  
Stop videotaping me.**
- ✓ **Right to access - What do you know about me?**
- ✓ **Right to correct/rectify - I want to amend/correct my details.**
- ✓ **Right to block/remove - Remove me from your database.**
- ✓ **Right to data portability - I want a copy of my data.**
- ✓ **Right to file a complaint**
- ✓ **Right to be indemnified**

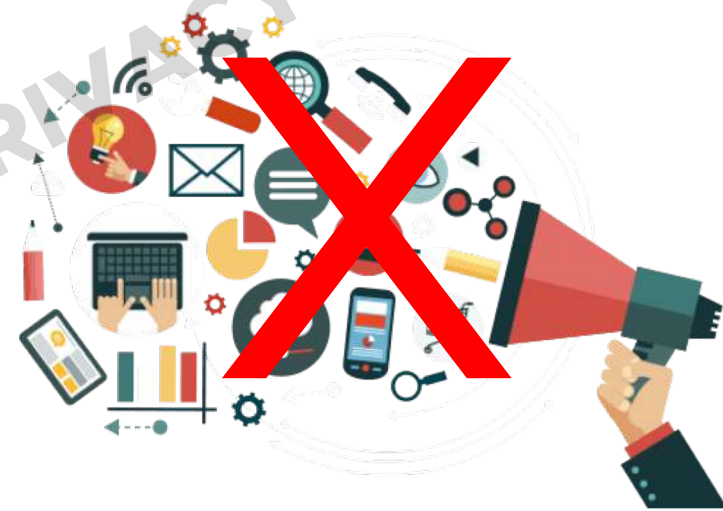
# Right to OBJECT

When does the right apply?

- processing is based on **consent** (includes direct marketing)
- processing is based on **legitimate interest**

If processing is for direct marketing purposes:

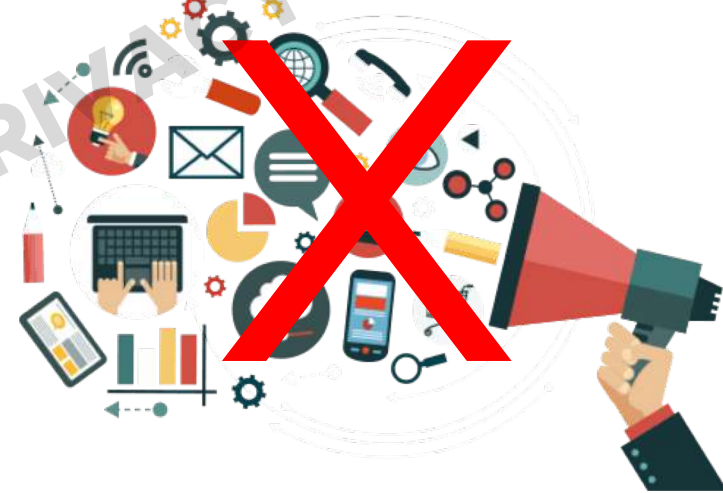
- PIC must stop processing upon receipt of data subject's objection.



# Right to OBJECT

If a data subject objects/ withholds consent, the PIC shall no longer process the personal data, unless the processing is:

1. Pursuant to a subpoena;
2. For obvious purposes, i.e. contract, employer-employee relationship, etc.; or
3. Result of a legal obligation.



# Right to ACCESS

Reasonable access to the following:

1. Contents of personal data;
2. Sources of personal data;
3. Names & addresses of recipients of the personal data;
4. Manner by which such data were processed;
5. Reasons for the disclosure of the personal data;
6. Information on automated processes (data will or likely to be made as the sole basis for decisions significantly affecting the data subject);
7. Date when personal data was last accessed/modified; and
8. Name/address of the PIC.



# Right to ERASURE OR BLOCKING

When does the right apply?



- a. When personal data is:
  - incomplete, outdated, false, or unlawfully obtained
  - used for unauthorized purpose
  - no longer necessary for the purpose
- b. Data subject withdraws consent/objects to the processing, and there is no other legal ground/legitimate interest for processing
- c. Processing is unlawful
- d. PIC or PIP violated the rights of the data subject.

