Data Privacy Act: Compliance Framework

Ivy D. Patdu, MD JD

National Privacy Commission

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)].

DPO

NATIONAL PRIVACY COMMISSION

RIGHT TO INFORMATION PRIVACY

The individual's ability to control the flow of information concerning or describing him, which however must be overbalanced by legitimate public concerns. To deprive an individual of his power to control or determine whom to share information of his personal details would deny him of his right to his own personhood.

Dissenting Opinion of Justice Consuelo Ynares-Santiago in G.R No 167798 Kilusang Mayo Uno, et al., v. The Director General, National Economic Development Authority, et al., and G.R No. 167930 Bayan Muna Representatives Satur C. Ocampo, et al., v. Eduardo Ermita, et al. (19 April 2006)

DPO

NATIONAL PRIVACY COMMISSION

“In this digital era, information is the currency of power – valuable, coveted, but at a very high risk.”

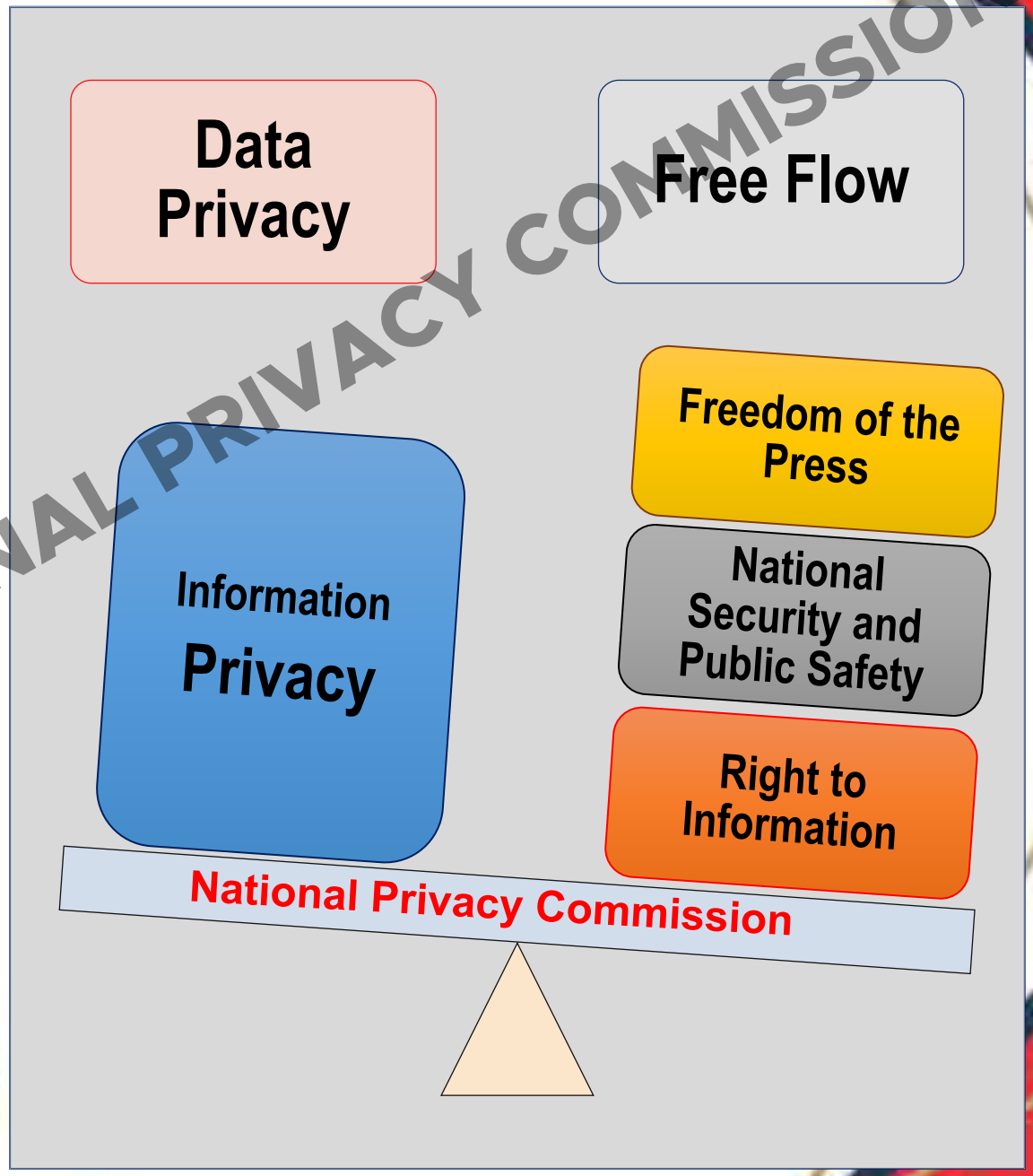
-Senator Edgardo Angara, sponsorship speech for the Data Privacy Act

