

REPUBLIC ACT NO. 10175

"Cybercrime Prevention Act of 2012"

REPUBLIC ACT NO. 10175

AN ACT DEFINING CYBERCRIME,
PROVIDING FOR THE PREVENTION,
INVESTIGATION,
SUPPRESSION
AND THE IMPOSITION OF PENALTIES
THEREFOR
AND FOR OTHER PURPOSES

LEGAL BACKGROUND

Electronic Commerce Act of 2000
(RA No. 8792)

- – AN ACT PROVIDING FOR THE RECOGNITION AND USE OF ELECTRONIC COMMERCIAL AND NON -COMMERCIAL TRANSACTIONS AND DOCUMENTS, PENALTIES FOR UNLAWFUL USE THEREOF AND FOR OTHER PURPOSES

Why is there a need to pass such law?

ILOVEYOU VIRUS by Onel de Guzman



- The current laws at that time did not provide a legal basis for criminalizing crimes committed on a computer in general.

Related Facts

Sonido maintains a blog called "Baratillo pamphlet" over the internet.



Sonido posted 2 blogs which express his opinion regarding Senator Sotto's alleged plagiarism of online materials for use in his speech against RH Bill.



Sotto warned his critics that when it became a law, they will be penalized



And so it happened, sotto materialized his threats

Reactions

The screenshot shows a Facebook interface. The main post is a black image with white text: "The PHILIPPINE GOVERNMENT yesterday passed the Cybercrime Law of 2012 is the E-Martial Law". Below this, a red box contains the word "STOP" in white, followed by "IT NOW!". Underneath, it says "THIS IS THE KILLING OF THE FREEDOM OF EXPRESSION". A small image of a man with a mustache and the text "I will not be silenced... NO TO RA 10175" is visible in the bottom right of the post. The post has a "Cover Photos" section showing "1 of 21". To the right, a sidebar shows the post's details: a profile picture, the date "Thursday 4/4", the text "STOP CYBERCRIME ACT! THIS IS KILLING OUR RIGHT TO FREEDOM OF EXPRESSION!", and buttons for "Tag Photo", "Add Location", and "Edit". Below this are options to "Like", "Comment", "Unfollow Post", "Share", and "Edit". A comment section shows a user's profile picture and the text "Write a comment...". At the bottom, a sponsored ad for "BE HOTspot!" is visible, featuring a small image of a device and the text "Be a 4G Hotspot! Get and give access for 6 devices. Click here for more details." The ad also mentions "16,275 people like wi-tribePH4."

The PHILIPPINE GOVERNMENT yesterday passed the Cybercrime Law of 2012 is the E-Martial Law

STOP IT NOW!
THIS IS THE KILLING OF THE FREEDOM OF EXPRESSION

I will not be silenced...
NO TO RA 10175

Cover Photos 1 of 21

Tag Photo Options Share Like

Thursday 4/4

STOP CYBERCRIME ACT!
THIS IS KILLING OUR RIGHT TO FREEDOM OF EXPRESSION!

Tag Photo Add Location Edit

Like Comment Unfollow Post Share Edit

Write a comment...

Sponsored

BE HOTspot!

Be a 4G Hotspot! Get and give access for 6 devices. Click here for more details.

16,275 people like wi-tribePH4.

How did it become a law?

This law emanated from HB No. 5808, authored by Representative Susan Yap-Sulit of the second district of Tarlac and 36 other co-authors,

Senate Bill No. 2976, proposed by Senator Edgardo Angara.

Both bills were passed by their respective chambers within one day of each other on June 5 and 4, 2012, respectively, shortly after the impeachment of Renato Corona

the final version of the Act was later signed into law by President Benigno Aquino III on September 12, 2012.

Some Terms to be familiarized

Access

- refers to the instruction, communication with, storing data in, retrieving data from, or otherwise making use of any resources of a computer system or communication network.

Cyber

- refers to a computer or a computer network, the electronic medium in which online communication takes place.

Interception

- refers to listening to, recording, monitoring or surveillance of the content of communications, including procurement of the content of data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring.

Section 4: Punishable Acts

Offenses against the confidentiality, integrity and availability of computer data and systems

- Computer-related Offenses
- Content-related Offenses

Offenses against the confidentiality, integrity and availability of computer data and systems

Illegal Access – The intentional access to the whole or any part of a computer system without right;

Illegal Interception – The intentional interception made by TECHNICAL MEANS

- Exception: Employee or agent of a service provider
- Exception to the Exception: Except that the latter shall not utilize service observing or random monitoring except for mechanical or service control quality checks;

Data Interference – The intentional or reckless alteration, damaging, deletion or deterioration of computer DATA

System Interference – The intentional alteration or reckless hindering or interference with the functioning of a computer or computer NETWORK

Offenses against the confidentiality, integrity and availability of computer data and systems

Misuse of Devices.

- The use, PRODUCTION, SALE, PROCUREMENT, IMPORTATION, DISTRIBUTION or otherwise MAKING available intentionally and without right, of:
 - A device for the purpose of committing any of the offenses
 - A computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed with the intent that it be used for the purpose of committing any of the offenses under this Act;
- The POSSESSION of an item referred to in paragraphs (a), 5(i)(aa) or (bb) herein with the intent to use said devices for the purpose of committing any of the offenses under this section

Offenses against the confidentiality, integrity and availability of computer data and systems

Cyber-squatting

- The ACQUISITION OF A DOMAIN name over the internet in bad faith to profit, mislead, destroy reputation, and DEPRIVE OTHERS FROM REGISTERING THE SAME.
- Similar, identical, or confusingly similar to an existing trademark registered with the appropriate government agency at the time of the domain name registration:
- Identical or in any way similar with the name of a person other than the registrant, in case of a personal name; and
- Acquired without right or with intellectual property
- interests in it.

PUBLIC OF SINGAPORE

NTITY CARD NO. S [REDACTED] 8131



Name

BATMAN BIN SUPARMAN



باتمن بن سوپارمن

Race

JAVANESE

Date of birth

13-05-1990

Sex

M

Country of birth

SINGAPORE



Computer-related Offenses

Computer Forgery.

- The intentional input, alteration, deletion or suppression of any computer data, without right resulting in unauthentic data WITH THE INTENT that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible;
- The act of knowingly using a computer data which is the product of computer-related forgery as defined herein, for the purpose of perpetuating a fraudulent or dishonest design;

Computer-related Offenses

2. Computer-related Fraud

- o the intentional and unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system including, but not limited to, phishing, causing damage thereby, WITH THE INTENT of procuring an economic benefit for oneself or for another person or for the perpetuation of a fraudulent

3. Computer-related Identity Theft

- The intentional acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information BELONGING TO ANOTHER, whether natural or juridical, without right.

Content-related Offenses

1. Cybersex

- includes any form of interactive prostitution and other forms of obscenity through the cyberspace as the primary channel with the use of webcams, by inviting people either here or in other countries to watch men, women and children perform sexual acts;

2. Child Pornography

- The unlawful or prohibited acts defined and punishable by Republic Act No. 9775 or the Anti-Child Pornography Act of 2009, committed through a computer system: Provided, That the penalty to be imposed shall be (1) one degree higher than that provided for in Republic Act No. 9775.

Panda recém-nascido, com 11 cm e 129 gramas, é visto em centro de pesquisa de pandas gigantes, em Chengdu (China); a panda gigante Shu Qing deu à luz dois gêmeos. [Leia mais](#)



Content-related Offenses

Unsolicited Commercial Communications

- The transmission of commercial electronic communication with the use of a computer system which seeks to advertise, sell or offer for sale products and services are prohibited unless:
 - There is a prior affirmative consent from the recipient; or
 - The following conditions are present:
 - The commercial electronic communication contains a simple, valid and reliable way for the recipient to reject receipt of further commercial electronic communication from the same source, also referred to as opt-out;
 - The commercial electronic communication does not purposely disguise the source of the electronic message; and
 - The commercial electronic communication does not purposely include misleading information in any part of the message in order to induce the recipients to read the message.

Content-related Offenses

4. Libel

- o The unlawful or prohibited acts of libel as defined in Article 355 of the Revised Penal Code, as amended, committed through a computer system or any other similar means which may be devised in the future.

