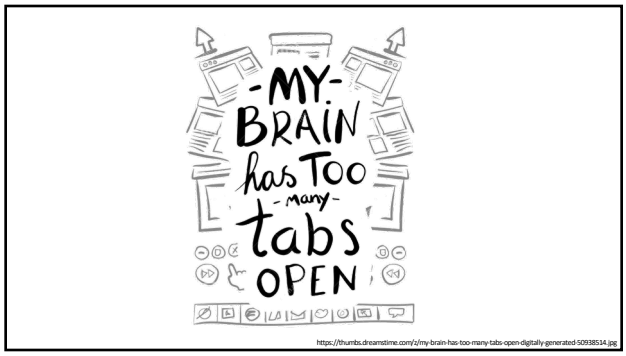
Complying with the Data Privacy Act

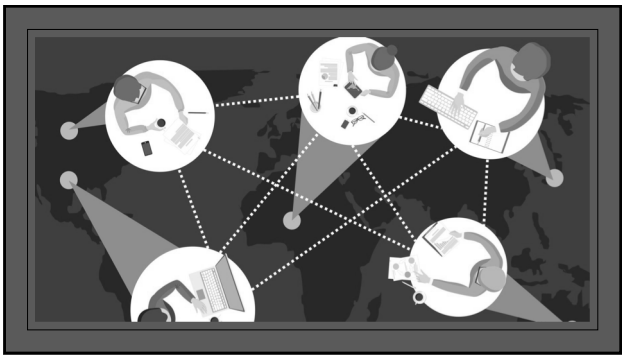
Danny C. Cheng
CISM CRISC COBIT5(F)
DPO(TUV)
Data Protection Officer

The goal is to protect the interest and privacy rights of the data subject not just to comply

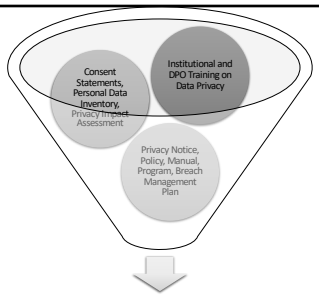
Our journey to date…



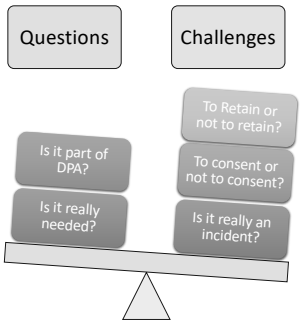
https://thumbs.dreamstime.com/z/my-brain-has-too-many-tabs-open-digitally-generated-50938514.jpg



Ground Zero → 2nd DPO → 9 months in



Where we are at so far...



Can something bad really happen or are we just over reacting?

ZDNET.COM

SingHealth data breach reveals several 'inadequate' security measures | ZDNet

CNET.COM

That British Airways breach shows hackers fine-tuning e-commerce attacks

MEDIUM.COM

Facebook's 29 Million Hack Got Personal Data – FutureSin – Medium

COMPUTERWEEKLY.COM

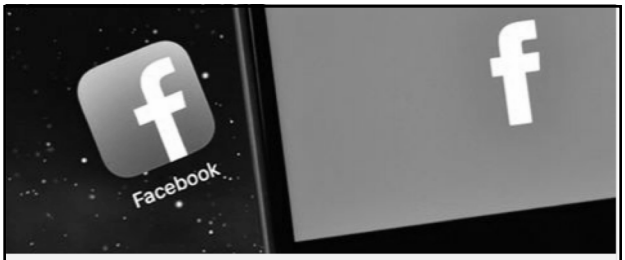
Singapore universities hit by advanced persistent threat attacks

lolloj - Fotolia Singapore universities hit by advanced persistent threat...

It's not all about hacking, privacy issues can be sanctioned

ABC.NET.AU

She's a model citizen, but she still can't hide in China's 'social credit' system

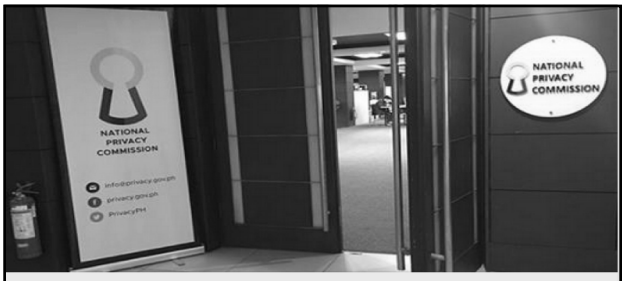


CNNPHILIPPINES.COM

Facebook says PH gov't sought data from 42 of its users

Requests for Facebook account data increase globally by around 26...

All this is already happening close to home (Philippines)

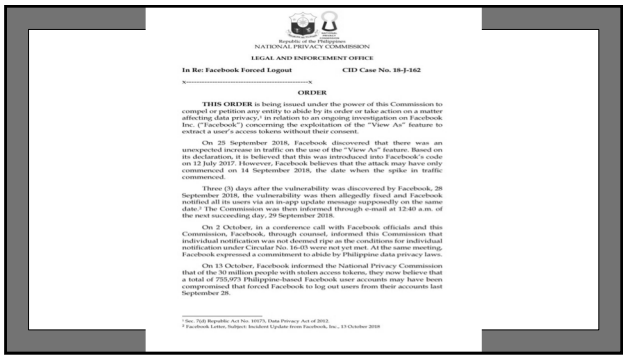


NEWSBYTES.PH

Cathay asked to explain data breach that affected 102,209 PH users

ZDNET.COM

Broadcaster ABS-CBN customer data stolen, sent to Russian servers | ZDNet



Republic of the Philippines
NATIONAL PRIVACY COMMISSION

LEGAL AND ENFORCEMENT OFFICE

In Re: Facebook Forced Logout **CID Case No. 18-J-162**

x----------x

ORDER

THIS ORDER is being issued under the power of this Commission to compel or petition any entity to abide by its order or take action on a matter affecting data privacy,[1] in relation to an ongoing investigation on Facebook Inc. ("Facebook") concerning the exploitation of the "View As" feature to extract a user's access tokens without their consent.