DPO

NATIONAL PRIVACY COMMISSION

Data Privacy Act

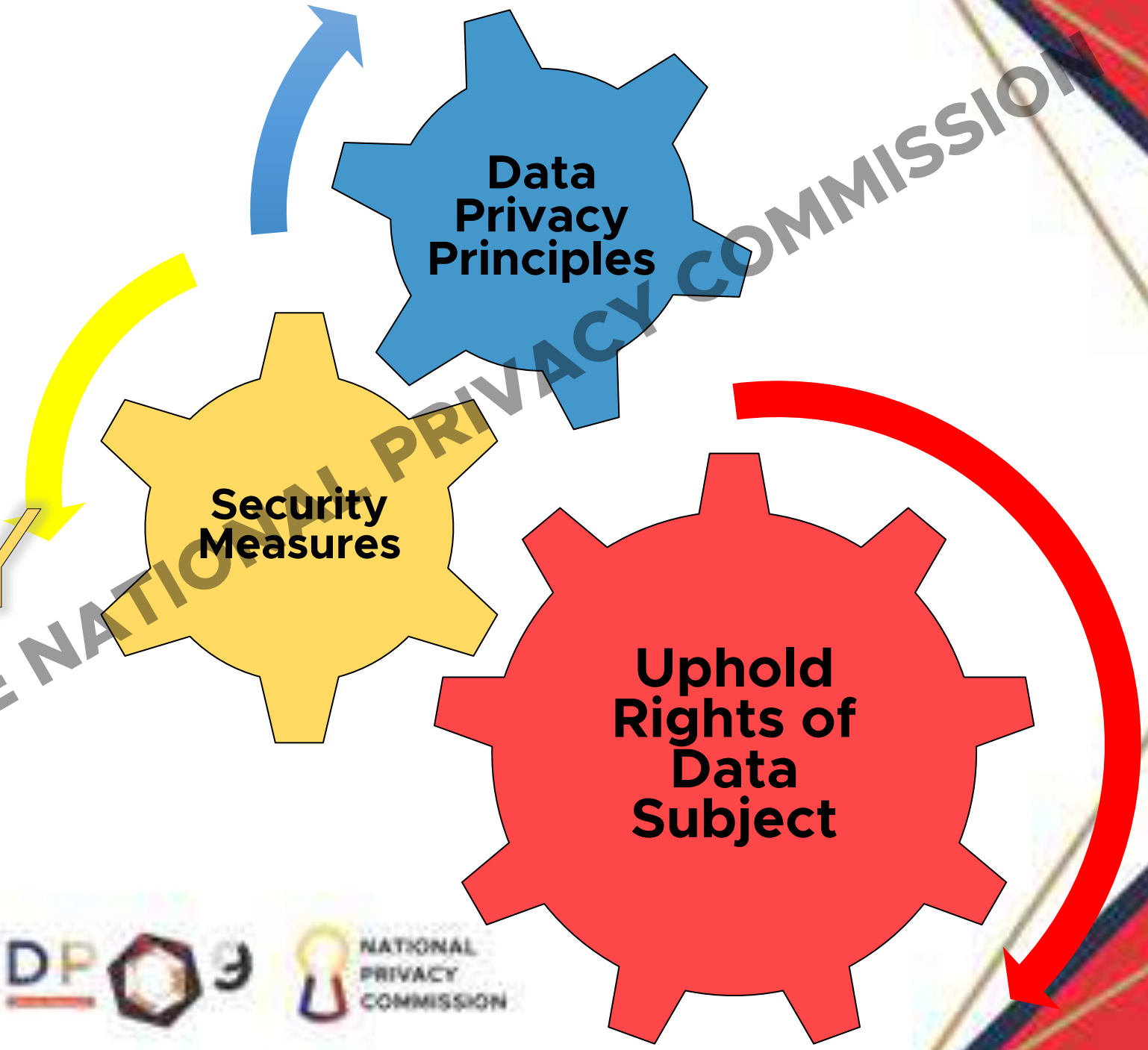
It is the policy of the State to protect the fundamental human right of privacy of communication while ensuring free flow of information to promote innovation and growth.



Personal Data

- Any information from which the identity of an individual is apparent
- Any information that can be put together with other information to reasonably and directly identify an individual
- Includes sensitive personal information such as your health, education, genetic or sexual life
- Includes information that is classified or privileged