All crimes defined and penalized by the Revised Penal Code, as amended, and special criminal laws committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act.²⁰

YOU ARE REGRETFULLY INVITED
TO THE WEDDING BETWEEN MY PERFECT SON,

The Doctor

AND SOME

Cheap Two-Bit Tramp

WHOSE NAME ESCAPES ME RIGHT NOW.

THE BIGGEST DISASTER IN MY
FAMILY'S HISTORY WILL TAKE PLACE AT

9pm on Saturday, September 8th

AND NO DOUBT END IN DIVORCE.

HOPEFULLY IN TIME TO STILL BE ELIGIBLE FOR AN ANNULMENT.
THE OVERWHELMINGLY DISAPPOINTING HEARTBREAK OF A CEREMONY
WILL BE FOLLOWED BY DINNER, WHERE NUTS WILL BE SERVED
BECAUSE WHATSHERFACE HAS AN ALLERGY.



Section 5: Other Offenses

Aiding or Abetting in the Commission of Cybercrime

- Any person who wilfully abets, aids or financially benefits in the commission of any of the offenses enumerated in this Act shall be held liable; or

Attempt to Commit Cybercrime

- Any person who wilfully attempts to commit any of the offenses enumerated in this Act shall be held liable.

Section 6

- All crimes defined and penalized by the Revised Penal Code, as amended, and special laws, if committed by, through and with the use of information and communications technologies shall be covered by the relevant provisions of this Act: *Provided*, That the penalty to be imposed shall be ONE (1) DEGREE HIGHER THAN THAT PROVIDED for by the Revised Penal Code, as amended, and special laws, as the case may be.

Section 7. Liability under Other Laws

- A prosecution under this Act shall be WITHOUT PREJUDICE TO ANY LIABILITY FOR VIOLATION OF ANY PROVISION OF THE REVISED PENAL CODE, as amended, or special laws.

Section 8. Penalties

Any person found guilty of any of the punishable acts enumerated in Sections 4(a) and 4(b) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos (PhP200,000.00) up to a maximum amount commensurate to the damage incurred or both.

Any person found guilty of the punishable act under Section 4(a)(5) shall be punished with imprisonment of *prision mayor* or a fine of not more than Five hundred thousand pesos (PhP500,000.00) or both.

Section 8. Penalties

If punishable acts in Section 4(a) are committed against critical infrastructure, the penalty of *reclusion temporal* or a fine of at least Five hundred thousand pesos (PhP500,000.00) up to maximum amount commensurate to the damage incurred or both, shall be imposed.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(1) of this Act shall be punished with imprisonment of *prision mayor* or a fine of at least Two hundred thousand pesos (PhP200,000.00) but not exceeding One million pesos (PhP1,000,000.00) or both.

Section 8. Penalties

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(2) of this Act shall be punished with the penalties as enumerated in Republic Act No. 9775 or the "Anti-Child Pornography Act of 2009": *Provided*, That the penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act No. 9775, if committed through a computer system.

Any person found guilty of any of the punishable acts enumerated in Section 4(c)(3) shall be punished with imprisonment of *arresto mayor* or a fine of at least Fifty thousand pesos (PhP50,000.00) but not exceeding Two hundred fifty thousand pesos (PhP250,000.00) or both.

Any person found guilty of any of the punishable acts enumerated in Section 5 shall be punished with imprisonment one (1) degree lower than that of the prescribed penalty for the offense or a fine of at least One hundred thousand pesos (PhP100,000.00) but not exceeding Five hundred thousand pesos (PhP500,000.00) or both.

Section 9. Corporate Liability

Liability shall based on:

- A power of representation of the juridical person;
- An authority to take decisions on behalf of the juridical person; or
- An authority to exercise control within the juridical person.

Juridical Person and natural person acting under the authority of the juridical person is liable for a fine equivalent to at least DOUBLE THE FINES imposable in Section 7

The chairperson of the board of directors, the president, the general manager of the corporation, the general partners of a partnership, and the officers and employees directly responsible shall be JOINTLY AND SEVERALLY LIABLE with the firm for the fine imposed therein.

For foreign corporations, the person or persons directly responsible for the management and operation thereof shall be liable.

Section 10. Enforcement and Implementation

- Law Enforcement Agencies: PNP and NBI



Section 12. Real-Time Collection of Traffic Data

Law enforcement authorities, with due cause, shall be authorized to collect or record by technical or electronic means traffic data in real-time associated with specified communications transmitted by means of a computer system.

LIMITATION: Traffic data refer only to the communication's origin, destination, route, time, date, size, duration, or type of underlying service, but not content, nor identities

When Court Warrant Could Be Issued

upon written application and the examination under oath or affirmation of the applicant and the witnesses he may produce and the showing:

- that there are reasonable grounds to believe that any of the crimes enumerated hereinabove has been committed, or is being committed, or is about to be committed.
- that there are reasonable grounds to believe that evidence that will be obtained is essential to the conviction of any person for, or to the solution of, or to the prevention of, any such crimes; and
- that there are no other means readily available for
- obtaining such evidence.

Custody of Data

Preservation of Computer Data: maximum of 90 days and furnishing of transmittal document shall be deemed a notification to preserve the data until the termination of the case

Disclosure of Computer Data. – within 72 hours from receipt of the order

Search and Seizure: Within the time period specified in the warrant, to conduct interception but may request for an extension no longer than thirty (30) days from date of expiration of the warrant.

Custody of Data: within forty-eight (48) hours after the expiration of the period fixed therein, be deposited with the court in a sealed package

Destruction of Data - Upon expiration of the periods as provided in Sections 10 and 12

Jurisdiction

- The Regional Trial Court if committed within the Philippines or committed with the use of any computer system wholly or partly situated in the country.



Central Authority

- **Section 19.** *Restricting or Blocking Access to Computer Data.*
 - – When a computer data is prima facie found to be in violation of the provisions of this Act, the DOJ shall issue an **order to restrict or block access to such computer data.**



- The Department of Justice (DOJ) shall be responsible for extending immediate assistance to investigations or proceedings.

SEC. 18. Cybercrime Investigation and Coordinating Center

- There is hereby created, within thirty (30) days from the effectivity of this Act, an inter-agency body to be known as the Cybercrime Investigation and Coordinating Center (CICC), under the administrative supervision of the Office of the President

Cybercrime Prevention



www.affordablecebu.com

SEC. 29. Repealing Clause

- All laws, decrees or rules inconsistent with this Act are hereby repealed or modified accordingly. Specifically, Section 33(a) on Penalties of Republic Act No. 8792 or the "Electronic Commerce Act", is hereby modified accordingly.

Who caused the insertion of the libel

C
l
a
u
s
e

On January 24, 2012, while the nation was riveted on the impeachment trial of then Chief Justice Renato Corona, Sotto introduced an amendment to the proposed Cyber Crime Law.



SOTTO AMEND

Preliminarily, S are numerous abus the video and pho write-ups and cor systems. He read th vs. *Court of Appe* 1999), to wit:

...a public and ma of a vice or defec omission, condi tending to discre contempt of a na blacken the me Thus, the elemen of a discredita

(h) publication of the imputation; (e) identity of the person defamed; and, (d) existence of malice.

and the ruling in *Lacsa Court* (161 SCRA 427)

duce suspicion are o destroy reputation made. Ironical and favored vehicle for ent if the words are rers to suppose and or persons against ere guilty of certain to impeach their on, or to hold the blic ridicule.

**SOTTO: NO PLAGIARISM IN MY SPEECH
I ALWAYS CITE MY SOURCE**

Sotto said introducing internet libel would make people more cautious on the Net.

Further, Senator Sotto observed that the publication requirement in the crime of libel can be achieved by the mere fact that it is seen in cyberspace and this can further promote the habit of "think before you click." It is clear, he noted, that cybercrimes are not covered under Article 355 of Revised Penal Code.

On page 6, line 37, as proposed by Senator Sotto and accepted by the Sponsor, there being no objection, the Body approved the insertion of a new paragraph, to wit:

4. ***LIBEL*** – THE UNLAWFUL OR PROHIBITED ACTS OF LIBEL AS DEFINED IN ARTICLE 355 OF THE REVISED PENAL CODE COMMITTED THROUGH A COMPUTER SYSTEM OR ANY OTHER SIMILAR MEANS WHICH MAY BE DEvised IN THE FUTURE.



FROM DOWNTOWN!

HE'S ON FIRE!