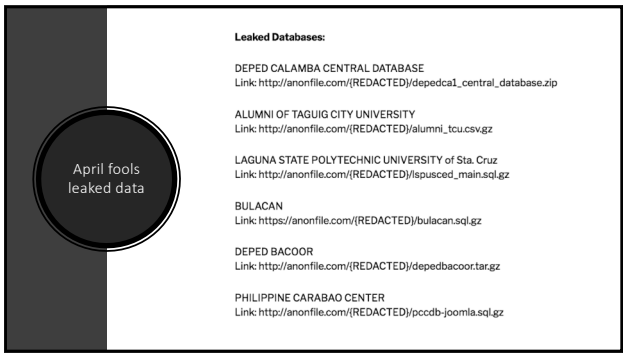
On 25 September 2018, Facebook discovered that there was an unexpected increase in traffic on the use of the "View As" feature. Based on its declaration, it is believed that this was introduced into Facebook's code on 12 July 2017. However, Facebook believes that the attack may have only commenced on 14 September 2018, the date when the spike in traffic commenced.

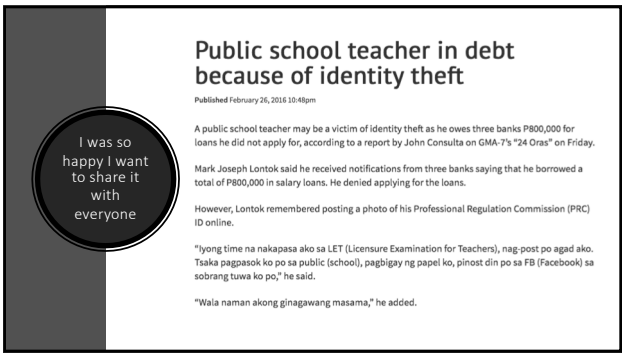
Three (3) days after the vulnerability was discovered by Facebook, 28 September 2018, the vulnerability was then allegedly fixed and Facebook notified all its users via an in-app update message supposedly on the same date.[2] The Commission was then informed through e-mail at 12:40 a.m. of the next succeeding day, 29 September 2018.

On 2 October, in a conference call with Facebook officials and this Commission, Facebook, through counsel, informed this Commission that individual notification was not deemed ripe as the conditions for individual notification under Circular No. 16-03 were not yet met. At the same meeting, Facebook expressed a commitment to abide by Philippine data privacy laws.

On 13 October, Facebook informed the National Privacy Commission that of the 30 million people with stolen access tokens, they now believe that a total of 755,973 Philippine-based Facebook user accounts may have been compromised that forced Facebook to log out users from their accounts last September 28.

[1] Sec. 7(d) Republic Act No. 10173, Data Privacy Act of 2012.
[2] Facebook Letter, Subject: Incident Update from Facebook, Inc., 13 October 2018





It won't happen to me, I change my passwords regularly

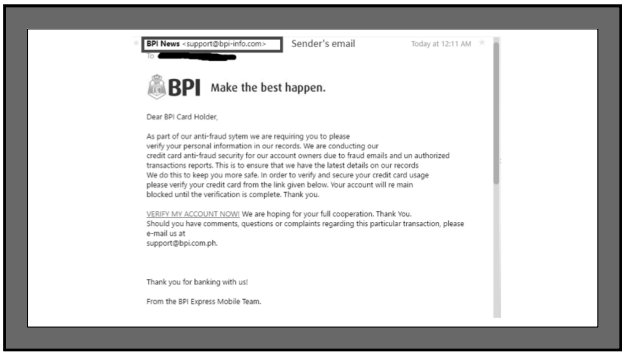
What you think is safe is not actually safe

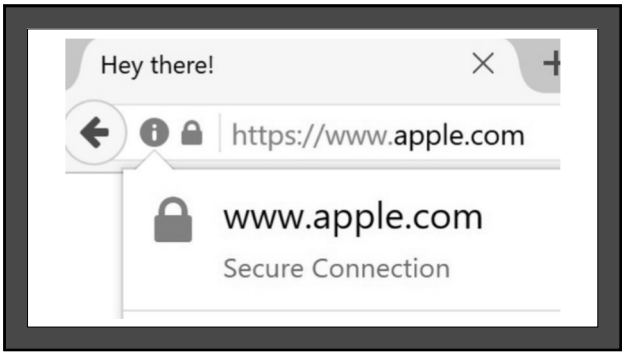
SIM Swap Scam exposes weakness of 2-factor authentication

by Abe Olandres · July 9, 2015

The recent incident of the SIM Swap Scam which victimized Ian Caballero has exposed the long-known weakness of 2-factor authentication which uses an owner's mobile number to verify online banking transactions and site logins.