DATA PRIVACY ACT



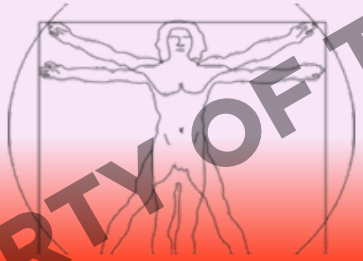
DPO

NATIONAL PRIVACY COMMISSION

DATA PRIVACY PRINCIPLES

TRANSPARENCY

LEGITIMATE PURPOSE



PROPORTIONALITY

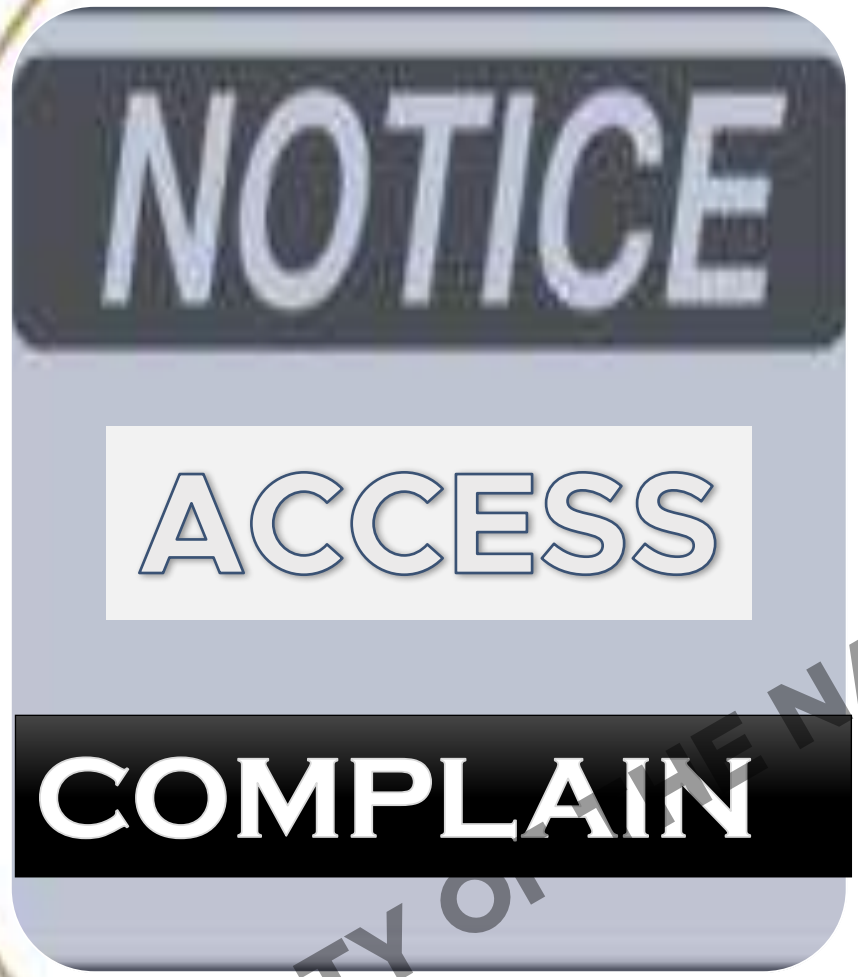
DPO

NATIONAL PRIVACY COMMISSION

SECURITY MEASURES

Organizational
Physical
Technical

Confidentiality
Integrity
Availability



Rights of Data Subjects

1. Right to Information
2. Right to Object
3. Right to Access
4. Right to Correct
5. Right to Erase
6. Right to Damages
7. Right to Data Portability
8. Right to File a Complaint