TRO RESOLUTION

GIVEN by the Supreme Court of the Philippines, this 9th day of October 2012

NOW, THEREFORE, effective immediately and for a period of one hundred twenty (120) days, You, Respondents, your agents, representatives, or persons acting in your place or stead, are hereby ENJOINED from implementing and/ or enforcing Republic Act No. 10175 (Cybercrime Prevention Act of 2012).

What then happened?

- On 5 February 2013, The Supreme Court extended the temporary restraining order on the law, "until further orders from the court."

RIGHTS ALLEGEDLY VIOLATED

FREEDOM OF
EXPRESSION

FREEDOM OF
PRESS

DUE PROCESS

EQUAL
PROTECTION

PRIVACY OF
COMMUNICATION

Sections that are violative of our constitutional rights

Sec 4c4 –reclassifying
libel as cybercrime

Sec 6 –increase
punishment

Sec 7 –double
jeopardy

Sec 12 –warrantless
search

Sec 19 –restriction to
content mandated by
DOJ to service
providers without
judicial determination

Assuming that the TRO lapse

- Can the one who "Shares" or "Likes" on Facebook or re-tweets on Twitter the offending piece now be held liable for libel?
- Can someone who posts a comment agreeing with the alleged libelous material also be sued?

Assuming that the TRO lapse

- In traditional media – newspapers, TV and radio networks – the origin of the libelous material is easy to identify. On the Web, can someone suing for libel obtain a court order to compel an ISP (Internet Service Provider) or Facebook or Twitter to divulge the identity of the one who posted the alleged libel?
- Can these entities also be held liable since they carried the offending material the way newspapers carry a libelous story?

Assuming that the TRO lapse

- As a blogger, I believe in giving a wide democratic space to commenters, including those who criticize me.
- Can I now be sued for any comment that appears on my site? Besides, libel is in the eyes of the offended.

Assuming that the TRO lapse

- Can someone living in Metro Manila file a case of internet libel in Zamboanga City on the pretext that the complainant was surfing in an Internet Cafe in Zamboanga City when he saw the offending piece?

Assuming that the TRO lapse

- If someone pretends to be me online and issues allegedly libelous material; or if someone hacks into my computer, obtains files and posts them online,
- can I be sued for libel? How do I defend myself on this?

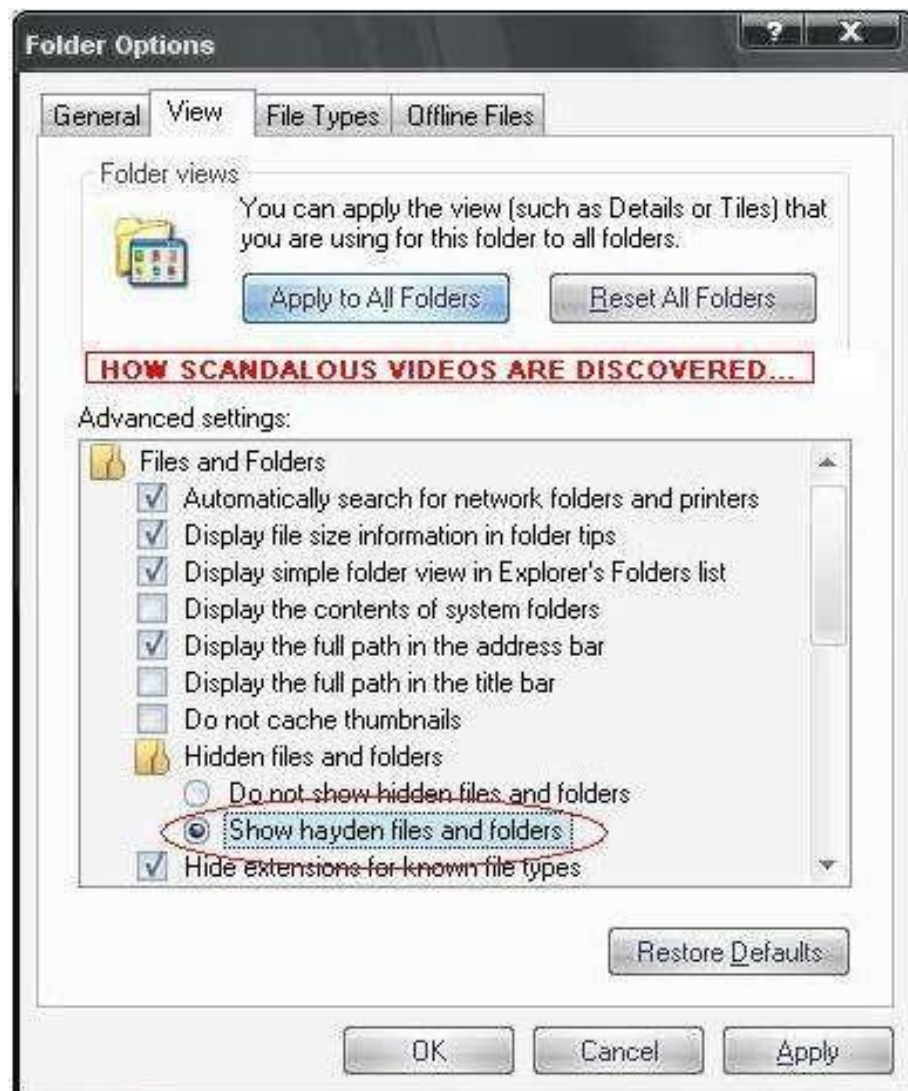
Assuming that the TRO lapse

- What kind of evidence would the court accept on internet libel cases?
- Would screencaps suffice?
- How will the court determine if an offensive image has been manipulated?
- Or an offending piece was really posted by the person being sued?

Assuming that the TRO lapse

- How is malice proven online? What should ordinary people online guard against so that they are not accused of malice?
- I'm fairly sure there are other issues and complications which will emerge.

The answer lies upon the interpretation of the Court



DATA PRIVACY IN THE PHILIPPINES

Republic Act 10173

DISCUSSION:

Data Privacy Act

Freedom of Information

Commission on Appointments

THE DATA PRIVACY ACT

REPUBLIC ACT
10173
DATA PRIVACY
ACT OF 2012 (DPA)

" 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"

RESPONSIBLE AGENCY:



REPUBLIC OF THE PHILIPPINES
DEPARTMENT OF INFORMATION AND
COMMUNICATIONS TECHNOLOGY



**NATIONAL
PRIVACY
COMMISSION**

*Country's privacy
watchdog*

BACKGROUND

The Philippines has a growing and important business process management and health information technology industry.

Total IT spending reached \$4.4 billion in 2016, and expected to more than double by 2020.

The country is also in the process of enabling free public Wi-Fi.

rapid growth of the digital economy and increasing international trade of data

Filipinos are heavy social media users 67M internet users – world's #1 in terms of social media usage (Digital 2018 by Hootsuite, and We Are Social Ltd.)

Facebook users – 30M in 2013 to 67M in 2017

Source: <https://iapp.org/news/a/summary-philippines-data-protection-act-and-implementing-regulations/>

