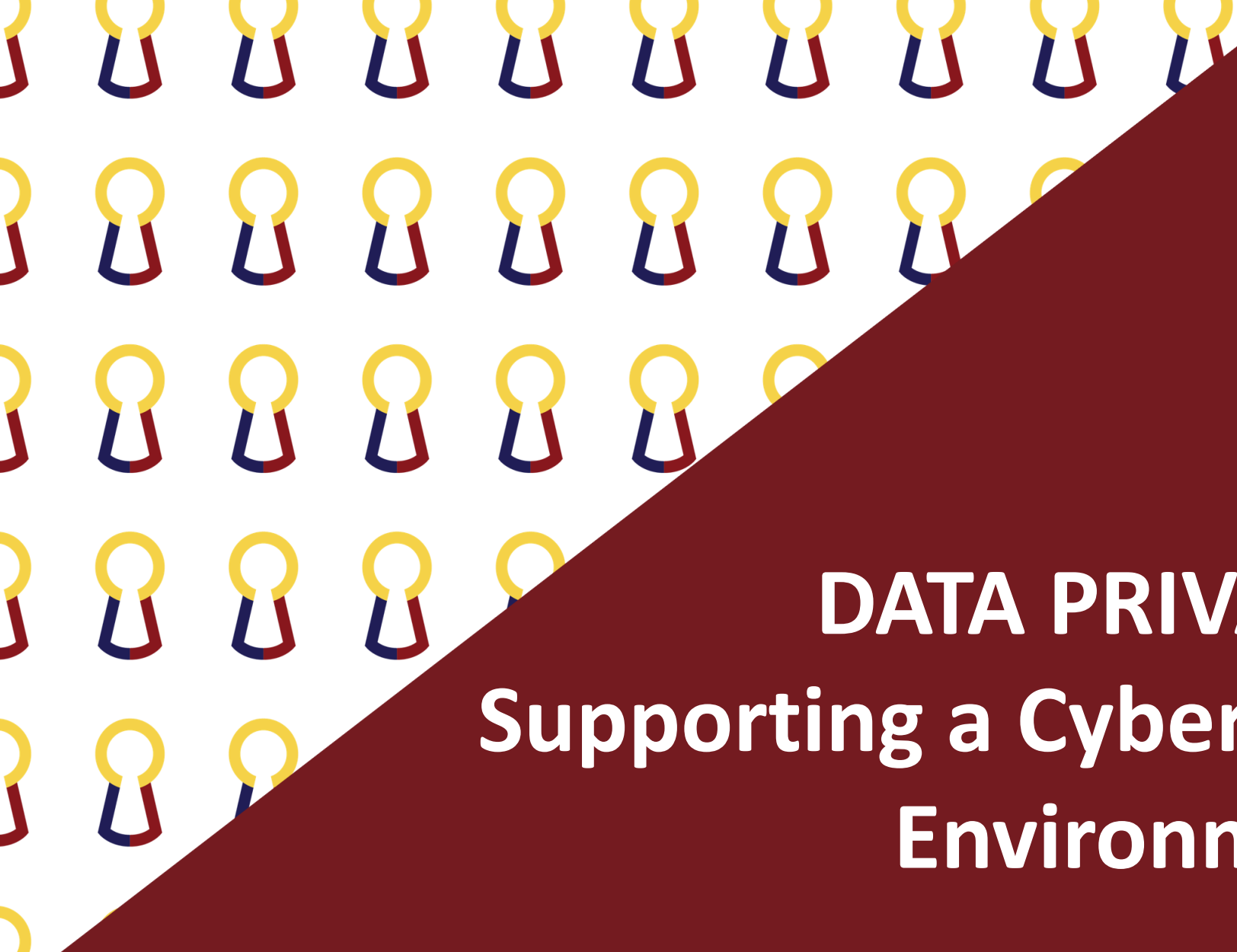


DATA PRIVACY: Supporting a Cybersafe Environment

Erlaine Vanessa D. Lumanog
Attorney IV, Policy Review Division
National Privacy Commission


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
Google
amazon
UBER
Microsoft
Google
TESLA
TESLA

Forbes Most Valuable Brands

2007	2017
Exxon Mobil	Apple
Petrochina	Google
General Electric	Microsoft
China Mobile	Facebook
ICBC	Coca Cola
Microsoft	Amazon
Royal Dutch	Disney
GazProm	Toyota
AT&T	McDonalds
	Samsung

Brand Value (in billions of $)

Industry

- Aerospace
- Alcohol
- Apparel
- Automotive
- Beverages
- Business Services
- Consumer Packaged Goods
- Diversified
- Financial Services
- Leisure
- Luxury
- Media
- Restaurants
- Retail
- Technology
- Telecom
- Tobacco
- Transportation

Article & Sources:
https://howmuch.net/articles/top-100-most-valuable-brands-2018
https://www.forbes.com/

howmuch.net

The world's largest taxi firm, Uber, owns no cars.