DPO

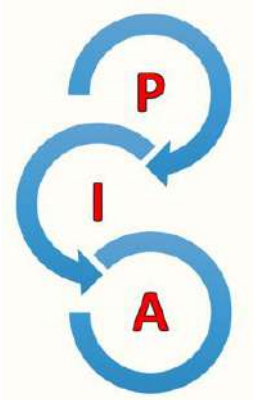
NATIONAL PRIVACY COMMISSION

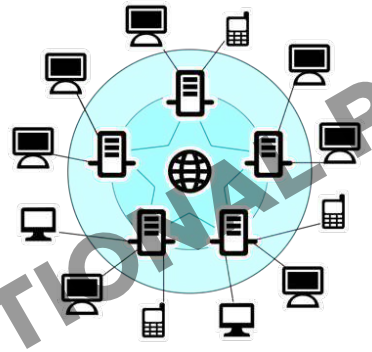
Compliance Framework

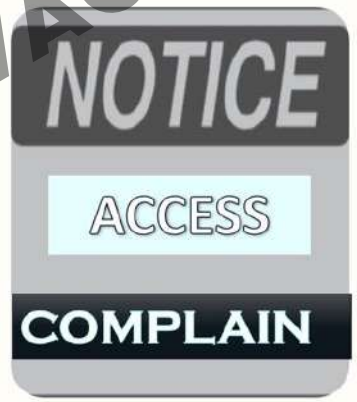
DPO

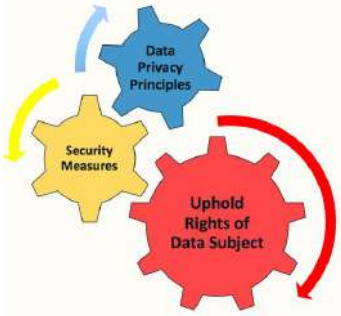
NATIONAL PRIVACY COMMISSION

1. Governance → 2. Risk Assessment → 3. Organization → 4. Day to Day → 5. Data Security









6. Breaches → 7. Third Parties → 8. Manage HR → 9. Continuity → 10. Privacy Ecosystem

DPO

NATIONAL PRIVACY COMMISSION

1. Governance

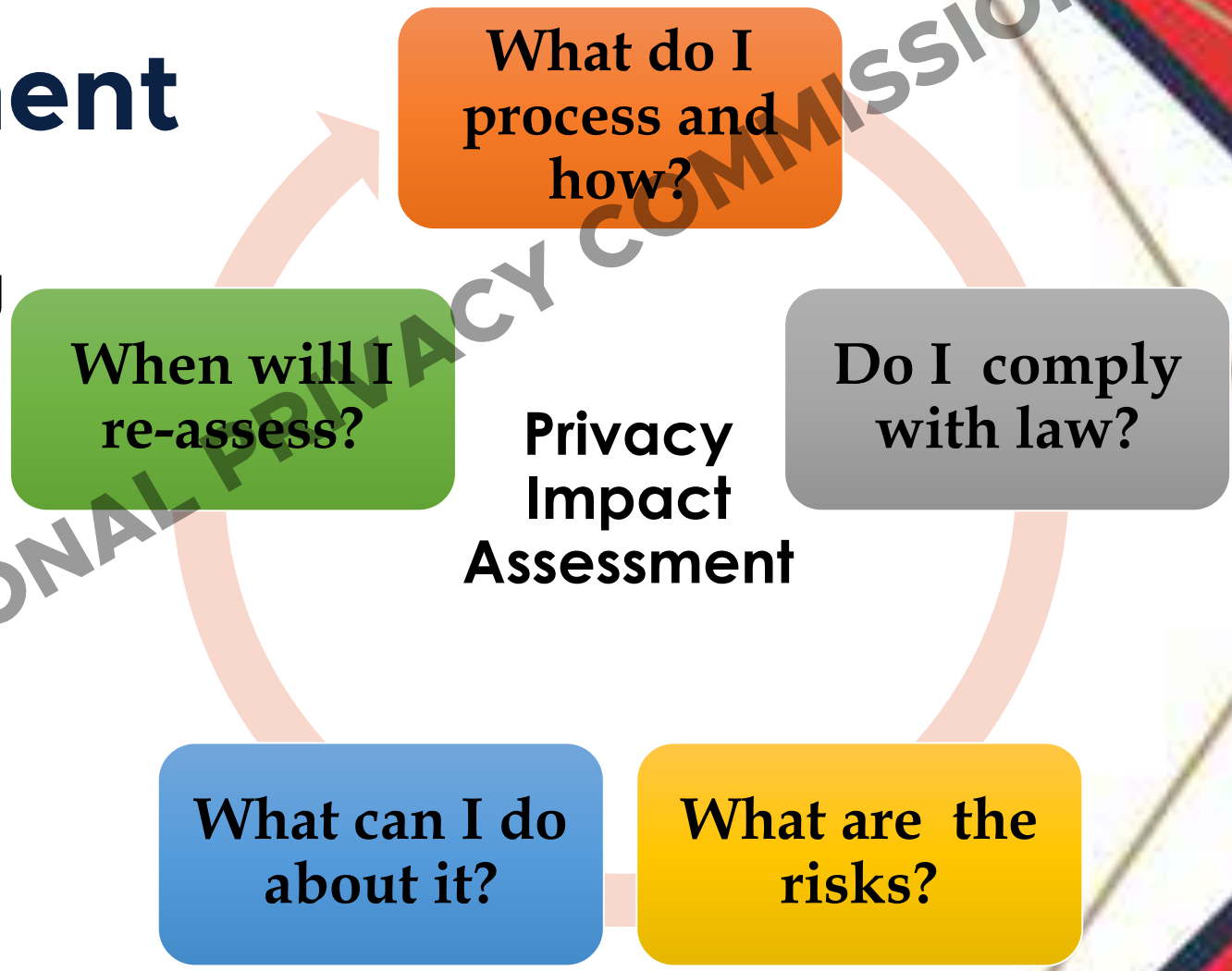
- Designate a DPO

THE DPO SHOULD POSSESS SPECIALIZED KNOWLEDGE AND DEMONSTRATE RELIABILITY NECESSARY FOR THE PERFORMANCE OF HIS OR HER DUTIES AND RESPONSIBILITIES.

Picture from http://www.computerweekly.com/news/450402719/GDPR-will-require-75000-DPOs-worldwide-study-shows

2. Risk Assessment

- ❑ Register Data Processing System
- ❑ Have Records of Processing Activities
- ❑ Conduct Privacy Impact Assessment



3. Organization

- ❑ Implement Privacy Management Program
- ❑ Develop Privacy Manual

DPO

NATIONAL PRIVACY COMMISSION

4. Day to Day

- ❑ Have Privacy Notices
- ❑ Mechanism for exercise of Data Subject Rights
- ❑ Policies for every stage of Data Life Cycle

Innovative Electronic Medical Record System Expands in Malawi (2014) available at http://www.cdc.gov/globalaids/success-stories/innovativemalawi.html (last accessed June 20, 2016).

DPO

NATIONAL PRIVACY COMMISSION

5. Data Security

- Implement Organizational, Physical and Technical Security Measures

6. Breaches

- Have in place Data Breach Management Program

Tyler Durden, "*Worst-Ever Recorded" Ransomware Attack Strikes Over 57,000 Users Worldwide, Using NSA-Leaked Tools*, ZeroHedge, 12 May 2017, available at http://www.zerohedge.com/news/2017-05-12/massive-ransomware-attack-goes-global-huge (last accessed May 14, 2017).

Security Policy → **Breach Response Team** → **Incident Response Procedure** → **Document** → **Notification and Reporting**

DPO

NATIONAL PRIVACY COMMISSION

7. Third Parties

- Manage Third Party Risks

Picture from Surabhi Agarwal, **BPOs edge towards high-end work in changing market, Live Mint Sep.6, 2012, available at** http://www.livemint.com/Industry/hdDwofLyBZc0XQl0bb70hO/BPOs-edge-towards-highend-work-in-changing-market.html (last accesed May 15, 2017)

DPO

NATIONAL PRIVACY COMMISSION

8. Manage HR

- ❑ Undergo Trainings and Get Certifications
- ❑ Give Security Clearance

Villupuram nurses jump on to technological bandwagon at http://www.thehindu.com/news/national/tamil-nadu/villupuram-nurses-jump-on-to-technological-bandwagon/article5699852.ece