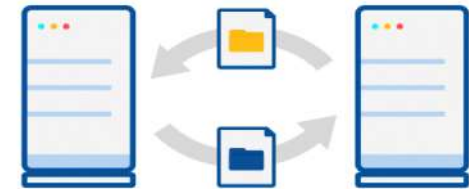
## Right to RECTIFICATION

- Right to dispute the inaccuracy or error in the personal data and have the PIC correct it immediately, unless the request is vexatious or otherwise unreasonable.
- If personal data was disclosed to third parties: PIC must inform them of the rectification upon reasonable request of the data subject.



## Right to DATA PORTABILITY

- Right to obtain from the PIC a copy of personal data in an **electronic/ structured format** that is commonly used/allows further use by the data subject.
- What are the **conditions** for this right to apply?
  - ✓ personal data requested concerns the data subject making the request;
  - ✓ personal data is processed electronically; and
  - ✓ processing is based on consent or contract.



## Right to DAMAGES

- The data subject shall be indemnified for any damages sustained due to such inaccurate, incomplete, outdated, false, unlawfully obtained or unauthorized use of personal data, taking into account any violation of his or her rights and freedoms as data subject.
- See: NPC Circular No. 16-04 – Rules of Procedure



**General  
Data Privacy  
Principle**

lawful objective reasonable justifiable authorized sanctioned  
**legitimate purpose**  
genuine appropriate statutory proper accepted  
fair

# Legitimate Purpose Consent



The data subject agrees to the collection and processing of personal information

- ✓ **Freely given**
- ✓ **Specific**
- ✓ **Informed indication of will**

Evidenced by written, electronic or recorded means:

- ✓ signature
- ✓ opt-in box/clicking an icon
- ✓ sending a confirmation email
- ✓ oral confirmation

# Legitimate Purpose Consent



- **Opt-in**
- Silence, pre-ticked boxes or inactivity does not constitute consent.

## Freely given, specific, and informed

- Consent means giving data subjects **genuine choice and control** over how a PIC uses their data.
- Consent should be **unbundled from other terms and conditions** (including giving granular consent options for different types of processing) wherever possible.
- Clear affirmative action means someone must take deliberate action to opt in.

# Is consent always needed?

- No. Consent is just one criterion for lawful processing of both personal and sensitive personal information.
- Consent will not always be the most appropriate basis for processing personal data.
- PICs should choose the lawful basis that most closely reflects the true nature of the relationship with the individual and the purpose of the processing.

# Processing which may not need consent:



**Securities and  
Exchange  
Commission**  
PHILIPPINES



# What are the alternatives to consent?

## For processing of personal information:

- **Contract:** to supply goods or services they have requested, or to fulfil your obligations under an employment contract. This also includes steps taken at their request before entering into a contract.
- **Compliance with a legal obligation:** if you are required by law to process the data.
- **Vital interests:** you can process personal information if it is necessary to protect the data subject's life and health.
- **national emergency or to comply with the requirements of public order and safety.**
- **Public task:** if you need to process personal information to carry out public function or service and you have a legal basis for the processing.
- **Legitimate interests:** for the private sector, you can process personal data without consent if you have a genuine and legitimate reason, unless this is overridden by fundamental rights and freedoms of the data subject.

# What are the alternatives to consent?

## For processing of sensitive personal information:

- **Existing law and regulation:** you can process sensitive personal information (SPI) when there is a regulatory enactment which requires the processing
- **Medical treatment:** when processing is carried out by a by a medical practitioner or a medical treatment institution, and there is adequate level of protection
- **Protection of life and health:** to protect someone's life – the data subject or another person, and the data subject is not legally/physically able to express his consent
- **Lawful rights and interests:** when processing is necessary to protect lawful rights and interests of in court proceedings, in the establishment/ exercise/defense of legal claims, or when provided to government or public authority.
- **Public organizations:** refers to processing done by non-stock, non-profit organizations, cooperatives, and the like, where processing is only confined and related to the bona fide members



# Special Cases

The DPA shall not apply to **specified information** but only to the minimum extent of collection, access, use, disclosure or other processing necessary to the purpose, function, or activity concerned:

1. Information of public concern
2. Personal information for journalistic, artistic or literary purpose
3. Personal information for research purpose

# Special Cases

4. Information necessary in order to carry out the functions of public authority
5. Information necessary for banks, other financial institutions, to the extent necessary to comply with applicable laws
6. Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, which is being processed in the Philippines.