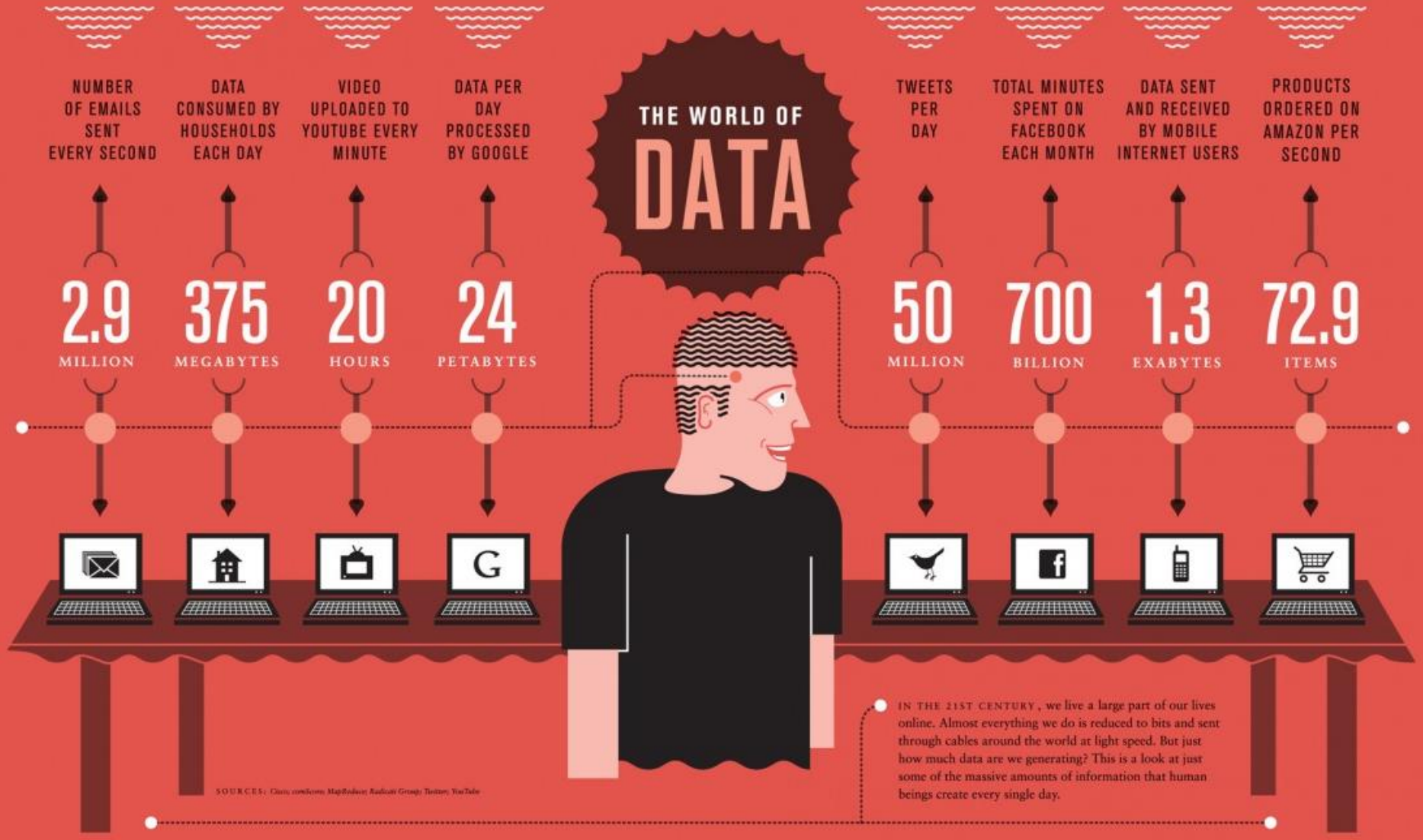
The world's most popular media company, Facebook, creates no content.

The world's most valuable retailer, Alibaba, carries no stock.

The world's largest accommodation provider, Airbnb, owns no property.