The premise of a two-factor authentication theoretically strengthens the security of online accounts. This has been used by GMail for the longest time (introduced by Google in 2011) and then implemented later on by several other sites like Facebook and Paypal.



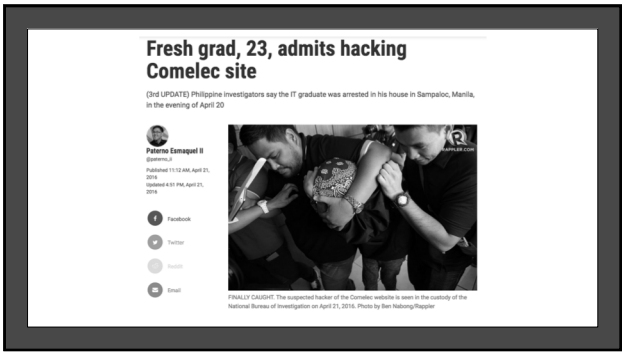


The trick employed by the site is to use Unicode characters that look the same as the appropriate ASCII characters for the site impersonated, explains researcher Xudong Zheng.

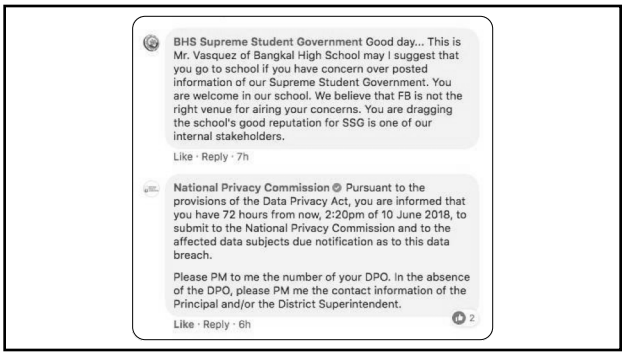
> *It is possible to register domains such as "xn--pple-43d.com", which is equivalent to "apple.com". It may not be obvious at first glance, but "apple.com" uses the Cyrillic "a" (U+0430) rather than the ASCII "a" (U+0061). This is known as a homograph attack.*

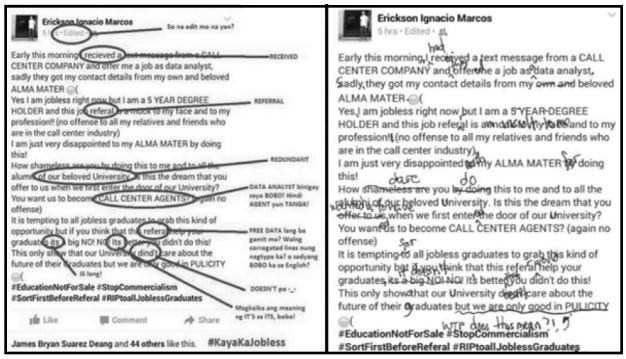
Safari isn't fooled by this, but Chrome, Firefox and Opera all are. You can see this for yourself by using any of them to visit https://www.xn--80ak6aa92e.com (this is perfectly safe, it's a site created by Zheng as a proof of concept). In Safari, you'll see this URL as it appears here – but in the other browsers it will look *exactly* like https://www.apple.com.

We won't be breached, it takes a hard core hacker to do this…



These are not schools, schools won't be targeted or affected…





In the case of Vivares and Suzara vs. St. Theresa's College, et. al. (G.R. No. 202666, September 29, 2014), the Supreme Court through Honorable former Associate Justice Presbitero J. Velasco, Jr., stated:

"This, along with its other features and uses, is confirmation of Facebook's proclivity towards user interaction and socialization rather than seclusion or privacy, as it encourages broadcasting of individual user posts. In fact, it has been said that OSNs have facilitated their users' self-tribute, thereby resulting into the "democratization of fame." Thus, it is suggested, that a profile, or even a post, with visibility set at "Friends Only" cannot easily, more so automatically, be said to be "very private," contrary to petitioners' argument.

Given all of these we really need to understand RA10173

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

What is the Data Privacy Act about?

- It is the policy of the State to protect the **fundamental human right of privacy**, of communication while ensuring free flow of information to promote innovation and growth. The State recognizes the vital role of information and communications technology in nation-building and its **inherent obligation to ensure that personal information in information and communications systems in the government and in the private sector are secured and protected**

Guiding Principle for RA10173

- The processing of personal information shall be allowed, subject to compliance with the requirements of this Act and other laws allowing disclosure of information to the public and adherence to the principles of ***transparency***, ***legitimate purpose*** and ***proportionality***.

What is Personal Data?

- Personal information refers to 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.

What is Personal Data?

- Sensitive personal information refers to personal information:
  1. About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
  2. About an individual's 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;
  3. Issued by government agencies peculiar to an individual which includes, but not limited to, social security numbers, previous or cm-rent health records, licenses or its denials, suspension or revocation, and tax returns; and
  4. Specifically established by an executive order or an act of Congress to be kept classified.