**General  
Data Privacy  
Principle**

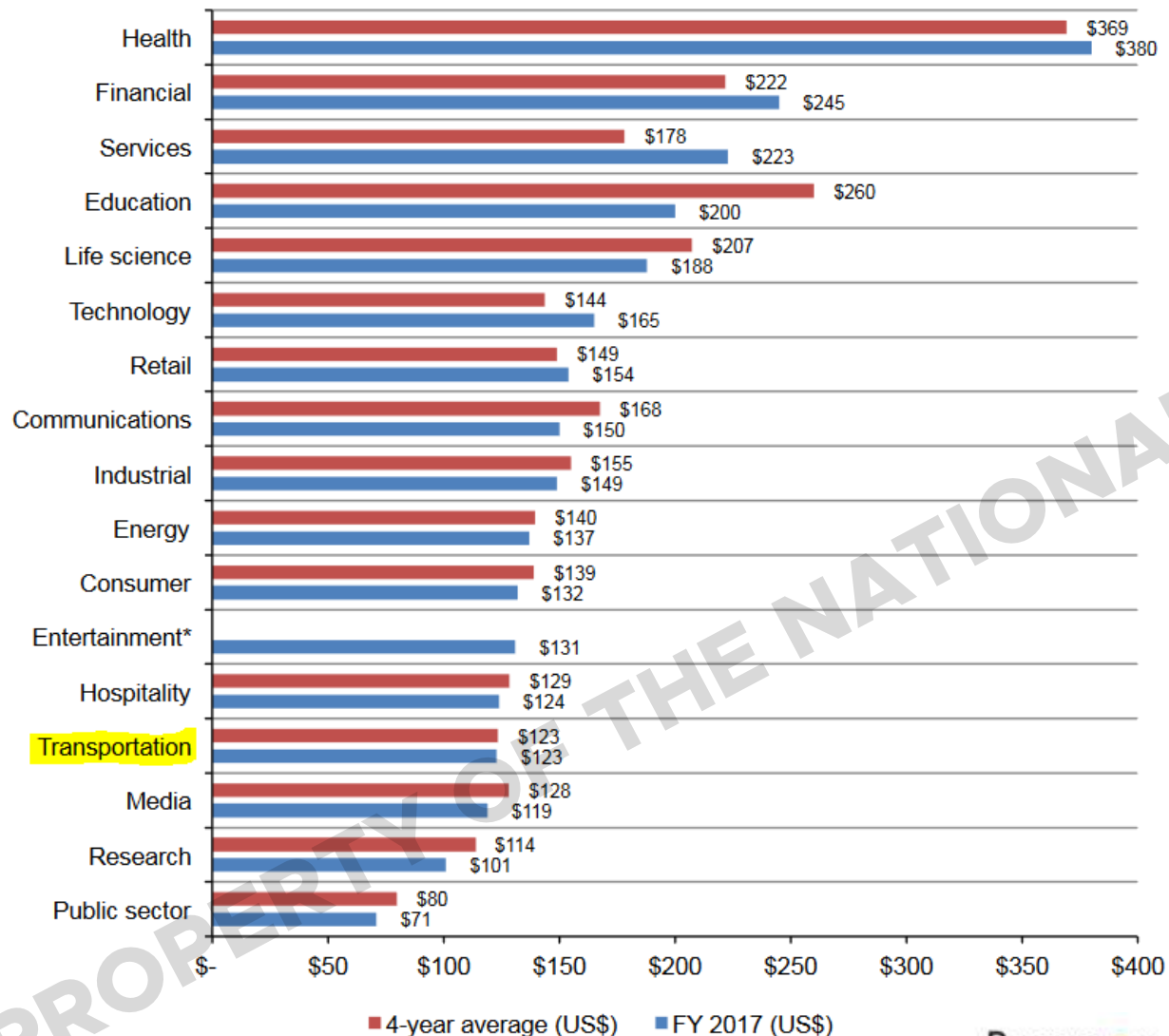
reciprocal  
equitable  
commensurate  
even  
proportionality  
comparative  
rational  
correlative  
corresponding  
equal  
just  
comparable