http://larsonjb.com/uploads/3/8/9/9/38990899/next_orig.jpg

THE WORLD OF DATA

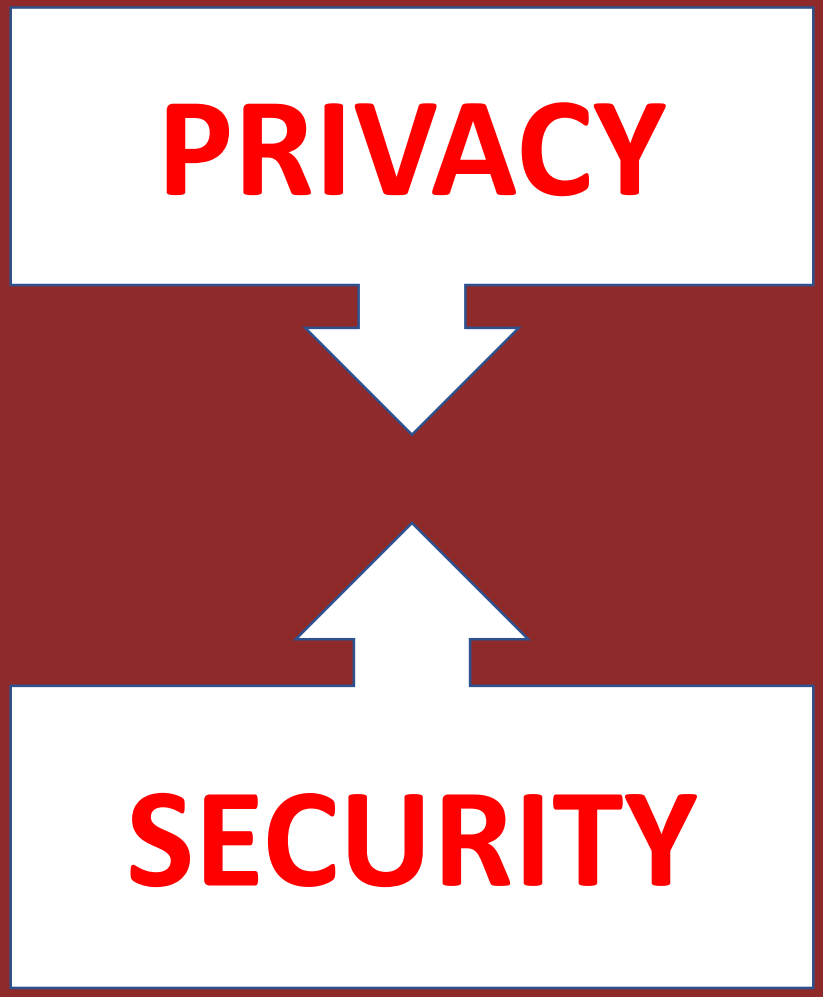


IN THE 21ST CENTURY, we live a large part of our lives online. Almost everything we do is reduced to bits and sent through cables around the world at light speed. But just how much data are we generating? This is a look at just some of the massive amounts of information that human beings create every single day.

SOURCES: *Cisco, comScore, MapReduce, Radicati Group, Twitter, YouTube*

A COLLABORATION BETWEEN GOOD AND OLIVER MUNDAY

IN PARTNERSHIP WITH IBM



NATIONAL
PRIVACY
COMMISSION

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

NATIONAL PRIVACY COMMISSION

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

Section 11, Article II of the 1987 Constitution

"The State values the dignity of every human person and guarantees full respect for human rights."

“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)]

NATIONAL PRIVACY COMMISSION

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.

Informational Privacy

The right to informational privacy is the **right of an individual to control** the collection of, access to, and use of personal information about him or her that are under the control or custody of the government and private sector.

It is essential to the protection of one's ability to develop ideas and personal relationships, and underpins human dignity and other values like freedom of association and freedom of speech.

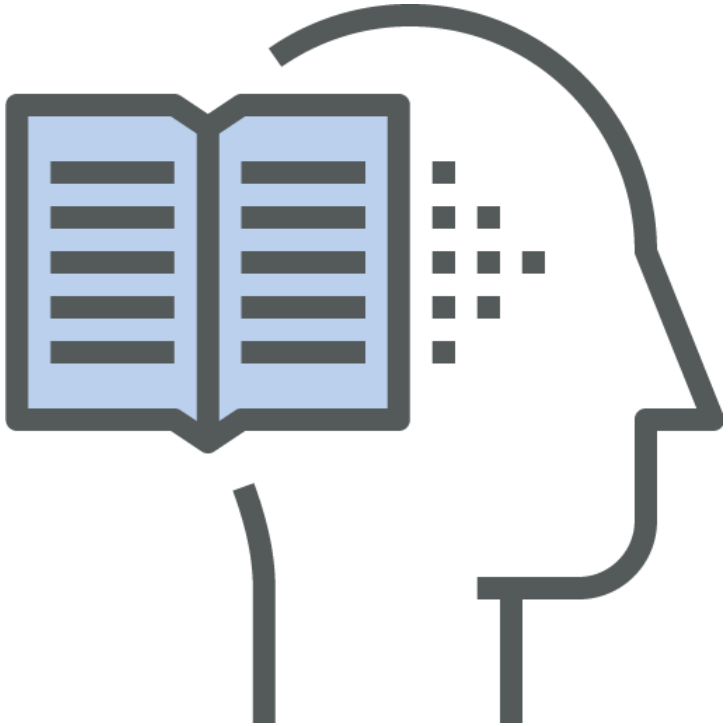
NATIONAL PRIVACY COMMISSION

SCOPE

Applies to the processing of all types of personal information and to any natural and juridical person involved in processing in the Philippines.

NATIONAL PRIVACY COMMISSION

PROCESSING



Refers to **any operation or any set of operations** performed upon personal information including, but not limited to the following:

- **Collection**
- **Recording**
- **Organization**
- **Storage**
- **Updating or modification**
- **Retrieval**
- **Consultation**
- **Use**
- **Consolidation**
- **Blocking**
- **Erasure**
- **Destruction**

NATIONAL PRIVACY COMMISSION

PERSONAL INFORMATION (PI)

- 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.

SENSITIVE PERSONAL INFORMATION (SPI)

- Race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- Health, education, genetic or sexual life of a person, or to any proceeding for any offense committed or alleged to have been committed by such person, the disposal of such proceedings, or the sentence of any court in such proceedings;
- Issued by government agencies peculiar to an individual (social security numbers, health records, licenses or its denials, suspension or revocation, and tax returns); and
- Specifically established by law to be kept classified.