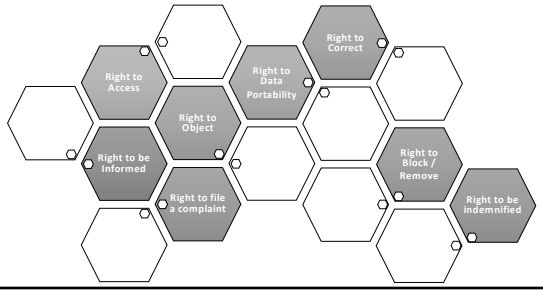
Legitimate Purpose for Personal Information

- For processing to be lawful, any of the following conditions must be complied with:
  1. The data subject must have given his or her consent prior to the collection, or as soon as practicable and reasonable;
  2. The processing involves the personal information of a data subject who is a party to a contractual agreement, 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. The processing is necessary for compliance with a legal obligation to which the personal information controller is subject;
  4. The processing is necessary to protect vitally important interests of the data subject, including his or her life and health;
  5. The processing of personal information is necessary to respond to national emergency or to comply with the requirements of public order and safety, as prescribed by law;
  6. The processing of personal information is necessary for the fulfillment of the constitutional or statutory mandate of a public authority; or
  7. The processing is necessary to pursue the legitimate interests of the personal information controller, or by a third party or parties to whom the data is disclosed, except where such interests are overridden by fundamental rights and freedoms of the data subject, which require protection under the Philippine Constitution.

Legitimate Purpose for Sensitive Personal Information

1. Consent is given by data subject, or by the parties to the exchange of privileged information, prior to the processing of the sensitive personal information or privileged information, which shall be undertaken pursuant to a declared, specified, and legitimate purpose;
2. The processing of the sensitive personal information or privileged information is provided for by existing laws and regulations: Provided, that said laws and regulations do not require the consent of the data subject for the processing, and guarantee the protection of personal data;
3. The processing is 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;
4. The processing is necessary to achieve the lawful and noncommercial objectives of public organizations and their associations provided that:
   1. Processing is confined and related to the bona fide members of these organizations or their associations;
   2. The sensitive personal information are not transferred to third parties; and
   3. Consent of the data subject was obtained prior to processing;
5. The processing is necessary for the purpose of medical treatment: *Provided*, that it is carried out by a medical practitioner or a medical treatment institution, and an adequate level of protection of personal data is ensured; or
6. The processing concerns sensitive personal information or privileged information 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.

Rights of the Data Subject



Right to be Informed

- The data subject has a right to be informed whether personal data pertaining to him or her shall be, are being, or have been processed, including the existence of automated decision-making and profiling.
- The data subject shall be notified and furnished with information indicated hereunder before the entry of his or her personal data into the processing system of the personal information controller, or at the next practical opportunity:
  - Description of the personal data to be entered into the system;
  - Purposes for which they are being or will be processed, including processing for direct marketing, profiling or historical, statistical or scientific purpose;
  - Basis of processing, when processing is not based on the consent of the data subject;
  - Scope and method of the personal data processing;
  - The recipients or classes of recipients to whom the personal data are or may be disclosed;
  - Methods utilized for automated access, if the same is allowed by the data subject, and the extent to which such access is authorized, including meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject;
  - The identity and contact details of the personal data controller or its representative;
  - The period for which the information will be stored; and
  - The existence of their rights as data subjects, including the right to access, correction, and object to the processing, as well as the right to lodge a complaint before the Commission.

Right to Access

- The data subject has the right to reasonable access to, upon demand, the following:
  1. Contents of his or her personal data that were processed;
  2. Sources from which personal data were obtained;
  3. Names and addresses of recipients of the personal data;
  4. Manner by which such data were processed;
  5. Reasons for the disclosure of the personal data to recipients, if any;
  6. Information on automated processes where the data will, or is likely to, be made as the sole basis for any decision that significantly affects or will affect the data subject;
  7. Date when his or her personal data concerning the data subject were last accessed and modified; and
  8. The designation, name or identity, and address of the personal information controller.

Right to Erasure or Blocking

- The data subject shall have the right to suspend, withdraw or order the blocking, removal or destruction of his or her personal data from the personal information controller's filing system.
  - This right may be exercised upon discovery and substantial proof of any of the following:
    - The personal data is incomplete, outdated, false, or unlawfully obtained;
    - The personal data is being used for purpose not authorized by the data subject;
    - The personal data is no longer necessary for the purposes for which they were collected;
    - The data subject withdraws consent or objects to the processing, and there is no other legal ground or overriding legitimate interest for the processing;
    - The personal data concerns private information that is prejudicial to data subject, unless justified by freedom of speech, of expression, or of the press or otherwise authorized;
    - The processing is unlawful;
    - The personal information controller or personal information processor violated the rights of the data subject.
  - The personal information controller may notify third parties who have previously received such processed personal information.

How to comply?

Appoint a Data Protection Officer	Conduct a Privacy Impact Assessment	Write your Privacy Management Program and Manual	Implement Privacy and Data Protection Measures	Regularly Exercise Breach Reporting Process

Penalties as well as Risks or Exposures

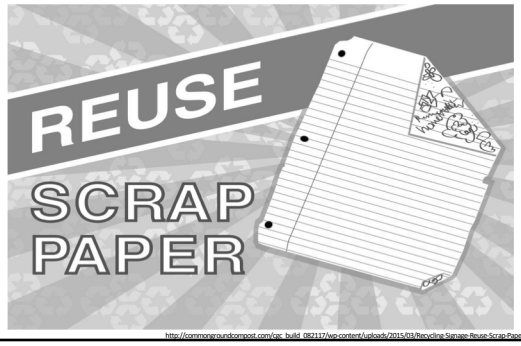
Section	Punishable Act	Jail Term	Fine
25	Unauthorized processing	1y to 3y – 3y to 6y	500k to 4m
26	Access due to negligence	1y to 3y – 3y to 6y	500k to 4m
27	Improper disposal	6m to 2y – 3y to 6y	100k to 1 m
28	Unauthorized purposes	18m to 5y – 2y to 7y	500k to 2m
29	Intentional breach	1y to 3y	500k to 2m
30	Concealment of breach	18m to 5y	500k to 1m
31	Malicious Disclosure	18m to 5y	500k to 1m
32	Unauthorized Disclosure	1y to 3y – 3y to 5y	500k to 2m
33	Combination of Acts	3y to 6y	1m to 5m