EDPS

**Figure 5. Per capita cost by industry classification**

\*Historical data are not available for all years  
Measured in US\$



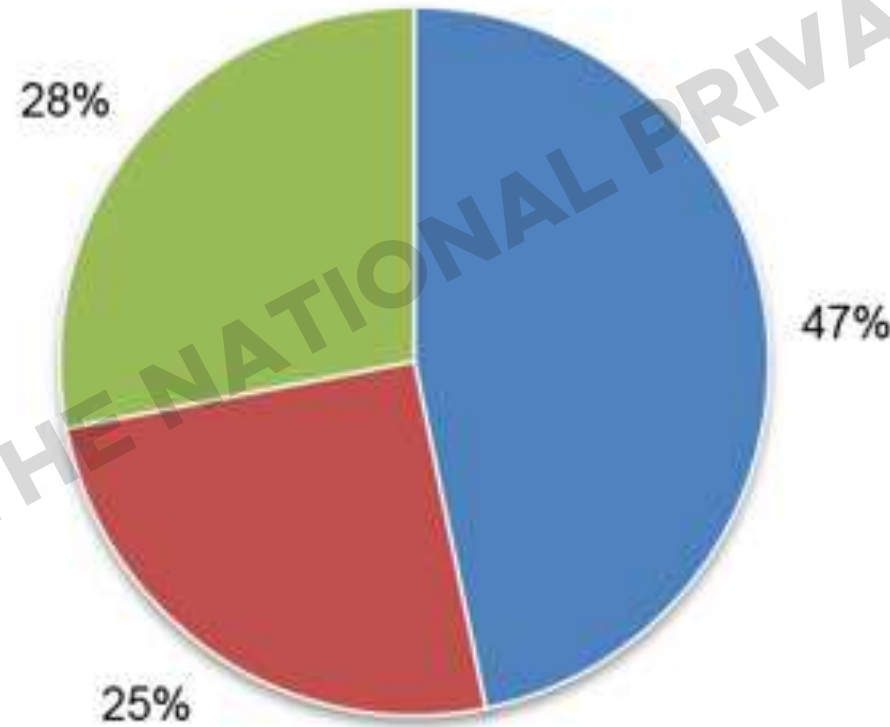
# The Bigger role of Data Privacy in the Transportation industry

...privacy reaches far beyond simple confidentiality – which is crucial in the transportation sector as the data collected may often lead to actual or perceived privacy violations.

## Root cause of Data Breach

**Malicious or criminal attacks cause the most data breaches.**<sup>7</sup> Pie Chart 2 provides a summary of the main root causes of data breaches on a consolidated basis for organizations in all countries. Forty-seven percent of incidents involved a malicious or criminal attack, 25 percent were due to negligent employees or contractors (human factor) and 28 percent involved system glitches, including both IT and business process failures.<sup>8</sup>

**Pie Chart 2. Distribution of the benchmark sample by root cause of the data breach**



**Malicious Attack**

**System Glitch**

**Human Error**

**47 % External**

**53 % Internal**

# HOW DO PRIVACY BREACHES OCCUR?

- **lost or stolen laptops**, removable storage devices, or paper records containing personal information
- **hard disk drives and other digital storage** media (integrated in other devices, for example, multifunction printers, or otherwise) being disposed of or returned to equipment lessors without the contents first being erased
- **databases containing personal information** being ‘hacked’ into or otherwise illegally accessed by individuals outside of the agency or organization

# HOW DO PRIVACY BREACHES OCCUR?

- **employees accessing** or disclosing personal information outside the requirements or authorization of their employment
- **paper records stolen** from insecure recycling or garbage bins
- an agency or organization **mistakenly providing personal information** to the wrong person, for example by sending details out to the wrong address, and
- an **individual deceiving an agency** or organization into improperly releasing the personal information of another person.