DPO

NATIONAL PRIVACY COMMISSION

9. Continuity

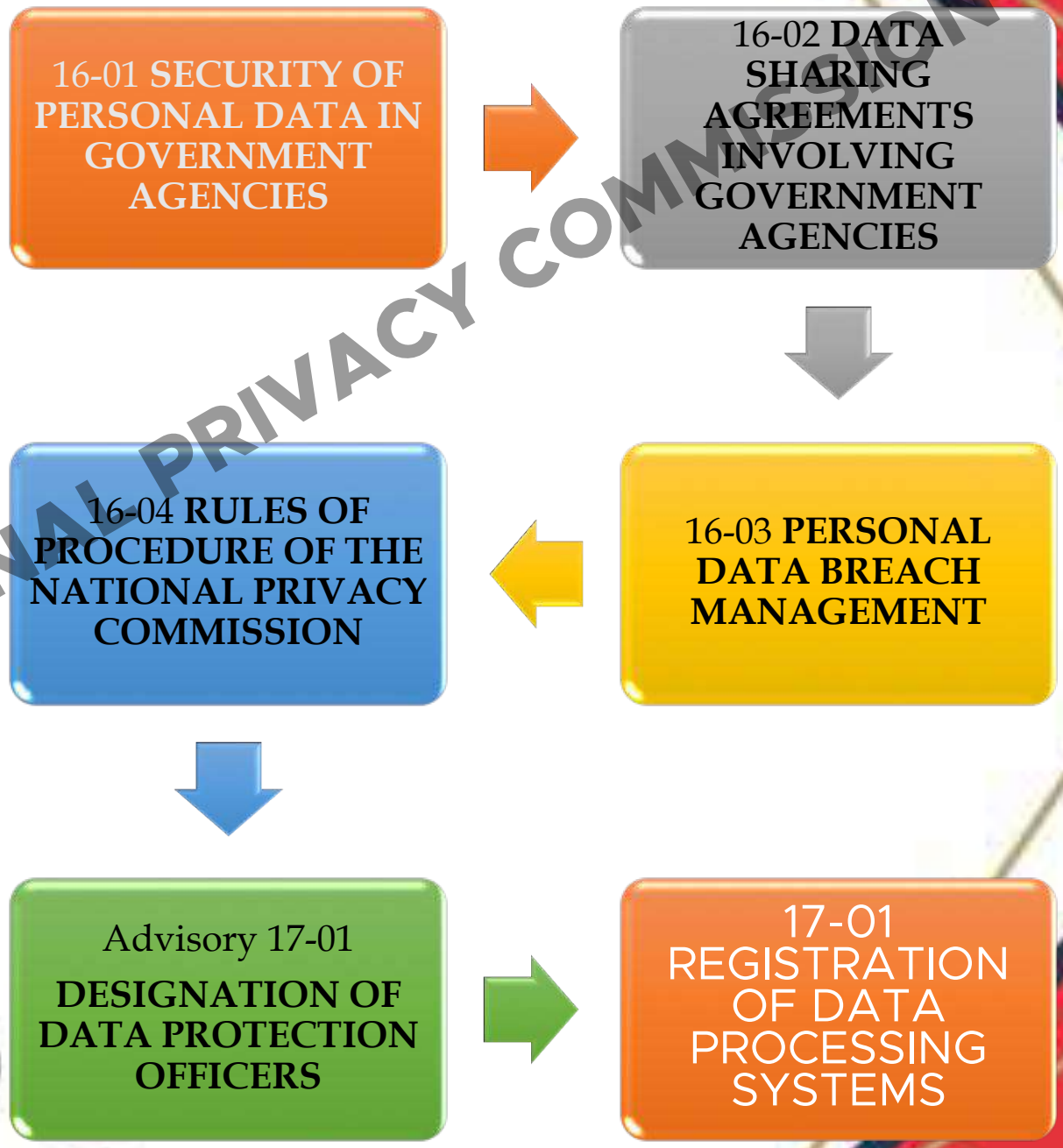
- Regular Assessment and Review, Get Accreditations

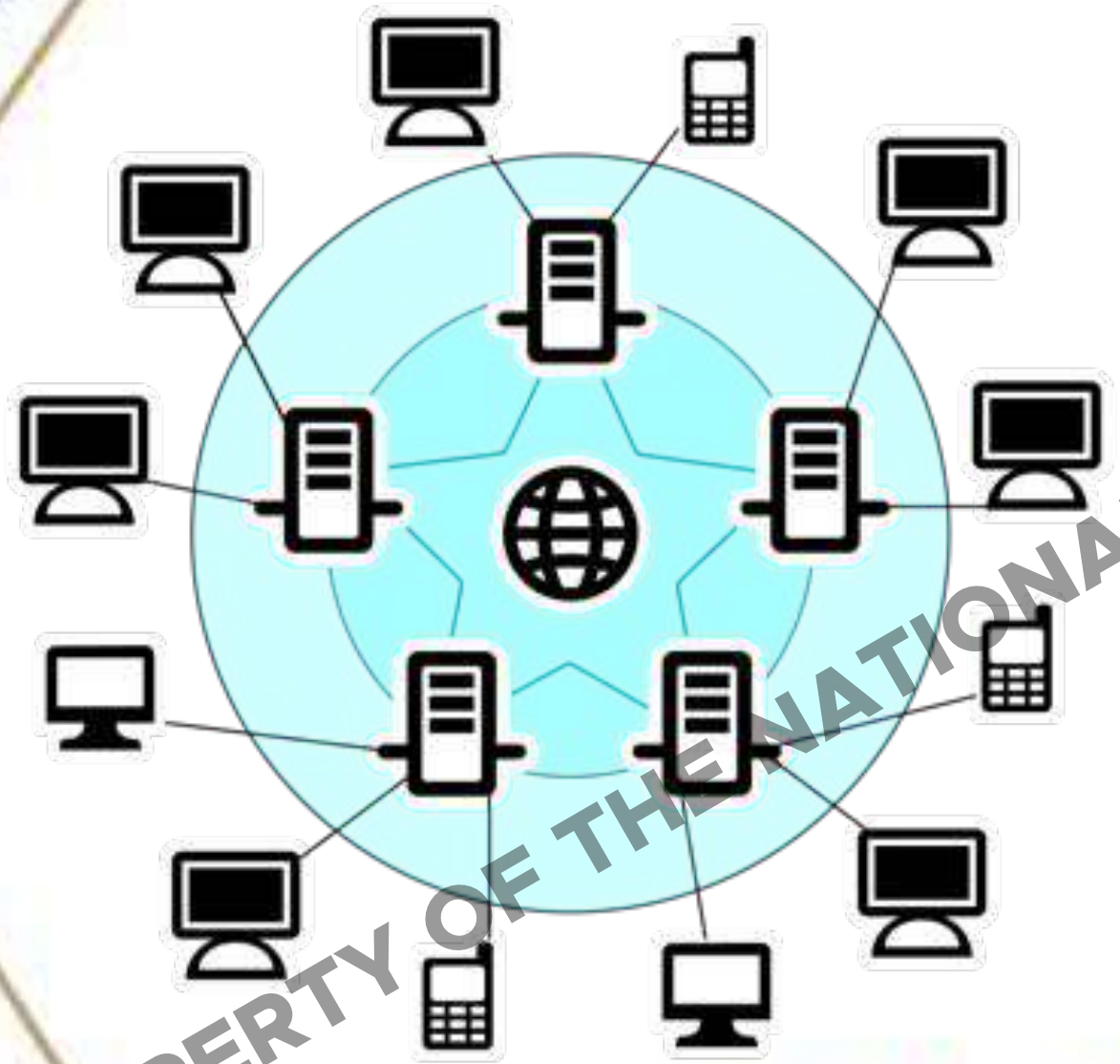
DPO

NATIONAL PRIVACY COMMISSION

10. Privacy Ecosystem

- Be updated on New technologies and standard, New legal requirements





WHY SHOULD PERSONAL DATA BE PROTECTED?