NATIONAL PRIVACY COMMISSION

PRIVILEGED INFORMATION

- Husband-Wife
- Lawyer- Client
- Doctor-Patient
- Priest-Penitent
- any and all forms of data, which, under the Rules of Court and other pertinent laws constitute privileged communication

NATIONAL PRIVACY COMMISSION

Personal Information Controller (PIC)

controls the processing of personal data, or instructs another to process personal data on its behalf

Personal Information Processor (PIP)

any natural or juridical person to whom a PIC may outsource or instruct the processing of personal data

Data Subject

an individual whose personal, sensitive personal, or privileged information is processed

NATIONAL PRIVACY COMMISSION

Criteria for Lawful Processing of Personal Information

1. The data subject must have given **consent** prior to the collection, or as soon as practicable and reasonable;

2. Processing involves the personal information of a data subject who is a party to a **contractual agreement**, or in order to fulfill obligations under the contract or to take steps at the request of the data subject prior to entering the said agreement;

3. Processing necessary for **compliance with a legal obligation** to which the PIC is subject;

NATIONAL PRIVACY COMMISSION

4. Processing necessary to protect **vitally important interests of the data subject**, including his or her **life and health**;

5. Processing necessary to respond to **national emergency** or to comply with requirements of **public order and safety**, as prescribed by law.

6. Processing necessary for the **fulfillment of a constitutional or statutory mandate of a public authority**; or

7. Necessary to **pursue the legitimate interests** of the PIC, or by a third party or parties to whom data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject.

NATIONAL PRIVACY COMMISSION

Processing of Sensitive Personal and Privileged Information

1. **Consent** given by data subject, or by the parties to the exchange of privileged information, prior to the processing of such information;

2. Processing is provided for by **existing laws and regulations**: Provided, that the said laws and regulations do not require consent of the data subject for the processing, and guarantee the protection of personal data;

3. Processing necessary to **protect the life and health** of the data subject or another person, and the data subject is not legally or physically able to express his or her consent prior to the processing;

NATIONAL PRIVACY COMMISSION

4. Processing necessary to achieve the **lawful and noncommercial objectives of public organizations** and their associations provided that:

- Processing is confined and related to the bona fide members of these organizations or their associations;
- SPI are not transferred to third parties;
- Consent of data subject obtained prior to processing

5. Processing necessary **for medical treatment**: Provided, that it is carried out by a medical practitioner or medical treatment institution, and an adequate level of protection of personal data is ensured; or

6. Necessary for the **protection of lawful rights and interests** of natural or legal persons in court proceedings, or the establishment, exercise or defense of legal claims or when provided to government or public authority pursuant to a constitutional or statutory mandate.

NATIONAL PRIVACY COMMISSION

RIGHTS OF THE DATA SUBJECT

Right to Information

Right to Object

Right to Access

NATIONAL PRIVACY COMMISSION

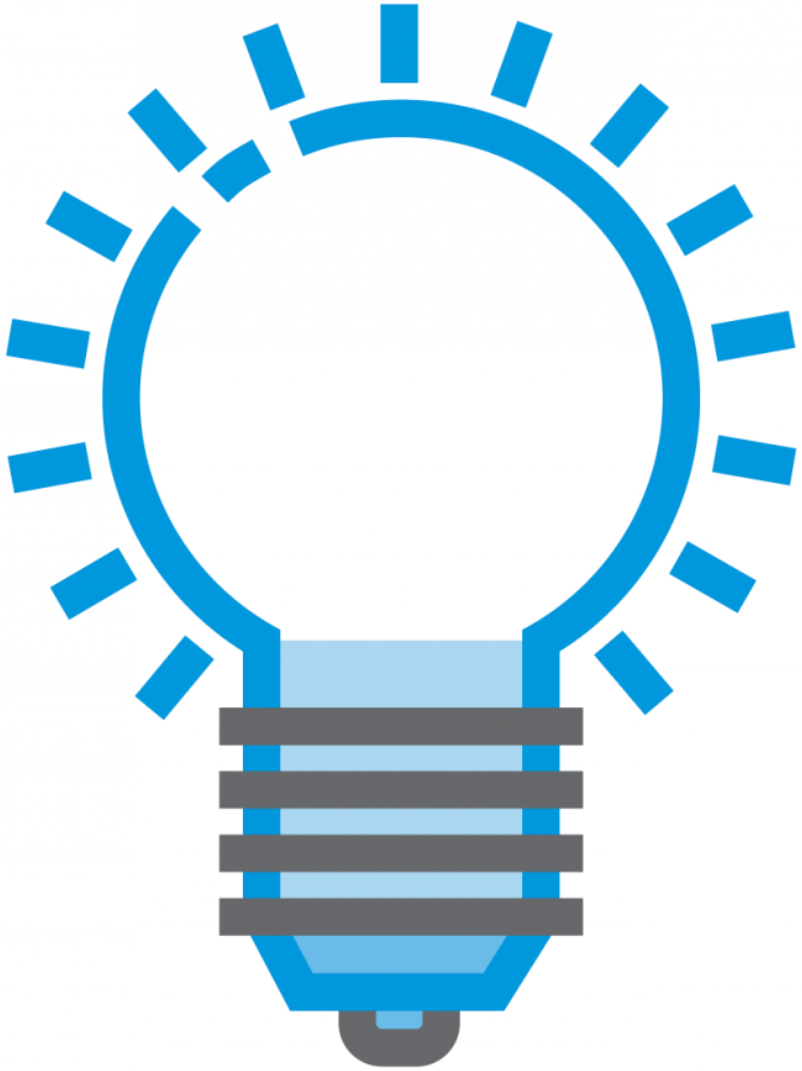
Right to Correct

Right to Erase

Right to Damages

Right to File a Complaint

NATIONAL PRIVACY COMMISSION



GENERAL DATA PRIVACY PRINCIPLES

Transparency

The data subject must be aware of the following:

- Purpose and extent of processing;
- Risks and safeguards;
- Identity of the PIC;
- Rights as data subject and how these can be exercised

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

Proportionality

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

Processing only if the purpose could not be reasonably fulfilled by other means.