# Offenses and Penalties

| Punishable Act   | Imprisonment |       | Fine      |         |
|--|--------------|-------|-----------|---------|
|  | PI           | SPI   | PI        | SPI     |
| Unauthorized processing (without consent of the data subject or without being authorized by law)   | 1y-3y        | 3y-6y | 500k-2m   | 500k-4m |
| Access due to negligence (provided access to without being authorized by law)  | 1y-3y        | 3y-6y | 500k-2m   | 500k-4m |
| Improper disposal (knowingly or negligently dispose, discard, or abandon the personal information in an area accessible to the public or otherwise placed the personal information for trash collection) | 6m-2y        | 3y-6y | 100k-500k | 100k-1m |
| Unauthorized purposes  | 18m-5y       | 2y-7y | 500k-1m   | 500k-2m |

# Offenses and Penalties

| Punishable Act   | Imprisonment |       | Fine    |         |
|--|--------------|-------|---------|---------|
|  | PI           | SPI   | PI      | SPI     |
| Intentional breach (knowingly and unlawfully, or violating data confidentiality and security data systems, breaks in any way into any system where personal and sensitive personal information are stored) | 1y-3y        |       | 500k-2m |         |
| Concealing breach (intentionally or by omission conceals the fact of breach)   | 18m-5y       |       | 500k-1m |         |
| Malicious disclosure (with malice/in bad faith, discloses unwarranted or false information)  | 18m-5y       |       | 500k-1m |         |
| Unauthorized disclosure (discloses to a third party personal information not covered by the immediately preceding section without consent)   | 1y-3y        | 3y-5y | 500k-1m | 500k-2m |
| Combination of acts  | 3y-6y        |       | 1m-5m   |         |

# Extent of Liability

- If the offender is a juridical person, the penalty shall be imposed upon the **responsible officers** who:
  - ✓ participated in; or
  - ✓ allowed the commission of the crime by their gross negligence.
- Maximum penalty shall be imposed when the personal information of at least 100 persons is harmed, affected or involved as the result of the abovementioned actions.
- When the offender is a public officer in the exercise of his or her duties, an accessory penalty consisting in the disqualification to occupy public office for a term double the term of criminal penalty imposed shall be applied.



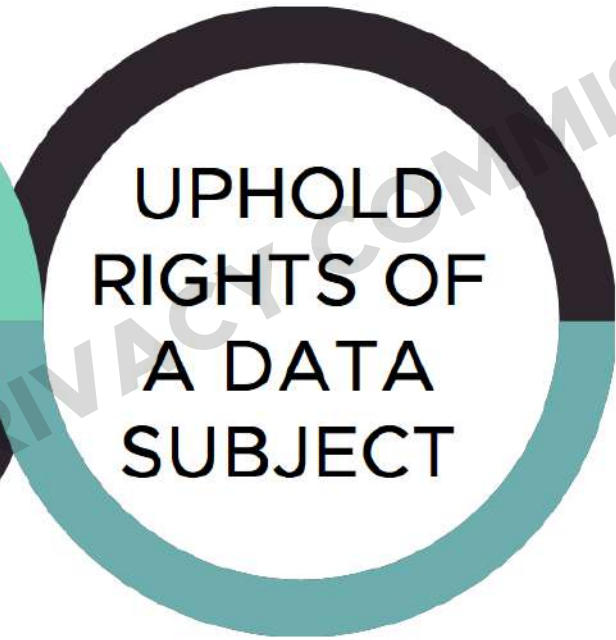
DATA  
PRIVACY  
PRINCIPLES

- TRANSPARENCY
- LEGITIMATE PURPOSE
- PROPORTIONALITY



SECURITY  
MEASURES

- SECURITY
- ACCOUNTABILITY



UPHOLD  
RIGHTS OF  
A DATA  
SUBJECT

- CHOICE
- NOTICE
- ACCESS
- REMEDY

# Transparency, Legitimate Purpose and Proportionality



- TRANSPARENCY
- LEGITIMATE PURPOSE
- PROPORTIONALITY

a. **Transparency** – The 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 data subjects, 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.