Triggers for Investigation

Events that may trigger a visit or Investigation from the National Privacy Commission

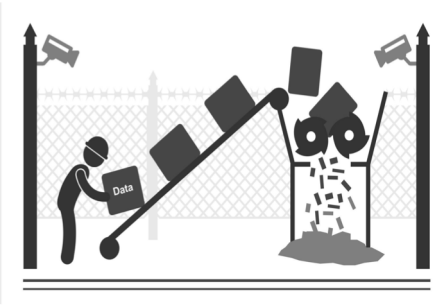
- Complaint from a data subject
- Report from a whistle blower
- Own Initiative
- Random Audit

Some cases or common practice that can lead to problems…



http://commongroundcompost.com/cgc_build_082117/wp-content/uploads/2015/03/Recycling-Signage-Reuse-Scrap-Paper-850x657.jpg


http://deptmed.queensu.ca/blog/wp-content/uploads/pic1.png



http://www.adlprocess.com/wp-content/uploads/2016/11/SDD-slide-3.jpg

NPC as a good source of information

Circulars from the National Privacy Commission

- 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
- NPC Circular 18-01 – Rules of procedure on requests for Advisory Opinions
- NPC Circular 18-02 – Guidelines on Compliance Checks

NPC on Consent and Consent Management

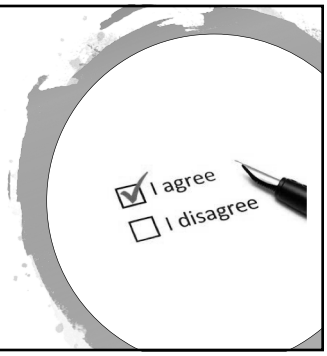
CONSENT

Freely Given
Reversible
Informed
Enthusiastic
Specific

How is consent defined?

- "Consent of the data subject" refers to any freely given, specific, informed indication of will, whereby the data subject agrees to the collection and processing of his or her personal, sensitive personal, or privileged information. Consent shall be evidenced by written, electronic or recorded means. It may also be given on behalf of a data subject by a lawful representative or an agent specifically authorized by the data subject to do so;

Minors cannot give consent and privacy rights cannot be waived, just given consent for processing…



Implied Consent

"**By continuing to avail of XXX XXX XXX products and services:**

- You explicitly authorize XXX XXX XXX, its employees, duly authorized representatives, related companies and third-party service providers, to use, process and share Personal Data needed in the administration of your XXX XXX XXX;
- You consent to XXX XXX XXX using your contact details, demographic information and accounting details to contact you with marketing or promotional information regarding financial products and studies/surveys to be conducted by XXX XXX XXX via phone calls, mail, email, SMS or any type of electronic facility; and,
- You consent to XXX XXX XXX using your Personal Data for purposes of providing services to you or for other reasonable purposes which are related to the services it provides or improvements/upgrades in its systems and business processes, including but not limited to data analytics and automated processing.

xxx

Please take the time to read our Privacy Policy Statement available at this link HERE to know more about.

- The purposes for collecting and processing Personal Data;
- The parties with whom XXX XXX XXX may disclose and share your Personal Data;
- The risks of processing and data security measures in place to protect you against these risks;
- Your rights as data subjects, i.e., your right to be informed, to object, access, correct or block your Personal Data, right to data portability, right to file a complaint and right to damages; and,
- How long your information will be processed and retained.

This authorization and consent are as valid as a signed document and will continue to have effect throughout the duration of your coverage under your policy/plan, or existence of your account(s), and/or until expiration of the retention limit set by laws and regulations from account disclosure, and the period set until destruction or disposal of records, unless withdrawn in writhing or withheld due to changes in the information supplied by the Company."

The NPC would like to reiterate that implied or inferred consent is not recognized in this jurisdiction. The entity, as personal information controller or personal information processor must never assume the data subject's consent for any activity involving his or her personal information, most especially, sensitive personal information, **unless circumstances permit the processing of personal or sensitive personal information without consent, pursuant to the DPA and the IRR.** In cases where consent is not required, a privacy notice would be sufficient.

Storage and Disclosure

Advisory Opinion No. 2018-006

- In your letter, you stated that you have requested information regarding your biological father from the LPU Registrar and the Alumni Affairs Office, specifically the following information: a) middle name; b) last registered address; and c) parents' names.
- We understand that you will use these information in relation to your personal search of your father whom you have not seen since you were a child.
- Given the responsibility of LPU to secure personal information, its denial of your request for information may be justified due to the lack of consent of the data subject. Although consent is not the only condition for lawful disclosure or processing, in general, of personal information, it may be the most appropriate criterion in this scenario
- Likewise, LPU as the PIC is mandated to recognize and enforce the rights of the data subject, including the right to be informed regarding the recipients to whom data will be disclosed. Thus, the data subject, your biological father, must be informed, and most importantly, approve of the disclosure of his personal information to you.