NATIONAL PRIVACY COMMISSION


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

NATIONAL PRIVACY COMMISSION

Data Privacy Accountability and Compliance Framework

GOVERNANCE
A. Appoint your DPO

RISK ASSESSMENT
B. Register systems
C. Maintain records
D. Conduct a PIA

ORGANIZATION
E. Privacy Management Program
F. Privacy Manual

DAY-TO-DAY
G. Privacy Notice
H-O. Data Subjects' Rights
P. Data Life Cycle

DATA SECURITY
Q. Organizational Measures
R. Physical Measures
S. Technical Security Measures

BREACH
T. Data Breach Management
- Security Policy
- Data Breach Response Team
- Incident Response Procedure
- Documentation
- Breach Notification

THIRD PARTIES
U. Third Parties
- Legal Basis for Disclosure
- Data Sharing Agreements
- Cross Border Transfer Agreement

HUMAN RESOURCES
V. Training and Capacity Building
W. Security Clearances and NDA

PROGRAM REVIEW
X. Continuing Assessment and Development
- Regular PIA
- Review Contracts
- Internal Assessments
- Review PMP
- Accreditations

LEGAL AND ICT
Y. New technologies and standards
Z. New legal requirements

Obligations of a Personal Information Controller

The PIC should collect personal information only for specified and legitimate purposes

The PIC should process personal information fairly and lawfully.

The PIC should process accurate, relevant and up to date personal information.

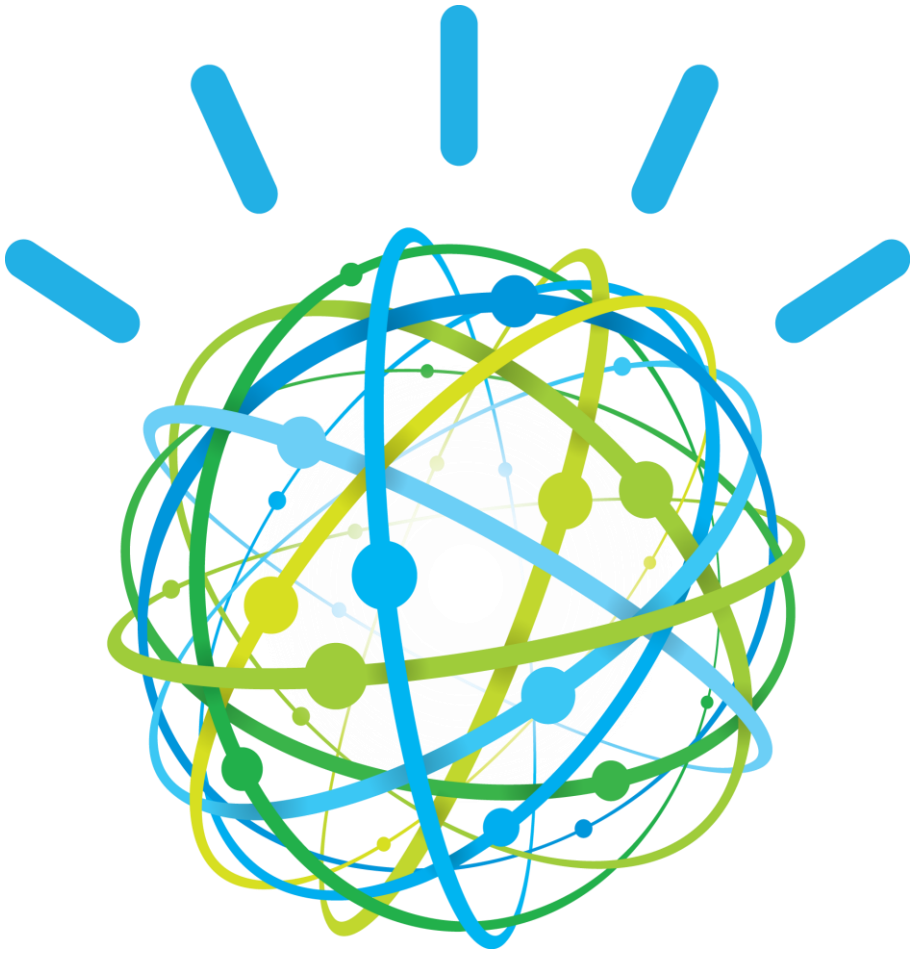
The PIC should collect and process personal information adequately and not excessively.

The PIC should retain personal information only for as long as necessary

The PIC must implement reasonable organizational, physical, technical security measures to protect personal data.