DPO

NATIONAL PRIVACY COMMISSION

CRIME		IMPRISONMENT	FINE
Processing of Personal/Sensitive Information for Unauthorized Purpose	Processing information for other purposes which are no longer authorized by law or consent	1yr 6mos – 7 years	Php500,000 to Php2,000,000
Access to Personal/Sensitive Information due to Negligence	Persons who provide access due to negligence shall be liable	1-6 years	Php500,000 to Php4,000,000
Concealment of Security Breach	Duty to notify Privacy Commission in case of breach (within 72 hours)	1yr 6mos – 5 years	Php500,000 to Php1,000,000
Improper Disposal	Negligently dispose, discard or abandon personal data of an in an area accessible to the public or placed in its container for trash collection.	6 months – 3 years	Php 100,000 to Php 1,000,000

Selling Personal Information without consent

- An example of very common privacy violation by Bank of America was reported by the Utility Consumers' Action Network. In the case Bank of America was charged for **selling the personal information** (social security numbers, bank account numbers etc) of **35 million customers** to **marketers and third parties without informing individuals**. Bank of America is now settling for $14 million, and agreeing to change its privacy polices, its Web site, and its privacy procedures.

Source: http://cis-india.org/internet-governance/blog/privacy/privacy-banking

Medical group fined $140K for tossing patients' health records into public dump

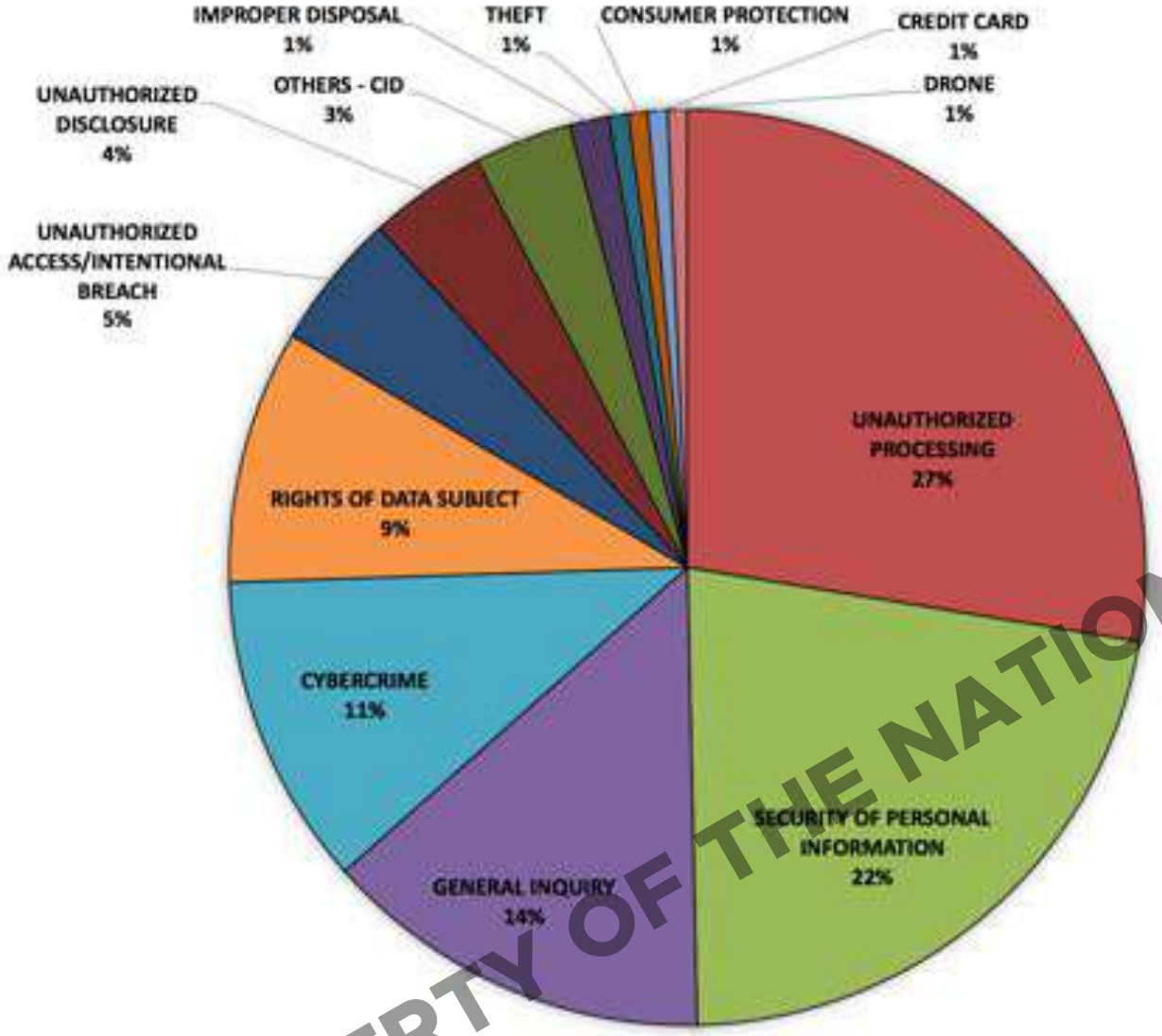
15 JAN 2013 5

Data loss, Law & order, Privacy

- Names, Social Security numbers, and medical diagnoses for more than 67,000 Massachusetts residents in the US were tossed into a public dump as is – no redacting, no shredding, no nothing
- Records in the pile included pathology reports for people tested for various kinds of cancer, along with other test results