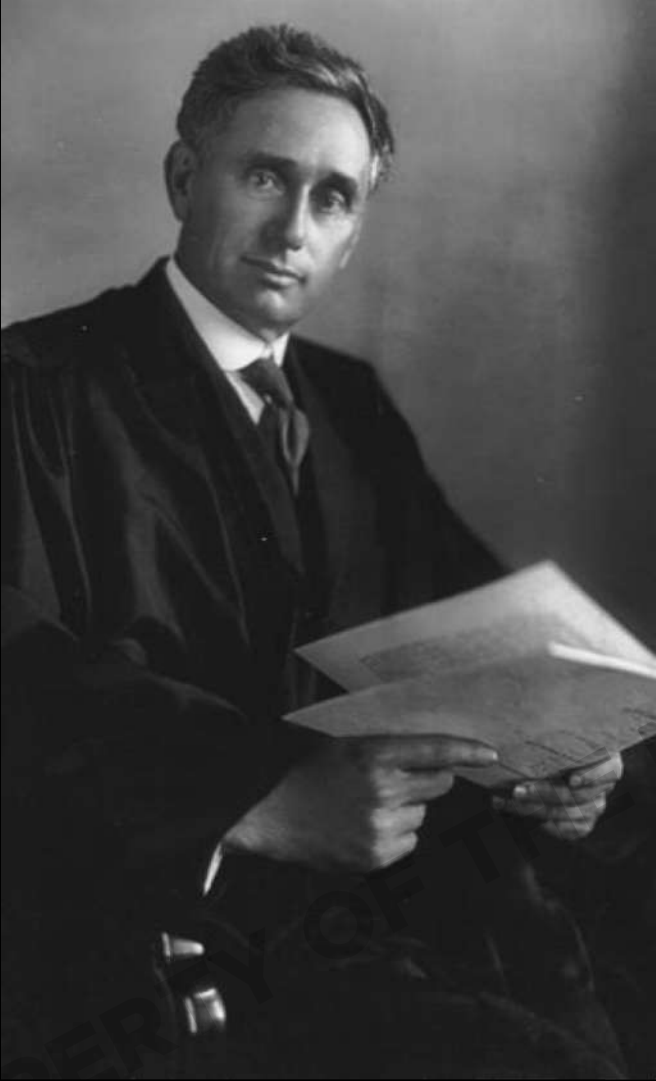
a. **Legitimate Purpose** – The processing of information shall be compatible with a declared and specific purpose which must not be contrary to law, morals, or public policy.

b. **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.

## PARA MAKAUTANG..

(PLEASE BRING THIS REQUIREMENTS)

- 6pcs 2x2 PICTURE
- 4pcs 1x1 PICTURE (WHOLE BODY)
- 3 VALID ID'S
- BRGY. CLEARANCE
- NBI CLEARANCE
- MAYORS PERMIT
- MEDICAL
- CEDULA
- BIRTH CERTIFICATE (NSO)
- SSS/TIN
- CO-MAKER
- X-RAY (WHOLE BODY)
- POLICE CLEARANCE
- PROOF OF BILLING
- FORM 137







CREATE AND COLLECT



STORE AND TRANSMIT

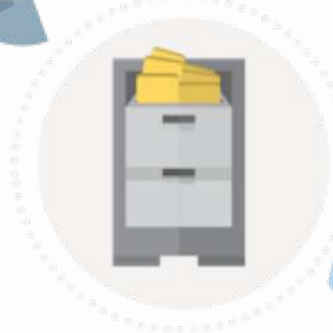


# THE DATA LIFE CYCLE

DISPOSE AND DESTROY



RETAIN



USE AND DISTRIBUTE



# I. CREATE AND COLLECT



| <b>Punishable Act</b>                                   | <b>Imprisonment</b>                          | <b>Fine (PHP)</b>         |
|---|--|---------------------------|
| Unauthorized Purposes                                   | 18 months to 5 years –<br>2 years to 7 years | 500 thousand to 2 million |
| Unauthorized Processing of Personal Information/Records | 1 year to 3 years – 3 years to 6 years       | 500 thousand to 4 million |

## II. STORE AND TRANSMIT



| Punishable Act   | Imprisonment                           | Fine (PHP)                |
|--|--|---------------------------|
| Accessing of Personal Information and Sensitive Personal Information due to Negligence | 1 year to 3 years – 3 years to 6 years | 500 thousand to 4 million |
| Intentional Breach   | 1 year to 3 years                      | 500 thousand to 2 million |
| Malicious Disclosure   | 18 months to 5 years                   | 500 thousand to 1 million |
| Unauthorized Disclosure  | 1 year to 3 years – 3 years to 5 years | 500 thousand to 2 million |