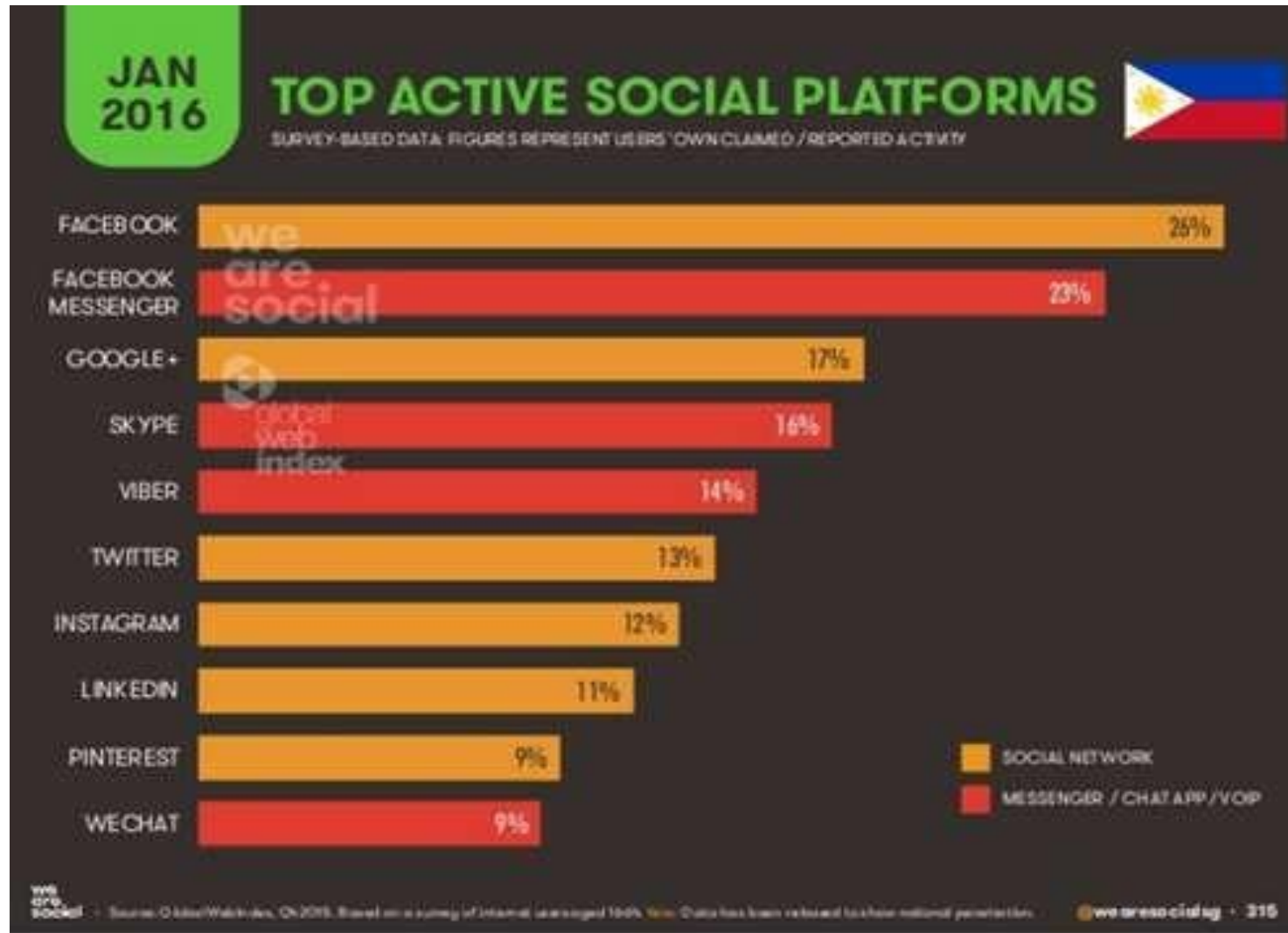
DIGITAL ENGAGEMENT IN 2016



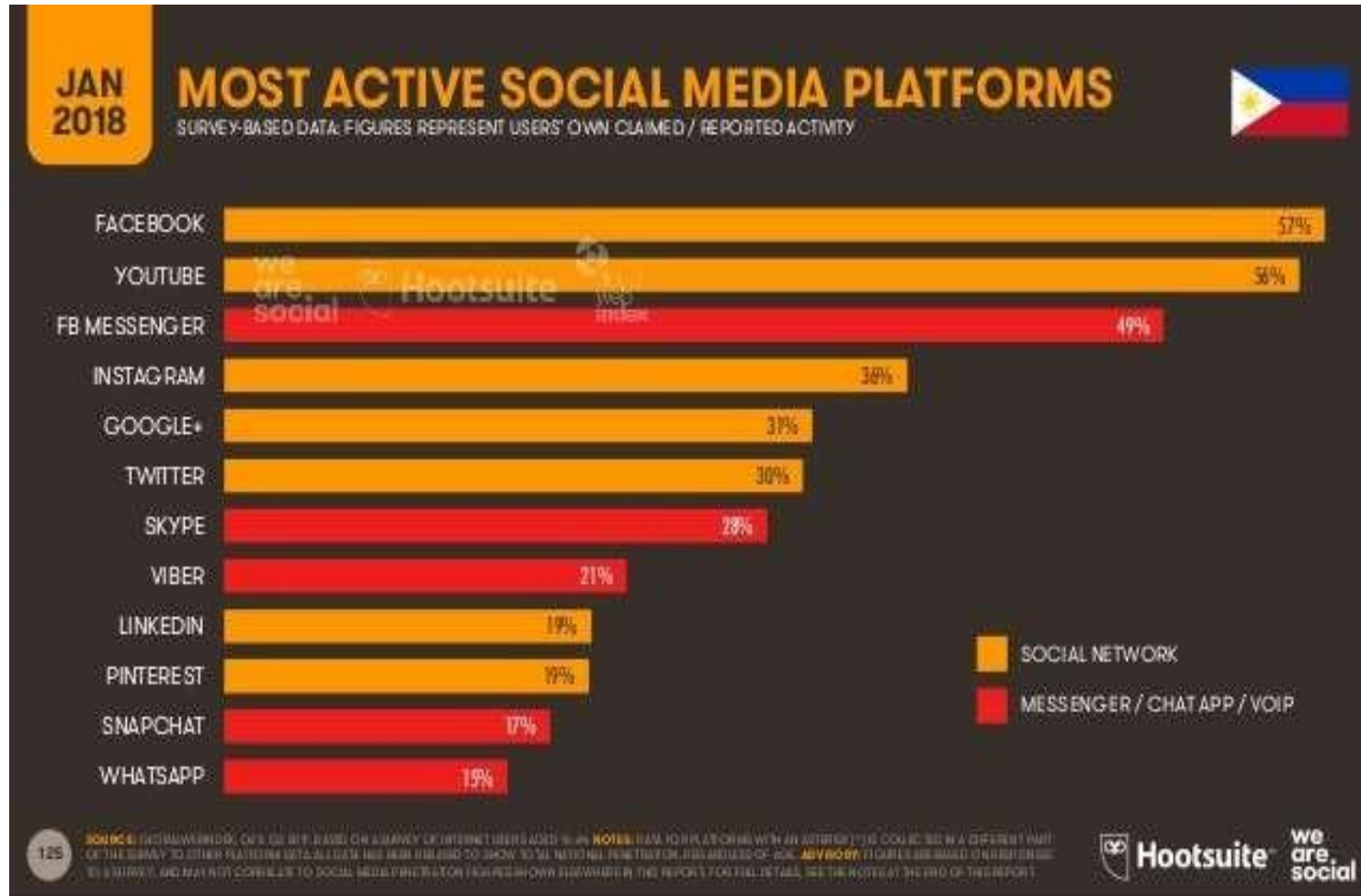
AN INCREASE OF ABOUT 20% IN 2018



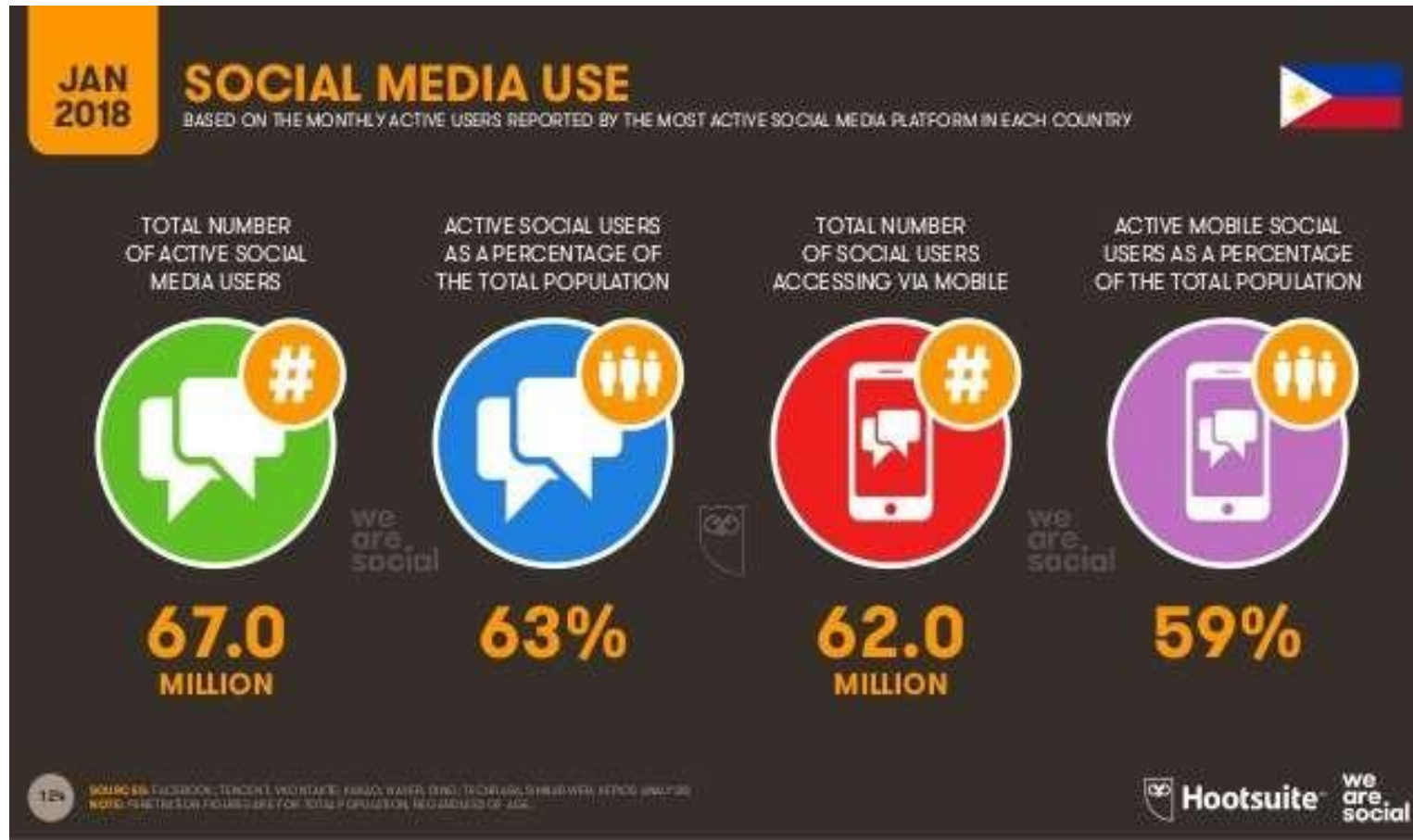
SOCIAL MEDIA ENGAGEMENT IN 2016



SOCIAL MEDIA ENGAGEMENT DOUBLES IN 2018



SOCIAL MEDIA USAGE IN 2018



THE JOURNEY OF THE DPA

European Union's 1995 Data Protection Directive

Electronic Commerce Act of 2000 (R.A. No. 8792) – recognition and use of electronic commercial and non-commercial transactions and documents membership in the Asia-Pacific Economic Cooperation (APEC) -- Privacy Framework in 2005

DTI Administrative Order No. 8 in 2006 -- which prescribed guidelines for a local data protection certification system

The DPA was signed into law in 2012, with the local BPO sector as its most visible endorser

Creation of the Dept. of Information and Communications Technology (DITC) in 2015 (R.A. No. 10844)

The activation of the National Privacy Commission (NPC) in 2016

DPA's Implementing Rules and Regulations was put in effect on September 9, 2016

PROVISION OF THE DPA

Chapter I – General Provisions

Chapter II – The National Privacy Commission

Chapter III – Processing of Personal Information

Chapter IV – Rights of the Data Subject

Chapter V – Security of Personal Information

Chapter VI – Accountability for Transfer of Personal Information

Chapter VII – Security of Sensitive Personal Information in Government

Chapter VIII – Penalties

Chapter IX – Miscellaneous Provisions

Source: <https://privacy.gov.ph/data-privacy-act/>

SCOPE

- SEC. 4. *Scope.* – This Act applies to the processing of all types of personal information and to any natural and juridical person involved in personal information processing including those personal information controllers and processors who, although not found or established in the Philippines, use equipment that are located in the Philippines, or those who maintain an office, branch or agency in the Philippines ...

SCOPE

This Act does not apply to the following:

- (a) Information about any individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual, including:

(1) The fact that the individual is or was an officer or employee of the government institution;

(2) The title, business address and office telephone number of the individual;

(3) The classification, salary range and responsibilities of the position held by the individual; and

(4) The name of the individual on a document prepared by the individual in the course of employment with the government;

SCOPE

(b) Information about an individual who is or was performing service under contract for a government institution that relates to the services performed, including the terms of the contract, and the name of the individual given in the course of the performance of those services;

(c) Information relating to any discretionary benefit of a financial nature such as the granting of a license or permit given by the government to an individual, including the name of the individual and the exact nature of the benefit;

(d) Personal information processed for journalistic, artistic, literary or research purposes;

SCOPE

(e) Information necessary in order to carry out the functions of public authority which includes the processing of personal data for the performance by the independent, central monetary authority and law enforcement and regulatory agencies of their constitutionally and statutorily mandated functions.

(f) Information necessary for banks and other financial institutions under the jurisdiction of the independent, central monetary authority or Bangko Sentral ng Pilipinas to comply with Republic Act No. 9510, and Republic Act No. 9160, as amended, otherwise known as the Anti-Money Laundering Act and other applicable laws; and

(g) Personal information originally collected from residents of foreign jurisdictions in accordance with the laws of those foreign jurisdictions, including any applicable data privacy laws, which is being processed in the Philippines.

APPROACH OF THE GOVERNMENT

- The processing of personal data shall be allowed subject to adherence to the principles of:



transparency

legitimate
purpose

proportionality

DATA PROCESSING AND CONSENT

- Collection of personal data must be:



Declared

Specified

Legitimate
purpose

DATA PROCESSING AND CONSENT

Consent is required prior to the collection of *all* personal data.