NATIONAL PRIVACY COMMISSION

SECURITY MEASURES FOR THE PROTECTION OF PERSONAL DATA



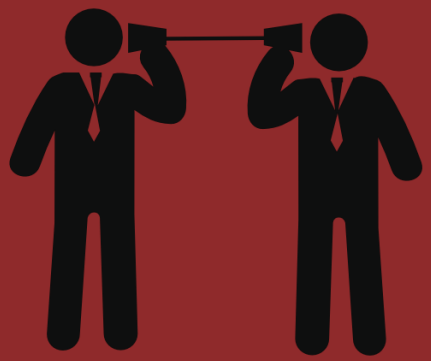
Organizational Security Measures

- Designation of a Data Protection Officer/ Compliance Officer for Privacy
- Data Protection Policies
  - Amount and extent of processing
  - Storage of personal data
  - Regular review and evaluation of privacy policies and practices
- Records of Processing Activities and Personnel responsible/accessible to such records
- Management of Human Resources
- Procedure and Policies for processing of personal data
- Contracts with Personal Information Processors

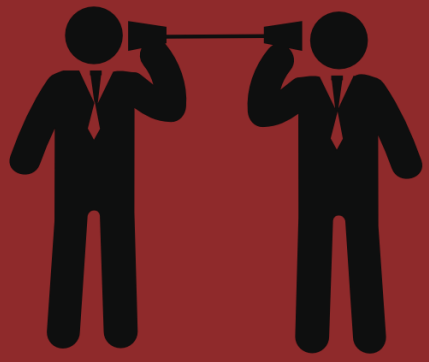
NATIONAL PRIVACY COMMISSION

Physical Security Measures

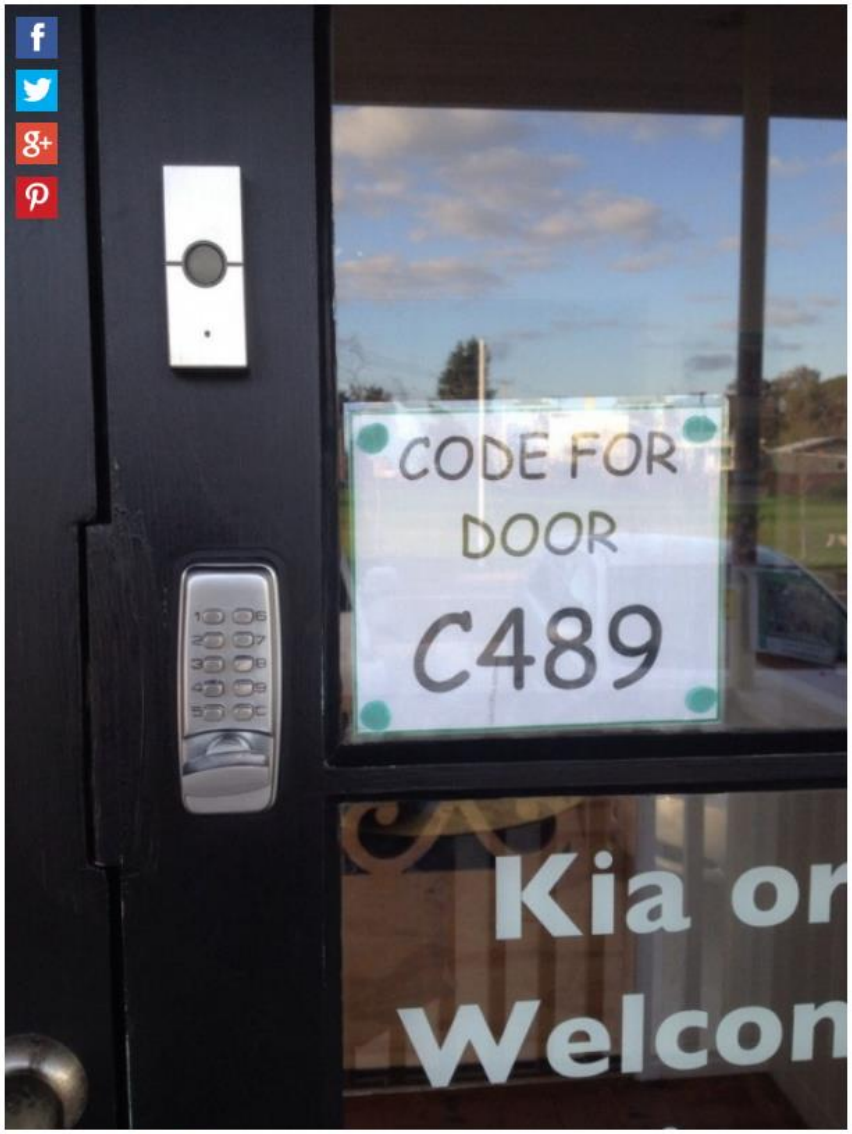
- Policies and procedures to monitor and limit access to and activities in the workstation or facility
- Design of office space and work stations
- Define duties, responsibilities and schedule of individuals involved in the processing of personal data
- Policies on transfer, removal, disposal and re-use of electronic media
- Procedures that prevent mechanical destruction of files and equipment
- The workstation must be secured against natural disasters, power disturbances, external access and similar threats



NATIONAL PRIVACY COMMISSION



secured against natural disasters, power disturbances, external access, and other threats



NATIONAL
PRIVACY
COMMISSION

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).

Medical device company reports data breach due to stolen laptop

January 07, 2015 | Print | Email

Share

Tweet

1

Share

G+

DJO Global, an orthopedic medical device company based in Vista, Calif., reported a data breach after a laptop was stolen from a DJO consultant's car in Roseville, Minn., Nov. 7.