Advisory Opinion No. 2018-020

- We understand that it has been a common practice among universities such as the University of the East Ramon Magsaysay Memorial Medical Center, Inc. (UERMMMCI), a personal information controller (PIC), to post on its bulletin board, the names of successful applicants to the College of Medicine. This is done without the consent of the students. Under the DPA, such activity is considered as processing of personal information
- The aforesaid publication of the names of admitted applicants is permitted even without the consent of the students, pursuant to Section 12(f) of the DPA.
- Presumably, when an applicant applies for admission, which involves submitting forms with his or her personal information, and subsequently taking the examination, the applicant is aware that the school will process the personal information, particularly his or her name for purposes that are relevant to his or her admission, such as publication of successful applicants' names. This means that the applicant could reasonably expect that his or her name may be posted on the bulletin board of the school if one has successfully hurdled the examinations.
- This being said, it is still recommended, in the future, to obtain their consent. For instance, consent may be obtained in their application form for purpose of posting in bulletin boards the names of those accepted. This is a means to ensure that the PIC adheres to principles of transparency and legitimate purpose.

Retention and Disposal

d. Personal Data shall not be retained longer than necessary.

1. Retention of personal data shall only for as long as necessary:

(a) for the fulfillment of the declared, specified, and legitimate purpose, or when the processing relevant to the purpose has been terminated;

(b) for the establishment, exercise or defense of legal claims; or

(c) for legitimate business purposes, which must be consistent with standards followed by the applicable industry or approved by appropriate government agency.

2. Retention of personal data shall be allowed in cases provided by law.

3. Personal data shall be disposed or discarded in a secure manner that would prevent further processing, unauthorized access, or disclosure to any other party or the public, or prejudice the interests of the data subjects.

e. Any authorized further processing shall have adequate safeguards.

1. Personal data originally collected for a declared, specified, or legitimate purpose may be processed further for historical, statistical, or scientific purposes, and, in cases laid down in law, may be stored for longer periods, subject to implementation of the appropriate organizational, physical, and technical security measures required by the Act in order to safeguard the rights and freedoms of the data subject.

2. Personal data which is aggregated or kept in a form which does not permit identification of data subjects may be kept longer than necessary for the declared, specified, and legitimate purpose.

3. Personal data shall not be retained in perpetuity in contemplation of a possible future use yet to be determined.

The need to register personal data processing systems

Have you registered your data processing systems with NPC?

- The PIC or PIP employs at least two hundred fifty (250) employees;
- The processing includes sensitive personal information of at least one thousand (1,000) individuals;
- The processing is likely to pose a risk to the rights and freedoms of data subjects. Processing operations that pose a risk to data subjects include those that involve:
  - information that would likely affect national security, public safety, public order, or public health;
  - information required by applicable laws or rules to be confidential;
  - vulnerable data subjects like minors, the mentally ill, asylum seekers, the elderly, patients, those involving criminal offenses, or in any other case where an imbalance exists in the relationship between a data subject and a PIC or PIP;
  - automated decision-making; or
  - profiling;

Have you registered your data processing systems with NPC?

1. GOVERNMENT BRANCHES, BODIES OR ENTITIES, INCLUDING NATIONAL GOVERNMENT AGENCIES, BUREAUS OR OFFICES, CONSTITUTIONAL COMMISSIONS, LOCAL GOVERNMENT UNITS, GOVERNMENT-OWNED AND -CONTROLLED CORPORATIONS
2. BANKS AND NON-BANK FINANCIAL INSTITUTIONS, INCLUDING PAWNSHOPS NON-STOCK SAVINGS AND LOAN ASSOCIATIONS (NSSLAS)
3. TELECOMMUNICATIONS NETWORKS, INTERNET SERVICE PROVIDERS AND OTHER ENTITIES OR ORGANIZATIONS PROVIDING SIMILAR SERVICES
4. BUSINESS PROCESS OUTSOURCING COMPANIES
5. UNIVERSITIES, COLLEGES AND OTHER INSTITUTIONS OF HIGHER LEARNING, ALL OTHER SCHOOLS AND TRAINING INSTITUTIONS
6. 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

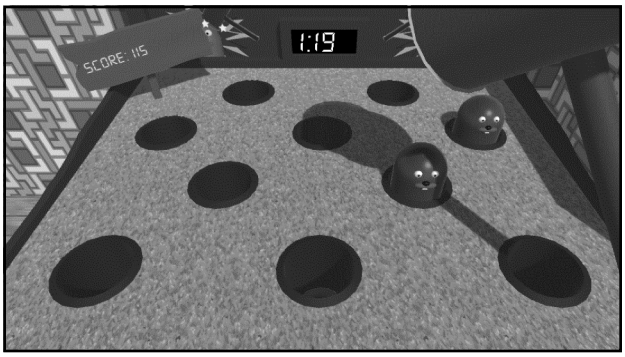
Have you registered your data processing systems with NPC?