the data subject must be informed about the extent and purpose of processing

for the "automated processing of his or her personal data for profiling, or processing for direct marketing, and data sharing"

for sharing information with affiliates or even mother companies

must be "freely given, specific, informed," and must be evidenced by recorded means

DATA PROCESSING AND CONSENT

Consent is not required for processing where the data subject is party to a contractual agreement, for purposes of fulfilling that contract.

- for protection of the vital interests of the data subject
- to response to a national emergency
- for the legitimate interests of the data controller

AGREEMENT

“The law requires that when sharing data, the sharing be covered by an agreement that provides adequate safeguards for the rights of data subjects, and that these agreements are subject to review by the National Privacy Commission”

SENSITIVE PERSONAL INFORMATION

The law defines sensitive personal information as being:

- About an individual's race, ethnic origin, marital status, age, color, and religious, philosophical or political affiliations;
- About an individual's health, education, genetic or sexual life of a person, or to any proceeding or any offense committed or alleged to have committed;
- Issued by government agencies "peculiar" (unique) to an individual, such as social security number;
- Marked as classified by executive order or act of Congress.

SENSITIVE PERSONAL INFORMATION

All processing of sensitive and personal information is prohibited except in certain circumstances.

- Consent of the data subject;
- Pursuant to law that does not require consent;
- Necessity to protect life and health of a person;
- Necessity for medical treatment;
- Necessity to protect the lawful rights of data subjects in court proceedings, legal proceedings, or regulation.

PENALTIES

- Ranging from P100,000 to P5,000,000 (approximately US\$2,000 to US\$100,000)
- Imprisonment of 1 year up to 6 years

Unauthorized Processing of Personal Information and Sensitive Personal Information

Accessing Personal Information and Sensitive Personal Information Due to Negligence.

Improper Disposal of Personal Information and Sensitive Personal Information

Processing of Personal Information and Sensitive Personal Information for Unauthorized Purposes

Unauthorized Access or Intentional Breach.

Concealment of Security Breaches Involving Sensitive Personal Information.

Malicious Disclosure.

Unauthorized Disclosure

WHO NEEDS TO REGISTER?

Companies with at least 250 employees or access to the personal and identifiable information of at

least 1,000 people are required to register with the National Privacy Commission and comply with the Data Privacy Act of 2012

COMPLIANCE OF THE DATA PRIVACY ACT

The National Privacy Commission, which was created to enforce RA 10173, will check whether companies are compliant based on a company having 5 elements:


- Appointing a Data Protection Officer
- Conducting a privacy impact assessment
- Creating a privacy knowledge management program
- Implementing a privacy and data protection policy
- Exercising a breach reporting procedure

FREEDOM OF INFORMATION ORDER

EXECUTIVE ORDER NO. 2 SERIES OF 2016

FREEDOM OF INFORMATION ORDER

"Operationalizing in the Executive branch the people's constitutional right to information and the state policies to full public disclosure and

- transparency in the public service and providing guidelines therefor"
-  The Freedom of Information Order provides for full public disclosure of all government records involving public interest and upholds the constitutional right of people to information on matters of public concern

SECTION 1. DEFINITION. FOR THE PURPOSE OF THIS EXECUTIVE ORDER, THE FOLLOWING TERMS SHALL MEAN:

(a) "Information" shall mean any records, documents, papers, reports, letters, contracts, minutes and transcripts of official meetings, maps, books, photographs, data, research materials, films, sound and video recording, magnetic or other tapes, electronic data, computer stored data, any other like or similar data or materials recorded, stored or archived in whatever format, whether offline or online, which are made, received, or kept in or under the control and custody of any government office pursuant to law, executive order, and rules and regulations or in connection with the performance or transaction of official business by any government office.