Available at https://nakedsecurity.sophos.com/2013/01/15/medical-patients-health-records-dump/

COMPLAINTS (AS OF AUG. 31, 2017)



NATURE OF COMPLAINTS RECEIVED AS OF 31 AUGUST 2017

CLASSIFICATION	NO. OF COMPLAINTS	PERCENTAGE
UNAUTHORIZED PROCESSING	40	28%
SECURITY OF PERSONAL INFORMATION	32	22%
GENERAL INQUIRY	20	14%
CYBERCRIME	16	11%
RIGHTS OF DATA SUBJECT	13	9%
UNAUTHORIZED ACCESS/ INTENTIONAL BREACH	7	5%
UNAUTHORIZED DISCLOSURE	6	4%
OTHERS - CID	5	3%
IMPROPER DISPOSAL	2	1%
THEFT	1	1%
CONSUMER PROTECTION	1	1%
CREDIT CARD	1	1%
DRONE	1	1%
TOTAL	145	100%

DPO

NATIONAL PRIVACY COMMISSION

NHS sexual health clinic fined £180K for patients' HIV status leak

56 Dean Street, the London-based sexual health clinic CREDIT: GOOGLE

The recipients' email addresses, of which 730 contained people's full names, were entered into the "to" field instead of "bcc", which masks the email addresses of people receiving the message.

Cara McGoogan, NHS sexual health clinic fined £180K for patients' HIV status leak (May 9, 2016)
Available at www.telegraph.co.uk/technology/2016/05/09/nhs-sexual-health-clinic-fined-180k-for-patients-hiv-status-leak/ (last accessed Jan.11, 2017).

DPO

NATIONAL PRIVACY COMMISSION

Available at https://www.pbs.org/newshour/show/data-breach

UK hospitals hit with massive ransomware attack

Sixteen hospitals shut down as a result of the attack

by Russell Brandom | @russellbrandom | May 12, 2017, 11:36am EDT

SHARE TWEET LINKEDIN

Peter O'Connor / Flickr

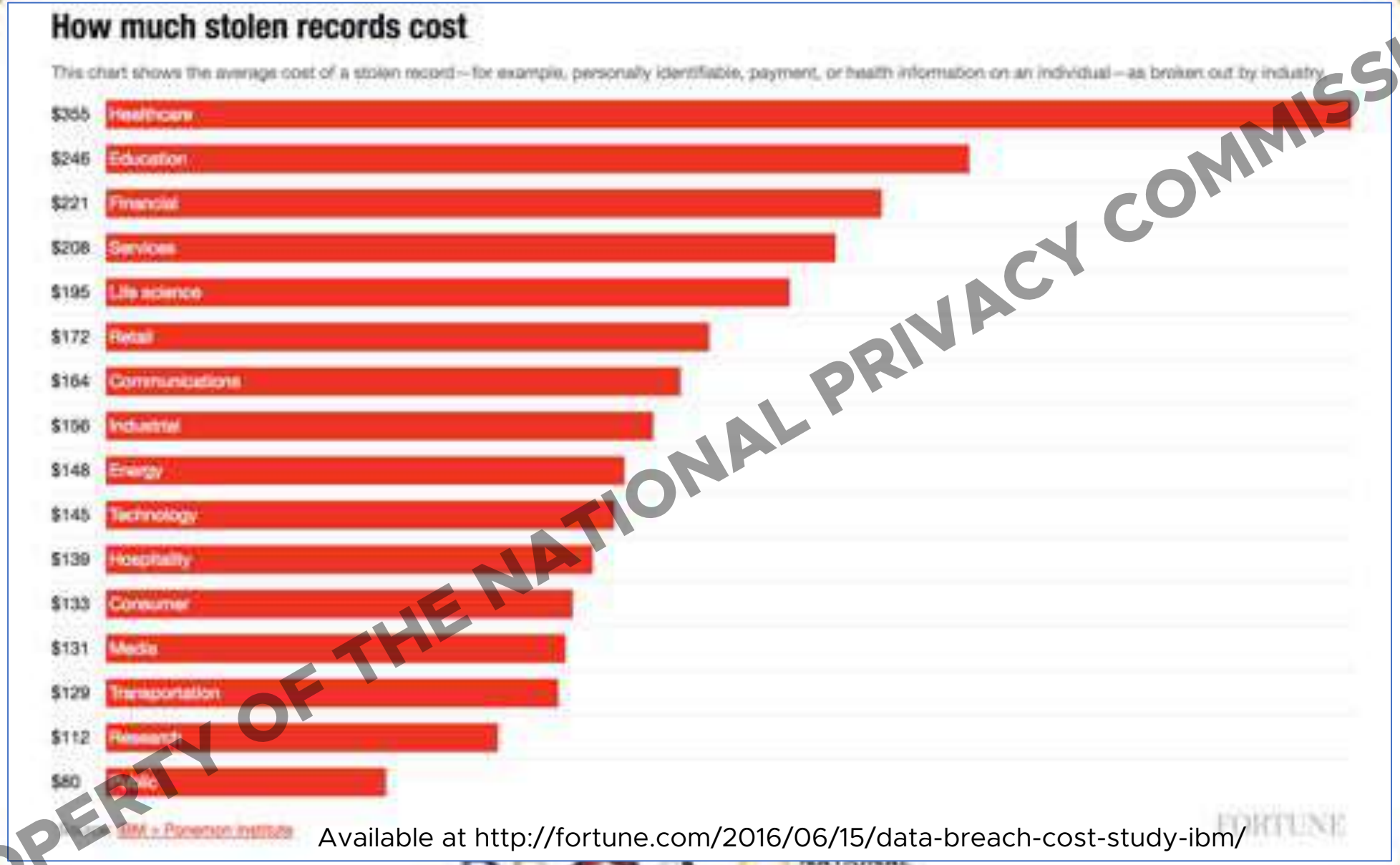
Sixteen hospitals shut down as a result of the attack

The result has been a wave of canceled appointments and general disarray, as many hospitals are left unable to access basic medical records. At least one hospital has canceled all non-urgent operations as a result.