7. PROVIDERS OF INSURANCE UNDERTAKINGS, INCLUDING LIFE AND NON-LIFE COMPANIES, PRE-NEED COMPANIES AND INSURANCE BROKERS
8. BUSINESS INVOLVED MAINLY IN DIRECT MARKETING, NETWORKING, AND COMPANIES PROVIDING REWARD CARDS AND LOYALTY PROGRAMS
9. PHARMACEUTICAL COMPANIES ENGAGED IN RESEARCH
10. PERSONAL INFORMATION PROCESSORS PROCESSING PERSONAL DATA FOR A PERSONAL INFORMATION CONTROLLER INCLUDED IN THE PRECEDING ITEMS, AND DATA PROCESSING SYSTEMS INVOLVING AUTOMATED DECISION-MAKING

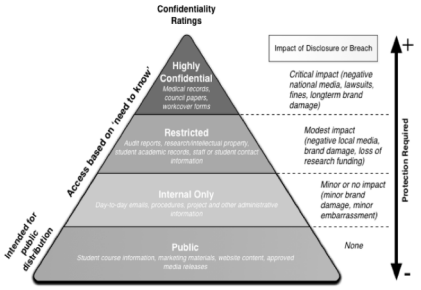
How can we protect ourselves?

Either from violating or being non-compliant or being the one impacted by violations on privacy

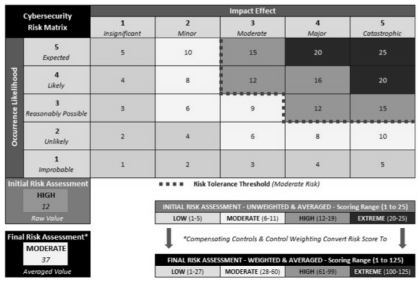
"Information security is a major priority at this company. We've done a lot of stupid things we'd like to keep secret."



Identify, Classify, and Maintain an Inventory



Know where you are vulnerable or at Risk and its Impact



Privacy Impact Assessment

- A **Privacy Impact Assessment (PIA)** is a process which assists organizations in identifying and minimizing the privacy risks of new projects or policies

A PIA is designed to accomplish three goals:

1. Ensure conformance with applicable legal, regulatory, and policy requirements for privacy;
2. Determine the risks and effects; and
3. Evaluate protections and alternative processes to mitigate potential privacy risks.

A PIA is designed to accomplish three goals:

- **Provides an early warning system, a way to detect privacy problems, build safeguards before, not after, heavy investment –Fix privacy problems now, not later**
- **Avoids costly or embarrassing privacy mistakes**
- **Provides evidence that an organization attempted to prevent privacy risks (reduce liability, negative publicity, damage to reputation)**
- **Enhances informed decision-making**
- **Helps the organization gain the public's trust and confidence**
- **Demonstrates to employees, contractors, customers, citizens that the organization takes privacy seriously**

Personal Data Inventory

Data Elements	Classification	Source	Purpose	Basis	Location	Internal Users	PIP Users	Other PIC Users	Use/Disclosure Policy	Protection Policy	Backup Policy	Disposal/Retention Policy

Privacy Impact Assessment

PROCESS/ PROGRAM	POTENTIAL RISKS	THREAT	VULNERABILITY	SEVERITY	LIKELIHOOD	RECOMMENDED CONTROLS

Types of Risks to Consider (Categories)

- Unauthorized Disclosure
- Unauthorized Purposes
- Unauthorized Processing
- Access due to Negligence
- Malicious Disclosure
- Improper Disposal
- Intentional Breach
- Concealment of Breach
- Incorrect information stored
- Loss of Information due to intentional and non-intentional acts

Types of Threats to Consider (Samples)

- Malicious and Non-malicious internal personnel or student
  - Shoulder surfing
  - Part of talking points with friends and family
- Acts of God or Nature
- Internal and External Hacking
  - Phishing
  - Negligence and malware infection
- Theft by individuals within and outside of the campus
- Third Party Provider misuse of data
- Please classify whether its Confidentiality, Integrity, Availability

Types of Vulnerabilities to Consider (Samples)

- Unknown or unclassified information
- Lack of existing policies and procedures
- Inconsistent implementation of policies and procedures
- Lack of awareness training / campaign
- Lack of physical or technical controls
- Lack of time and/or resource to implement policies and procedures
- Urgent needs and demands that contradict compliance
- Negligence of individuals
- Limitation of capabilities of processes and resources (really not possible)
- Lack of Data Sharing Agreement or Internal Sharing Policy

Threats, Vulnerabilities, and Risks

- Risk = Likelihood x Impact for a specific threat exploiting a vulnerability, where likelihood can further be divided into likelihood of attack from a threat and likelihood of success of an attack (based on threats and vulnerabilities). Where Impact can be divided on impact on Confidentiality, Integrity, and Availability
- Risk is a function of threats exploiting vulnerabilities to obtain, damage or destroy assets. Thus, threats (actual, conceptual, or inherent) may exist, but if there are no vulnerabilities then there is little/no risk. Similarly, you can have a vulnerability, but if you have no threat, then you have little/no risk.

Likelihood and Impact

Impact		
Rating	Types	Description
1	Negligible	The data subjects will either not be affected or may encounter a few inconveniences, which they will overcome without any problem.
2	Limited	The data subject may encounter significant inconveniences, which they will be able to overcome despite a few difficulties.
3	Significant	The data subjects may encounter significant inconveniences, which they should be able to overcome but with serious difficulties.
4	Maximum	The data subjects may encounter significant inconveniences, or even irreversible, consequences, which they may not overcome.
Probability		
1	Unlikely	Not expected, but there is a slight possibility it may occur at some time.
2	Possible	Casual occurrence. It might happen at some time.
3	Likely	Frequent occurrence. There is a strong possibility that it might occur.
4	Almost Certain	Very likely. It is expected to occur in most circumstances.