SECTION 1. DEFINITION. FOR THE PURPOSE OF THIS EXECUTIVE ORDER, THE FOLLOWING TERMS SHALL MEAN:

(b) "Official record/records" shall refer to information produced or received by a public officer or employee, or by a government office in an official capacity or pursuant to a public function or duty.

(c) "Public record/records" shall include information required by laws, executive orders, rules, or regulations to be entered, kept and made publicly available by a government office.

FREEDOM OF INFORMATION ORDER

Protects Data Privacy

.....

WHEREAS, the Data Privacy Act of 2012 (R.A. 10173), including its implementing Rules and Regulations, strengthens the fundamental human right of privacy, and of communication while ensuring the free flow of information to promote innovation and growth

E-COMMERCE LAW IN THE PHILIPPINES

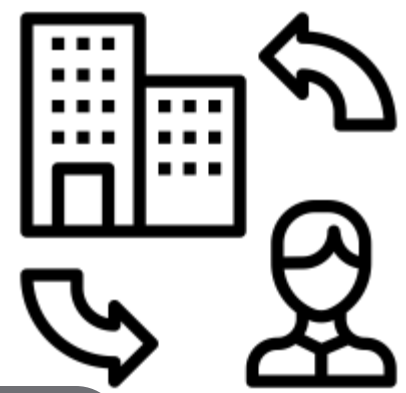


What's E-Commerce?

❖ E-commerce(electronic commerce)
refers to business over the Internet.



Business-to-Consumer (B2C)

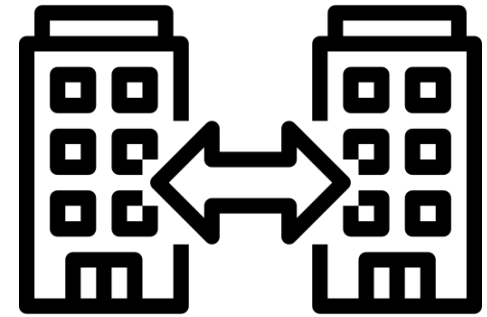


business transactions between companies, business-to-consumer models are those that sell products or services directly to personal-use customers

connects, communicates and conducts business transactions with consumers most often via the Internet

larger than just online retailing; it includes online banking, travel services, online auctions, and health and real estate sites.

Business-to-Business (B2B)



A type of commerce transaction that exists between businesses, such as those involving a manufacturer and wholesaler, or a wholesaler and a retailer

conducted between companies, rather than between a company and individual consumers

REPUBLIC ACT NO. 8792 OF PHILIPPINES ELECTRONIC COMMERCE ACT OF 2000

by the Senate and House of
Representatives of the Republic of the
Philippines

- ❖ An act providing for the recognition and use of electronic commercial and non-commercial transactions and documents, penalties for unlawful use thereof and for other purposes .

Definition in General

Electronic Commerce

- is defined as the process of buying and selling goods electronically by consumers and from company to company through computerized business transactions. The Organization for Electronic Cooperation and Development defines it as commercial transactions based on electronic transmission of data over communication networks such as the Internet. Although the definition of electronic commerce is strictly confined to commercial undertakings, RA8792 is made applicable both

Objectives

provide a secure legal framework and environment for electronic commerce.

protect the integrity of electronic documents and electronic signature as well as its transmission and communication so as to build and ensure the trust and reliance of the public on electronic transactions

Definition of Terms

a. "Addressee"

- a person who is intended by the originator to receive the electronic data message or electronic document.

b. "Computer"

- any device or apparatus which, by electronic, electro-mechanical or magnetic impulse, or by other means is capable of receiving, recording, transmitting, storing, processing, retrieving or producing information, data, figures, symbols or other modes of written expression according to mathematical and logical rules or of performing any one or more of those functions

c. "Electronic Data Message"

- information generated, sent, received or stored by electronic, optical or similar means.

(d) "Information and Communications System"

- refers to a system intended for and capable of generating, sending, receiving, storing, or otherwise processing electronic data messages or electronic documents and includes the computer system or other similar device by or in which data is recorded or stored and any procedures related to the recording or storage of electronic data message or electronic document.

(e) "Electronic Signature"

- refers to any distinctive mark, characteristic and/or sound in electronic form, representing the identity of a person and attached to or logically associated with the electronic data message or electronic document or any methodology or procedures employed or adopted by a person and executed or adopted by such person with the intention of authenticating or approving an electronic data message or electronic document.

(f) "Electronic Document"

- refers to information or the representation of information, data, figures, symbols or other modes of written expression, described or however represented, by which a right is established or an obligation extinguished, or by which a fact may be prove and affirmed, which is receive, recorded, transmitted, stored, processed, retrieved or produced electronically.

(g) "Electronic Key"

- refers to a secret code which secures and defends sensitive information that cross over public channels into a form decipherable only with a matching electronic key.

(h) "Intermediary"

- refers to a person who in behalf of another person and with respect to a particular electronic document sends, receives and/or stores provides other services in respect of that electronic data message or electronic document.

(i) "Originator"

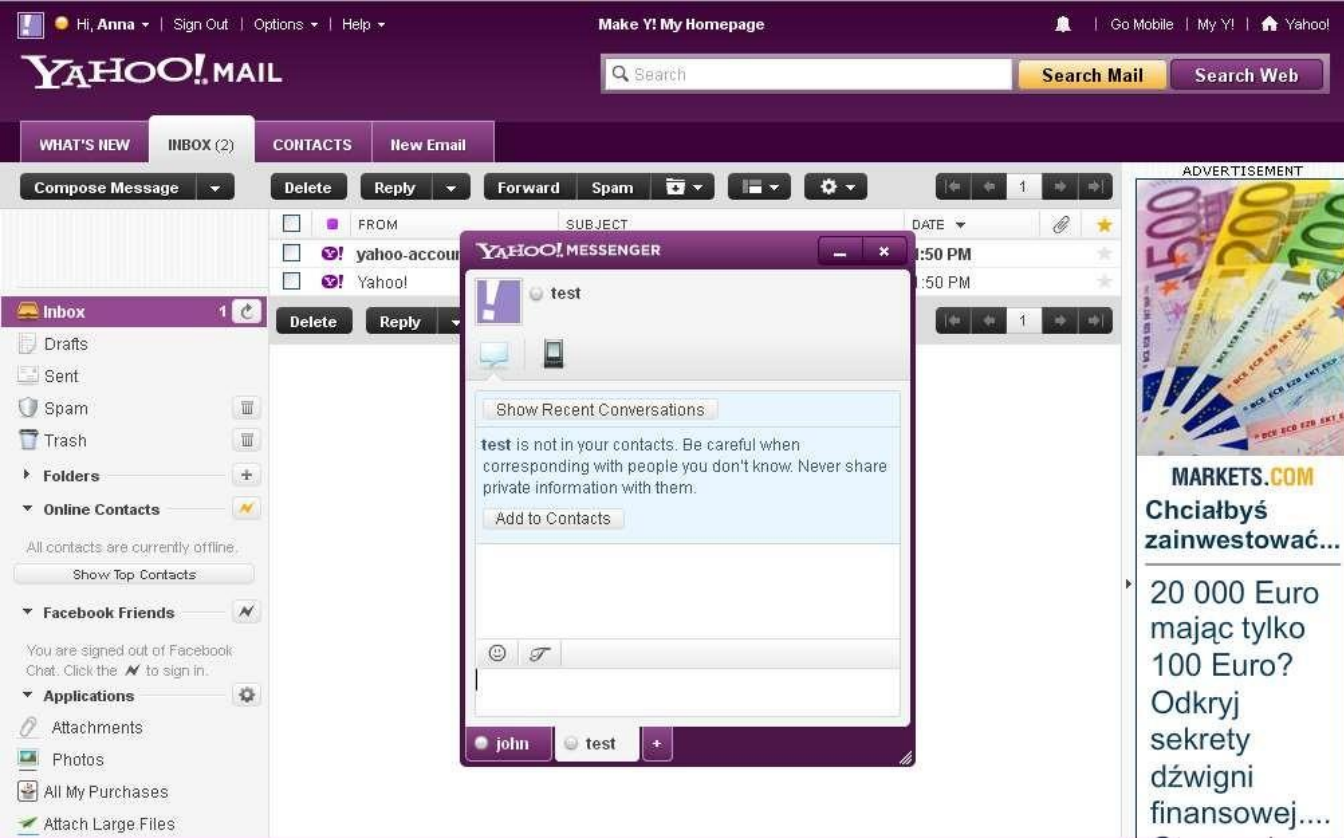
- refers to a person by whom, or on whose behalf, the electronic document purports to have been created, generated and/or sent. The term does not include a person acting as an intermediary with respect to that electronic document.

