The Data Privacy Act of 2012 for the Real Estate Sector

Raymund Enriquez Liboro
Privacy Commissioner
National Privacy Commission
September 27, 2018
What the law is all about

How it will affect you
How the first mass-market camera led to the right to privacy and Roe v. Wade
“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)].
210 terabytes per second in 2017
1.6 Billion Selfies a Minute
From 2005 to 2015, cross-border data flow grew 45 times.
Forbes Most Valuable Brands

2007

- Exxon Mobil
- Petrochina
- General Electric
- China Mobile
- ICBC
- Microsoft
- Royal Dutch
- GazProm
- AT&T

2017

- Apple
- Google
- Microsoft
- Facebook
- Coca Cola
- Amazon
- Disney
- Toyota
- McDonalds
- Samsung
AGGREGATION OF 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
AGGREGATION OF PERSONAL DATA

- age
- marital status
- car owner
- downloads
- purchases
- net worth
- email
- voting habits
- clicks
- average spending
- internet searches
- astrological sign
- political party
- clicks
- political party
- criminal record
- users
- homeowner
- voting habits
- kids in house
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
Access to personal information such as name, date of birth, address, or email address can result to fraudsters victimizing individuals.
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 Lontoh 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, Lontoh remembered posting a photo of his Professional Regulation Commission (PRC) ID online.

“Kaya naman ako (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, Chio Ong () - September 6, 2008 - 12:00am

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

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.
21st Century Hazards and Risks

Norse – Superior Attack Intelligence

Norse monitors the world’s largest dedicated cyber and digital networks. With over eight billion assets that resides over 15,000 networks appliances – from Apple laptops to ATM machines, to critical infrastructure systems, to traditional sensor TV cameras – the Norse Intelligence network platform data on who the attackers are and what they’re after. Norse delivers the facts through the Norse Applications, which proactively tracks attacks and improves your overall security, SOX, and the Norse Intelligence Service, which provides professional continuous asset monitoring for your network.
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

Passed in the Senate and House of Representatives of the Philippines in Congress assembled, 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:

CHAPTER I
GENERAL PROVISIONS
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
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
Transparency, Legitimate Purpose and 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.

b. **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.

c. **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
ROOT CAUSES OF BREACH

- Malicious or criminal attack: 47%
- System Glitch: 24%
- Human Error: 29%

• **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.
<table>
<thead>
<tr>
<th>The Rights of the Data Subject</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Right to be informed</strong></td>
</tr>
<tr>
<td><strong>Right to object</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Right to access</strong></td>
</tr>
<tr>
<td><strong>Right to correct/rectify</strong></td>
</tr>
<tr>
<td><strong>Right to block/remove</strong></td>
</tr>
<tr>
<td><strong>Right to data portability</strong></td>
</tr>
<tr>
<td><strong>Right to file a complaint</strong></td>
</tr>
<tr>
<td><strong>Right to be indemnified</strong></td>
</tr>
</tbody>
</table>
THE FIVE PILLARS OF ACCOUNTABILITY AND COMPLIANCE

1. Commit to Comply: Appoint a Data Protection Officer (DPO)
2. Know Your Risk: Conduct a Privacy Impact Assessment (PIA)
4. Demonstrate Your Compliance: Implement your privacy and data protection (PDP) measures.

NATIONAL PRIVACY COMMISSION
2018
Road to Data Privacy Resilience

Five Pillars of Compliance & Accountability

- (1) Appoint a DPO
- (2) Know your Risks: Conduct a Privacy Impact Assessment
- (3) Create a Privacy Management Program and Privacy Manual
- (4) Demonstrate accountability and compliance through Privacy and Data Protection Measures
- (5) Breach Management

Certification And Seals

Domestic
- Philippine DPO Certification
- The 5 Star Accountability and Compliance (ACE) program

Global Certification
- CBPR: Cross-border Privacy regulations
- GDPR adequacy

Sectoral Code of Conduct

- Privacy code of conduct
Sectors

Non-Compliant Personal Information Controllers/Processor
- Willful Violators; Evading Compliance
- Ignorant Violators; Non-Compliant

Enforcement
- Awareness Campaigns; 30-60-90 day

Compliant Personal Information Controllers/Processor
- Paper Compliance; Non-Operational
- Operational Compliance Accountability and Assurance

Aim of the Commission
- Data Privacy Council building proper accountability and assurance

Property of the National Privacy Commission
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
twitter.com/privacyPH
info@privacy.gov.ph