### III. USE AND DISTRIBUTE



| Punishable Act   | Imprisonment                              | Fine (PHP)                |
|--|---|---------------------------|
| Unauthorized Processing of Personal Information and Sensitive Personal Information | 1 year to 3 years — 3 years to 6 years    | 500 thousand to 4 million |
| Unauthorized Purposes  | 18 months to 5 years — 2 years to 7 years | 500 thousand to 2 million |
| Intentional Breach   | 1 year to 3 years                         | 500 thousand to 2 million |
| Concealing Breach  | 18 months to 5 years                      | 500 thousand to 1 million |
| Malicious Disclosure   | 18 months to 5 years                      | 500 thousand to 1 million |
| Unauthorized Disclosure  | 1 year to 3 years — 3 years to 5 years    | 500 thousand to 2 million |

## IV. RETAIN







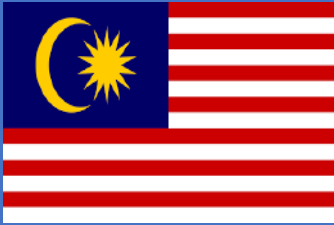





| <b>Punishable Act</b>               | <b>Imprisonment</b>                    | <b>Fine (PHP)</b>         |
|-------------------------------------|--|---------------------------|
| Access due to Negligence of Records | 1 year to 3 years — 3 years to 6 years | 500 thousand to 4 million |
| Malicious Disclosure                | 18 months to 5 years                   | 500 thousand to 1 million |
| Unauthorized Disclosure             | 1 year to 3 years — 3 years to 5 years | 500 thousand to 1 million |

## V. DISPOSE AND DESTROY



| <b>Punishable Act</b>        | <b>Imprisonment</b>                    | <b>Fine (PHP)</b>         |
|------------------------------|--|---------------------------|
| Improper Disposal of Records | 6 months 2 years — 1 year to 3 years   | 100 thousand to 1 million |
| Access due to Negligence     | 1 year to 3 years — 3 years to 6 years | 500 thousand to 4 million |
| Concealing Breach            | 18 months to 5 years                   | 500 thousand to 1 million |

# Data Privacy – Support for Multi-jurisdictions

|  |  |   |  |  |
|--|--|---|--|--|
|    | <b>Singapore</b><br>Up to S\$1 million.<br>\$10k per DNC breach<br>Legal Proceedings                         |    | <b>Australia</b><br>Up to A\$1.7 million for each breach   | <b>New Laws</b><br><br><b>Indonesia</b><br><br><br><b>Thailand</b><br> |
|    | <b>Malaysia</b><br>RM 500,000<br>Up to 3 years jail  |    | <b>Hong Kong</b><br>Fines – HK\$500k-1m<br>And 3 to 5 years jail   |  |
|   | <b>European Union</b><br>Up to 4% of global annual turnover for companies<br>Euro 10m-20m                    |   | <b>Philippines</b><br>1-3 years jail – unauthorized disclosure (up to Php 1m fine)<br>3-6 years jail – sensitive data breach (up to Php 4m fine) |  |
|  | <b>Taiwan</b><br>Up to 5 years jail in addition to or instead of fines of up to NT\$500k-1m (sensitive data) |  | <b>India</b><br>Fine up to INR 500,000 or up to 3 years jail or both   |  |

# THE FIVE PILLARS OF COMPLIANCE



Commit to Comply:  
Appoint a **Data Protection Officer (DPO)**



Know Your Risk:  
Conduct a **Privacy Impact Assessment (PIA)**



Be Accountable:  
Create your **Privacy Management Program and Privacy Manual**



Demonstrate Your Compliance: Implement your **privacy and data protection (PDP)** measures.



Be Prepared for Breach: Regularly exercise your **Breach Reporting Procedures (BRP)**.