(j) "Service provider"

- refers to a provider of
 - i. On-line services or network access or the operator of facilities therefor, including entities offering the transmission, routing, or providing of connections for online communications, digital or otherwise, between or among points specified by a user, of electronic documents of the user's choosing; or
 - ii. The necessary technical means by which electronic documents of an originator may be stored and made accessible to designated or undesignated third party.

Such service providers shall have no authority to modify or alter the content of the electronic data message or electronic document received or to make any entry therein on behalf of the originator, addressee or any third party unless specifically authorized to do so, and who shall retain the electronic document in accordance with the specific request or as necessary for the purpose of performing the services it was engaged to perform.

Salient Features of Republic Act 8792



1. It gives legal recognition of electronic data messages, electronic documents, and electronic signatures.
(section 6 to 13)

Sec. 6. Legal Recognition of Data Messages.

Section 7. Legal Recognition of Electronic documents

Section 8. Legal Recognition of Electronic Signatures

Section 9. Presumption Relating to Electronic Signatures

Section 10. Original Documents.

Section 11. Authentication of Electronic Data Messages and Electronic Documents

Section 12. Admissibility and Evidential Weight of Electronic Data Message or electronic document.

SEC. 13. Retention of Electronic Data Message and Electronic Document.



2. Allows the formation of contracts in electronic form. (section 16)



SEC. 16. Formation and Validity of Electronic Contracts.

3. Makes banking transactions done through ATM switching networks absolute once consummated. (section 16)



4. Parties are given the right to choose the type and level of security methods that suit their needs.
(section 24)

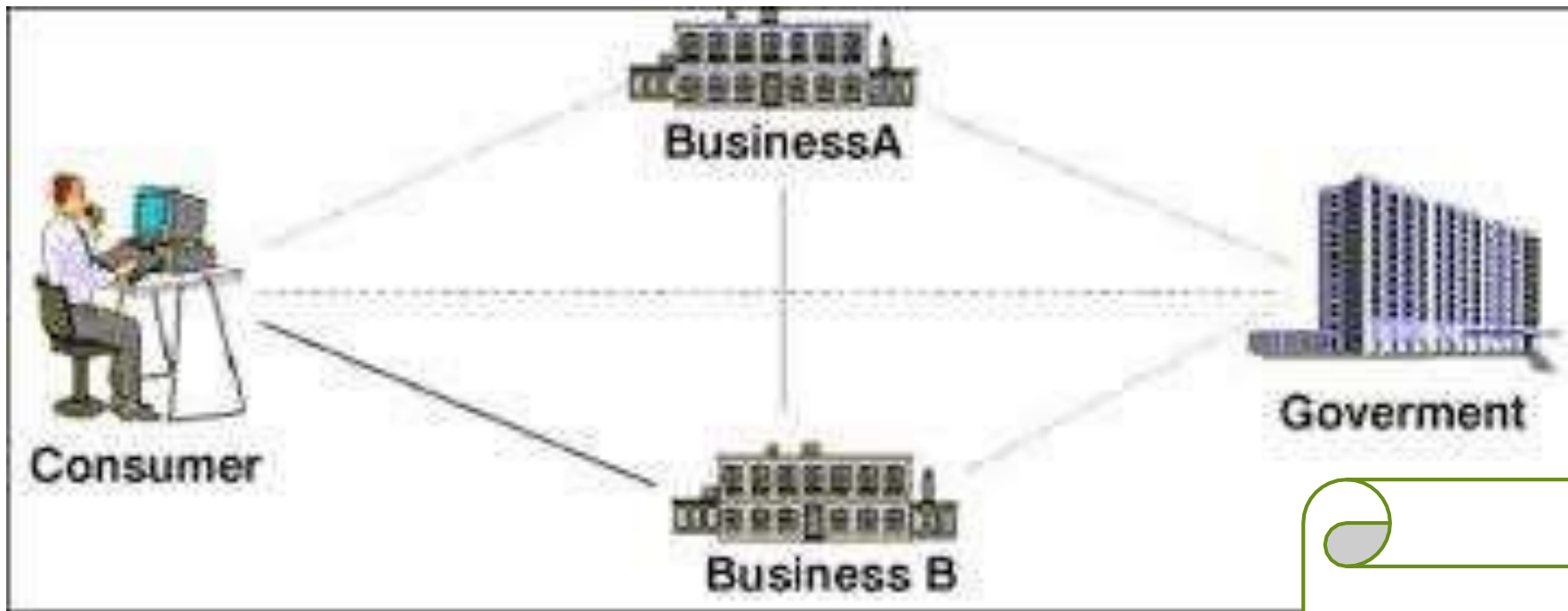
SEC. 24. Choice of Security Methods.



SEC. 25. Actions Related to Contracts of Carriage of Goods.

SEC. 26. Transport Documents.

5. Provides the mandate for the electronic implementation of transport documents to facilitate carriage of goods. This includes documents such as, but not limited to, multi-modal, airport, road, rail, inland waterway, courier, post receipts, transport documents issued by freight forwarders, marine/ocean bill of lading, non-negotiable seaway bill, charter party bill of lading. (section 25 and 26)



SEC. 27. Government Use of Electronic Data Messages, Electronic Documents and Electronic Signatures.

6. Mandates the government to have the capability to do e-commerce within 2 years or before June 19, 2002.
(section 27)



SEC. 28. RPWEB To Promote the Use Of Electronic Documents and Electronic Data Messages In Government and to the General Public.

7. Mandates RPWeb to be implemented. RPWeb is a strategy that intends to connect all government offices to the Internet and provide universal access to the general public. The Department of Transportation and Communications, National Telecommunications Commission, and National Computer Center will come up with policies and rules that shall lead to substantial reduction of costs of telecommunication and Internet facilities to ensure the implementation of RPWeb. (section 28)



8. Made cable, broadcast, and wireless physical infrastructure within the activity of telecommunications. (section 28)

SEC. 28. RPWEB To Promote the Use Of Electronic Documents and Electronic Data

Messages In Government and to



9. Empowers the Department of Trade and Industry to supervise the development of e-commerce in the country. It can also come up with policies and regulations, when needed, to facilitate the growth of e-commerce. (section 29)

SEC. 29. Authority of the Department of Trade and Industry and Participating Entities.



10. Provided guidelines as to when a service provider can be liable.
(section 30)

SEC. 30. Extent of Liability of a Service Provider.



SEC. 31. Lawful
Access.

SEC. 32. Obligation of
Confidentiality.

11. Authorities and parties with the legal right can only gain access to electronic documents, electronic data messages, and electronic signatures. For confidentiality purposes, it shall not share or convey to any other person.
(section 31 and 32)



**China's alleged claim on maritime territories
and oppressive poaching can no longer be tolerated.**

**Stand against Oppression!
It's time to fight back!**

Say NO to China's Bullying!

12. Hacking or cracking, refers to unauthorized access including the introduction of computer viruses, is punishable by a fine from 100 thousand to maximum commensurating to the damage. With imprisonment from 6 months to 3 years. (section 33)

SEC. 33.
Penalties.