Russell Brandom, UK hospitals hit with massive ransomware attack (May 12, 2017), available at https://www.theverge.com/2017/5/12/15630354/nhs-hospitals-ransomware-hack-wannacry-bitcoin (last accessed September 14, 2017).

DPO

NATIONAL PRIVACY COMMISSION



Available at http://fortune.com/2016/06/15/data-breach-cost-study-ibm/

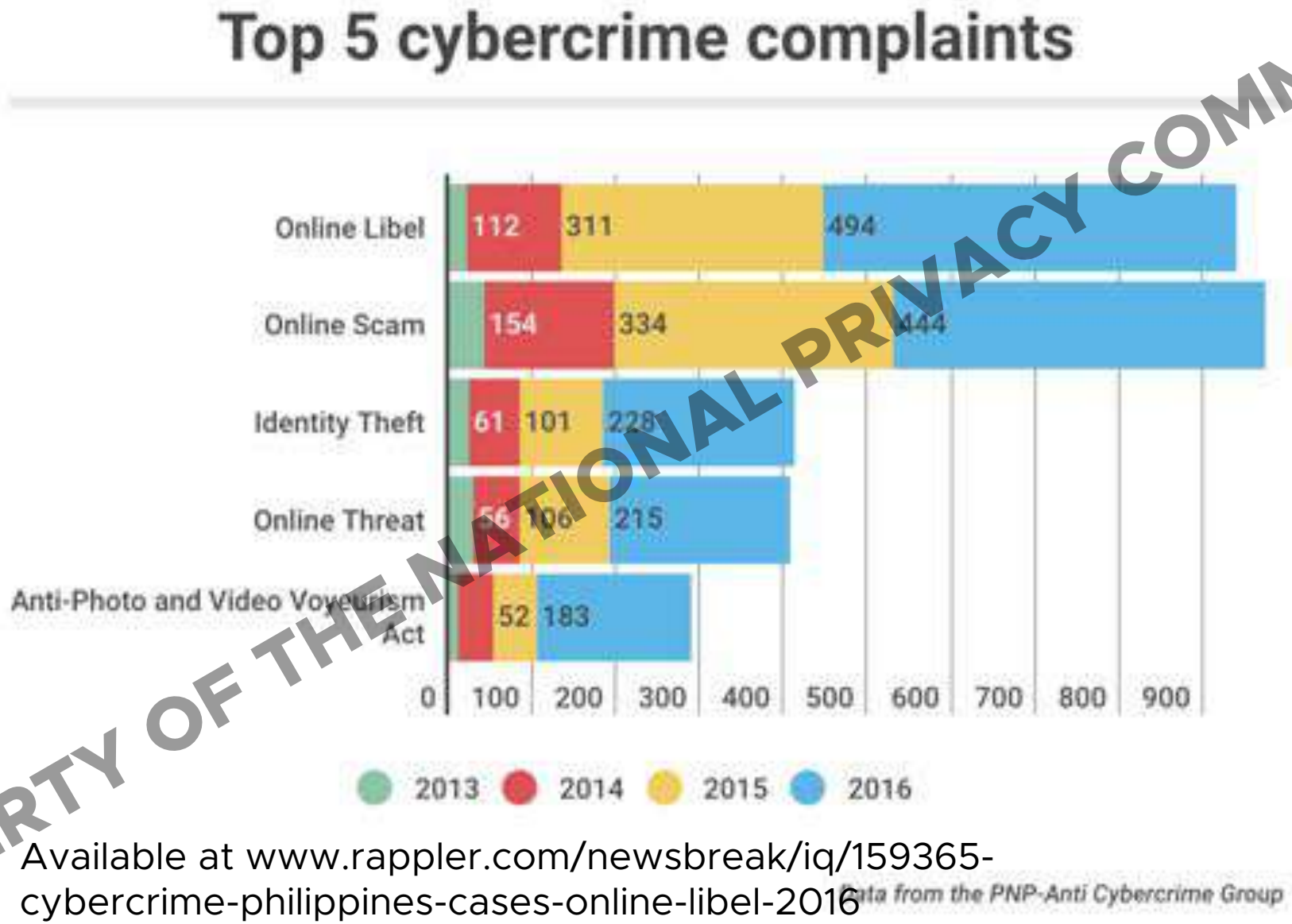
MAG-INGAT: Impormasyon ng netizen, ginamit sa panloloko, ABS CBN (May 3, 2017) available at http://news.abs-cbn.com/video/news/05/03/17/mag-ingat-impormasyon-ng-netizen-ginamit-sa-panloloko.

His modus operandi is to steal his victims' information and then contact call centers of certain banks to request for credit card replacement.

Identity theft suspect falls, available at http://www.philstar.com/metro/2017/04/07/1688420/identity-theft-suspect-falls

Identity theft suspect falls

(The Philippine Star) | Updated April 7, 2017 - 12:00am



Available at www.rappler.com/newsbreak/iq/159365-cybercrime-philippines-cases-online-libel-2016

Privacy and Personal Data Protection

Benefits

Harm

NATIONAL PRIVACY COMMISSION

privacy.gov.ph

Thank you!

ivypatdu@privacy.gov.ph

info@privacy.gov.ph

Ivy D. Patdu

National Privacy Commission