The laptop was password protected but contained patient information, which may have included patient names, phone numbers, diagnosis codes, DJO products received, dates products were ordered and/or shipped, surgery dates, health insurance names, clinic names and provider information, according to the notice.

NATIONAL PRIVACY COMMISSION

Technical Security Measures

- Security policy with respect to processing of personal data
- Protect computer against accidental, unlawful or unauthorized usage or any interference that will affect data integrity
- Regular monitoring for security breaches and process for identifying and accessing reasonably foreseeable vulnerabilities
- Ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident
- Regular testing, assessing and evaluating effectiveness of security measure
- Encryption of personal data during storage, while in transit, authentication process and other technical security measures that control and limit access.

NATIONAL PRIVACY COMMISSION

Ransomware Hijacks Hotel Smart Keys to Lock Guests Out of their Rooms

Saturday, January 28, 2017 Mohit Kumar

What's the worst that could happen when a Ransomware hits a Hotel?

Recently, hundreds of guests of a luxurious hotel in Austria were locked in or out of their rooms when ransomware hit the hotel's IT system, and the hotel had no choice left except paying the attackers.

Bangladesh Bank exposed to hackers by cheap switches, no firewall: police

Serajul Quadir

5 MIN READ

Commuters pass by the front of the Bangladesh central bank building in Dhaka March 8, 2016. Ashikur Rahman/File Photo

DHAKA (Reuters) - Bangladesh's central bank was vulnerable to hackers because it did not have a firewall and used second-hand, $10 switches to network computers connected to the SWIFT global payment network, an investigator into one of the world's biggest cyber heists said.

Processing of personal data that is likely to pose a risk to the rights and freedoms of data subjects:

1. Government branches, bodies or entities;
2. Banks and non-bank financial institutions;
3. Business process outsourcing companies;
4. Universities, colleges and other institutions of higher learning;
5. Hospitals including primary care facilities, multi-specialty clinics, custodial care facilities, diagnostic or therapeutic facilities, specialized out patient facilities, and other organizations processing genetic data;

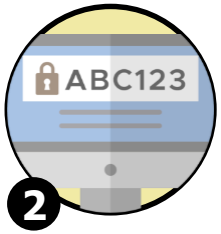
NATIONAL PRIVACY COMMISSION

Personal Data Breach

A **breach of security** leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed.