# NPC ISSUANCES

# CIRCULARS

NPC Circular 16-01 – Security of Personal Data in Government Agencies

NPC Circular 16-02 – Data Sharing Agreements Involving Government Agencies


NPC Circular 16-03 – Personal Data Breach Management

NPC Circular 16-04 – Rules of Procedure


NPC Circular 17-01 – Registration of Data Processing Systems

NPC Circular 17-01 Appendix 1 – Registration of Data Processing Systems Appendix 1

# ADVISORIES

 NPC Advisory No. 2017-01 – Designation of Data Protection Officers

 NPC Advisory No. 2017-02 – Access to Personal Data Sheets of Government Personnel

 NPC Advisory No. 2017-03 – Guidelines on Privacy Impact Assessments

# DATA PRIVACY ACCOUNTABILITY AND COMPLIANCE FRAMEWORK



A. Choose a DPO



B. Register  
C. Records of processing activities  
D. Conduct PIA



E. Privacy Management Program  
F. Privacy Manual



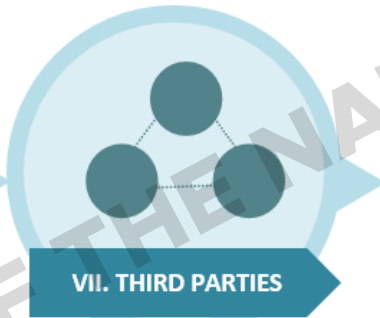
G. Privacy Notice  
H-O. Data Subject Rights  
P. Data Life Cycle



Q. Organizational  
R. Physical  
S. Technical  
▶ Data Center  
▶ Encryption  
▶ Access Control Policy



T. Data Breach Management;  
▶ Security Policy  
▶ Data Breach Response Team  
▶ Incident Response Procedure  
▶ Document  
▶ Breach Notification



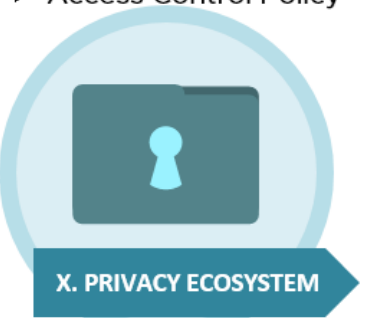
U. Third Parties;  
▶ Legal Basis for Disclosure  
▶ Data Sharing Agreements  
▶ Cross Border Transfer Agreement



V. Trainings and Certifications  
W. Security Clearance



X. Continuing Assessment and Development  
▶ Regular PIA  
▶ Review Contracts  
▶ Internal Assessments  
▶ Review PMP  
▶ Accreditations



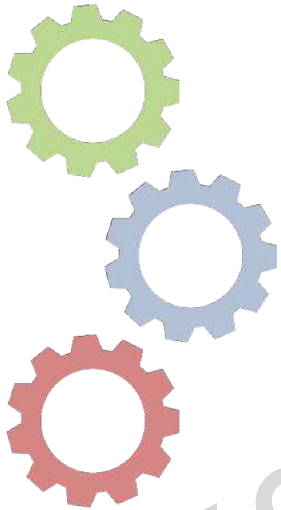
Y. New technologies and standards  
Z. New legal requirements



# ***Building a Culture of Privacy***

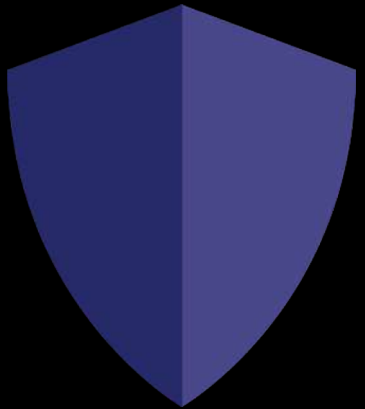
---

- 1. Privacy management is a top to bottom approach;**
- 2. You should appoint a data protection officer and be sure to listen to them;**
- 3. Conduct a privacy impact assessment on your organization;**
- 4. Develop privacy policies within your organization and Construct your privacy management program to guide your organization**
- 5. Start building a culture of privacy within your organizations by implementing organizational, Technical and physical measures to protect personal data;**
- 6. Build capacity among your staff.**
- 7. Be prepared for breach.**



# The Data Privacy Golden Rule

---



**If you Can't Protect It...**

**DONT Collect It.**





# Thank you for listening!

[facebook.com/privacy.gov.ph](https://facebook.com/privacy.gov.ph)  
[twitter.com/privacyPH](https://twitter.com/privacyPH)  
[info@privacy.gov.ph](mailto:info@privacy.gov.ph)