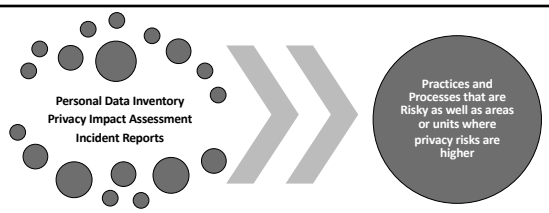
Assessment

	Unlikely	Possible	Likely	Almost Certain
Maximum				
Significant				
Limited				
Negligible				

Currently within acceptable level of risk

Need to implement controls to reduce the risk

Why are we doing this and what do we get out of it…



What We Based Our Findings On

Practices and Processes that are Risky as well as areas or units where privacy risks are higher

What We Discovered

http://www.ftjournal.com/uploads/images/resized/uploads/images/FTI-fakenews-930x470.jpg

What happens when there is a breach?

When do we have a breach / incident?

- "Personal data breach" refers to 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. A personal data breach may be in the nature of:
  - An availability breach resulting from loss, accidental or unlawful destruction of personal data;
  - Integrity breach resulting from alteration of personal data; and/or
  - A confidentiality breach resulting from the unauthorized disclosure of or access to personal data.

When is it required to report?

- SECTION 11. When notification is required. Notification shall be required upon knowledge of or when there is reasonable belief by the personal information controller or personal information processor that a personal data breach requiring notification has occurred, under the following conditions:
  - The personal data involves sensitive personal information or any other information that may be used to enable identity fraud. For this purpose, "other information" shall include, but not be limited to: data about the financial or economic situation of the data subject; usernames, passwords and other login data; biometric data; copies of identification documents, licenses or unique identifiers like Philhealth, SSS, GSIS, TIN number; or other similar information, which may be made the basis of decisions concerning the data subject, including the grant of rights or benefits.
  - There is reason to believe that the information may have been acquired by an unauthorized person; and
  - The personal information controller or the Commission believes that the unauthorized acquisition is likely to give rise to a real risk of serious harm to any affected data subject.

Other considerations for reporting…

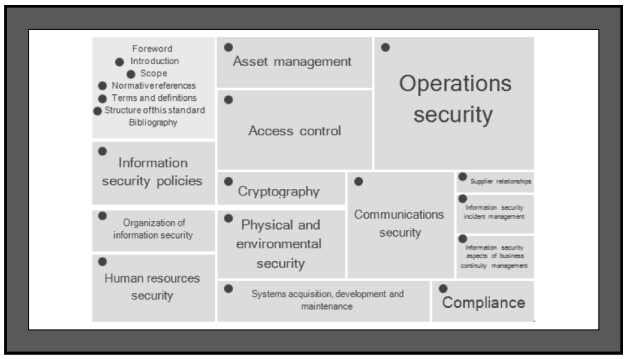
- SECTION 13. Determination of the Need to Notify. Where there is uncertainty as to the need for notification, the personal information controller shall take into account, as a primary consideration, the likelihood of harm or negative consequences on the affected data subjects, and how notification, particularly of the data subjects, could reduce the risks arising from the personal data breach reasonably believed to have occurred. The personal information controller shall also consider if the personal data reasonably believed to have been compromised involves:
  - Information that would likely affect national security, public safety, public order, or public health;
  - At least one hundred (100) individuals;
  - Information required by applicable laws or rules to be confidential; or
  - Personal data of vulnerable groups.

Notification to the Commission…

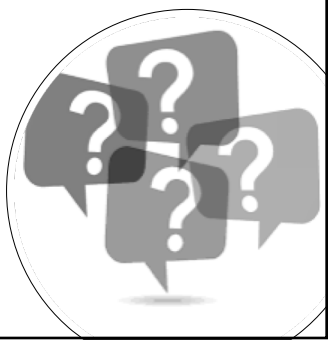
- When Notification Should be Done. The Commission shall be notified within seventy-two (72) hours upon knowledge of or the reasonable belief by the personal information controller or personal information processor that a personal data breach has occurred.
- Delay in Notification. Notification may only be delayed to the extent necessary to determine the scope of the breach, to prevent further disclosures, or to restore reasonable integrity to the information and communications system. The personal information controller need not be absolutely certain of the scope of the breach prior to notification.

How does one manage the Privacy Manual and Program?

How does one implement personal data protection measures?



Some commonly asked questions



Some previously asked questions…

- Can a school stop processing an application if applicants (e.g parents/guardians, student) give incomplete personal data or refuse to supply certain information in a form?
- If a parent requests for a copy of grades of her daughter who is no longer a minor, should the school disclose the grades even without the consent of the student or should we get the consent of the student?
- How to handle posting of pictures of students in social media accounts or marketing collaterals of the school?
- Do we need to get the consent of our faculty if we put their names, email addresses and pictures in the website?

Some previously asked questions…

- Are academic institutions allowed to store or file the personal data of its faculty (without being anonymized) in a database system to be utilized for school accreditation purposes?
- How do we deal with CHED and the personal data we share with them?
- What information, documents/ materials containing personal data can a school release for public information?
- Are foreign students or employees included in the Data Privacy Act of 2012?
- Can a school give out information for activities like tracer studies?

danny.cheng@dlsu.edu.ph