Availability Breach

Due to **loss**, accidental or unlawful **destruction** of personal data



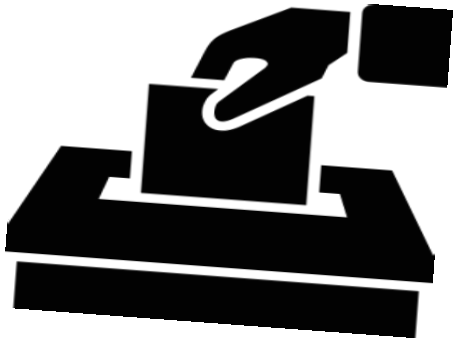
Integrity Breach

Due to **alteration** of personal data

Confidentiality Breach

Due to the **unauthorized disclosure** of or **access** to personal data

NATIONAL PRIVACY COMMISSION



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

NATIONAL PRIVACY COMMISSION

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	

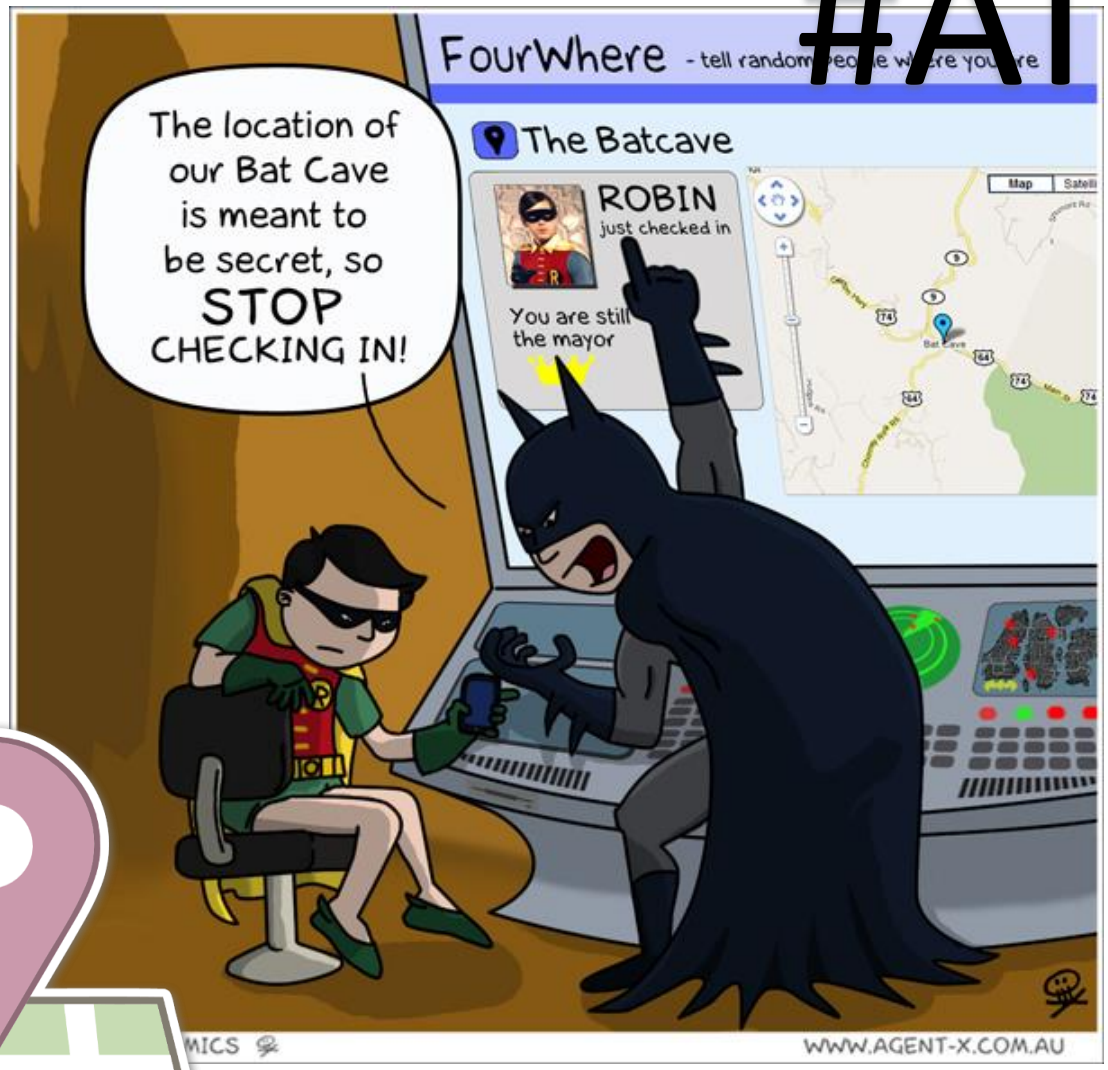
NATIONAL PRIVACY COMMISSION

Don’t be **too public**.

Sa panahon ngayon, mahirap nang ibigay ang lahat-lahat.

While sharing details about your life can be fun and exciting, there are just some things you should never, ever share on social media. Things like your home address, vacation details, ticket numbers, and the layout of your house should always be kept private.

#ATM


FourWhere - tell random people where you are
The Batcave
The location of our Bat Cave is meant to be secret, so STOP CHECKING IN!
ROBIN
just checked in
You are still the mayor
Map
Satelli
WWW.AGENT-X.COM.AU


WHICH
GAME OF THRONES
CHARACTER ARE YOU?


ANONG ITSURA
NG MOVIE
POSTER MO?


84%
Olivia
Angelina Jolie
Which Celebrity Do You Look Like?

30 Ways to Love Yourself Online

A Beginner's Guide to
Personal Data Privacy

NATIONAL
PRIVACY
COMMISSION

TIP#1

Create **strong** passwords.

Pumili ng password na talagang ipaglalaban ka sa mga hacker. Strong passwords are at least 12 characters long and contain a combination of upper and lower case letters, numbers, and if possible, symbols.

NATIONAL
PRIVACY
COMMISSION

TIP#2

Never use the same password on multiple accounts.

'Wag masyadong loyal sa isang password, para mo na ring sinuko lahat agad-agad. Having different passwords on multiple accounts makes it harder for hackers to guess them.

NATIONAL
PRIVACY
COMMISSION

TIP#7

Install an Anti-Virus...and **update** it.

Hindi porket nakuha mo na, iiwan mo nalang sa ere. New viruses are being created all the time, so simply installing an anti-virus program doesn't cut it. It is important to update the programs to keep up with new and emerging threats.

NATIONAL
PRIVACY
COMMISSION

TIP#6

Do not log in on personal accounts on **free or public wifi.**

Hindi lahat ng libre at willing magpagamit ay dapat gamitin. Open networks make it very easy for people to peek into your activity and accounts, and the people you share the network with may also be using compromised devices.

NATIONAL
PRIVACY
COMMISSION

TIP#3

Lock your device.

Diba kapag mahal mo, aalagaan mo?

Leaving a laptop or cellphone unlocked is like leaving an open purse, which hackers are more than happy to take advantage of.

NATIONAL
PRIVACY
COMMISSION

TIP#11

Clean up your **Facebook Third-Party Apps**.

Malaking problema ang mga third party, lalo na sa data privacy. While they are a fun way to find games or see which celebrity you look like, third-party apps on Facebook can and too often send your personal data to at least 25 outside data companies, so it is definitely a good idea to remove permissions from unnecessary ones.

NATIONAL PRIVACY COMMISSION

TIP#8

Don't click on pop-ups or virus warnings.

Kahit marupok, wag basta-basta magpauto. These warnings are now called "scareware," which are fake security alerts telling you to click a link to download software to remove the virus in your computer. The links, however, contain viruses.

NATIONAL
PRIVACY
COMMISSION

Contact us

For invitations: (02)565-9623
For complaints: (02)517-7806
For compliance: (02)517-7810
For public assistance: 09451534299 | 09399638715

or

Email us at
info@privacy.gov.ph

NATIONAL PRIVACY COMMISSION

Thank you!

NATIONAL
PRIVACY
COMMISSION