Cybercrime Penalties under Electronic Commerce Act (Republic Act 8792)

HACKING OR CRACKING



UNAUTHORIZED ACCESS INTO OR INTERFERENCE IN A COMPUTER SYSTEM, SERVER OR INFORMATION AND COMMUNICATION SYSTEM; OR ANY ACCESS IN ORDER TO CORRUPT, ALTER, STEAL, OR DESTROY USING A COMPUTER OR OTHER SIMILAR INFORMATION AND COMMUNICATION DEVICES, WITHOUT THE KNOWLEDGE AND CONSENT OF THE OWNER OF THE COMPUTER OR INFORMATION AND COMMUNICATIONS SYSTEM, INCLUDING THE INTRODUCTION OF COMPUTER VIRUSES AND THE LIKE, RESULTING IN THE CORRUPTION, DESTRUCTION, ALTERATION, THEFT OR LOSS OF ELECTRONIC DATA, MESSAGES OR ELECTRONIC DOCUMENT

PENALTIES

PUNISHED BY A MINIMUM FINE OF ONE HUNDRED THOUSAND PESOS (P100,000.00) AND A MAXIMUM COMMENSURATE TO THE DAMAGE INCURRED AND A MANDATORY IMPRISONMENT OF SIX (6) MONTHS TO THREE (3) YEARS

CONSUMER ACT AND ALL OTHER LAWS



REPUBLIC ACT NO. 7394 AND OTHER RELEVANT OR PERTINENT LAWS THROUGH TRANSACTIONS COVERED BY OR USING ELECTRONIC DATA MESSAGES OR ELECTRONIC DOCUMENTS

PENALTIES

PENALIZED WITH THE SAME PENALTIES AS PROVIDED IN THOSE LAWS

PIRACY



THE UNAUTHORIZED COPYING, REPRODUCTION, DISSEMINATION, DISTRIBUTION, IMPORTATION, USE, REMOVAL, ALTERATION, SUBSTITUTION, MODIFICATION, STORAGE, UPLOADING, DOWNLOADING, COMMUNICATION, MAKING AVAILABLE TO THE PUBLIC, OR BROADCASTING OF PROTECTED MATERIAL, ELECTRONIC SIGNATURE OR COPYRIGHTED WORKS INCLUDING LEGALLY PROTECTED SOUND RECORDINGS OR PHONOGRAMS OR INFORMATION MATERIAL ON PROTECTED WORKS, THROUGH THE USE OF TELECOMMUNICATION NETWORKS

PENALTIES

MINIMUM FINE OF ONE HUNDRED THOUSAND PESOS (P100,000.00) AND A MAXIMUM COMMENSURATE TO THE DAMAGE INCURRED AND A MANDATORY IMPRISONMENT OF SIX (6) MONTHS TO THREE (3) YEARS

OTHER VIOLATIONS IN E-COMMERCE LAW



OTHER VIOLATIONS OF THE PROVISIONS OF THIS ACT

EX: OBLIGATION OF CONFIDENTIALITY, LAWFUL ACCESS, AMONG OTHERS

PENALTIES

MAXIMUM PENALTY OF ONE MILLION PESOS (P1,000,000.00) OR SIX (6) YEARS IMPRISONMENT

13. Piracy through the use of telecommunication networks, such as the Internet, that infringes intellectual property rights is punishable. The penalties are the same as hacking. (section 33)

SEC. 33. Penalties.

The image shows the front cover of a book titled 'CONSUMER ACT OF THE PHILIPPINES'. The cover has a green background with a white rectangular area in the center containing the title in bold, black, sans-serif capital letters. Above the title, there is a dark brown rectangular area. The book is slightly angled to the right.

CONSUMER ACT OF THE PHILIPPINES

14. All existing laws such as the Consumer Act of the Philippines also applies to e-commerce transactions. (section 33

SEC. 33.
Penalties.



Innovation and Technology
Support Office

Intellectual Property in IT Systems

By

Dylan Josh Lopez,
MSc., RDPM

July 6, 2021



Welcome to today's webinar!

Topics for Today

- 01 Breaking down the IP of IT
- 02 Copyrights
- 03 Patents / Utility Models / Industrial Designs
- 04 Open Source: Copyleft and Creative Commons



Ownership

An effective intellectual and industrial property system is vital to the development of domestic and creative activity, facilitates transfer of technology, attracts foreign investments, and ensures market access for our products.

Intellectual Property Code of the Philippines
RA 8293



Intellectual Property

The creation or product of human mind





Part 1: Breaking Down the IP of IT

import intellectual_property as ip



The Common IP Protection

IP == Intellectual Property
IP != Internet Protocol



The Common IP Protection

Legal rights	Assets	Procedures
Copyright	Original creative or artistic forms	Exists automatically, registration
Trademarks	Distinctive identification of products or services	use and/or registration
Patents	inventions	Application and examination
Trade Secrets	valuable information not known to the public	Reasonable efforts to keep safe
Industrial Design	External Appearance	Registration



For IP in IPs

Patent

Copyright

Industrial
Design

Trademark

Trade
Secret





Part 2: Copyright

isLifetime = True



Copyright

Copyright (or author's right) is a legal term used to describe the rights that creators have over their literary and artistic works. Works covered by copyright range from books, music, paintings, sculpture, and films, to computer programs, databases, advertisements, maps, and technical drawings.

World Intellectual Property Organization



Copyright

Copyright protection extends only to expressions, and not to ideas, procedures, methods of operation or mathematical concepts as such.

Copyright may or may not be available for a number of objects such as titles, slogans, or logos, depending on whether they contain sufficient authorship.

World Intellectual Property Organization



Term of Protection

Exists upon creation

Territorial and national

Lifetime + 50 years (70 years in other countries)

Rights



Economic Rights

Moral Rights



Right to attribution

Right to integrity



Related Rights



Right to make adaptations and arrangements



Right to make reproductions



Right to translate

Related Rights



Right to perform in public



Right to recite literary works in public



Right to broadcast



Right to use the work as a basis for an audiovisual work



Fair Use

Personal or private use

Proper citation or quotation

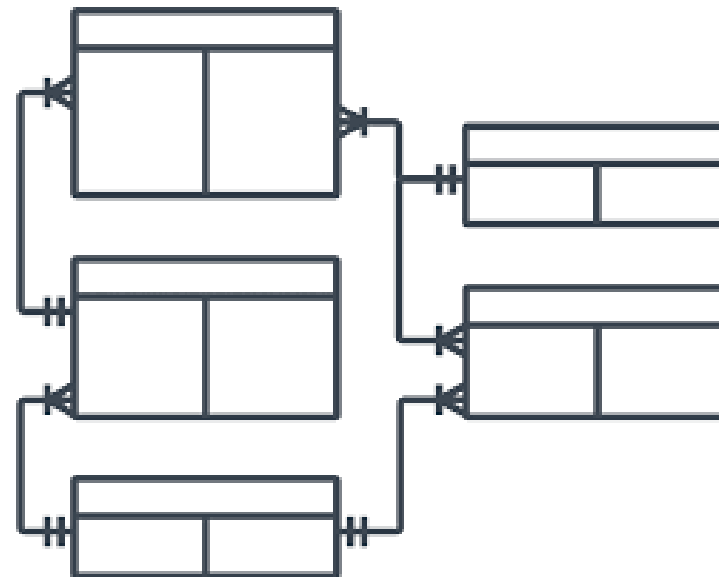
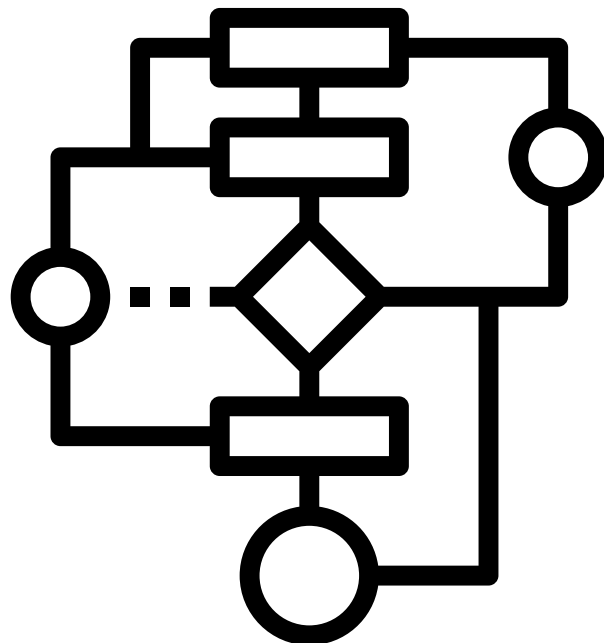
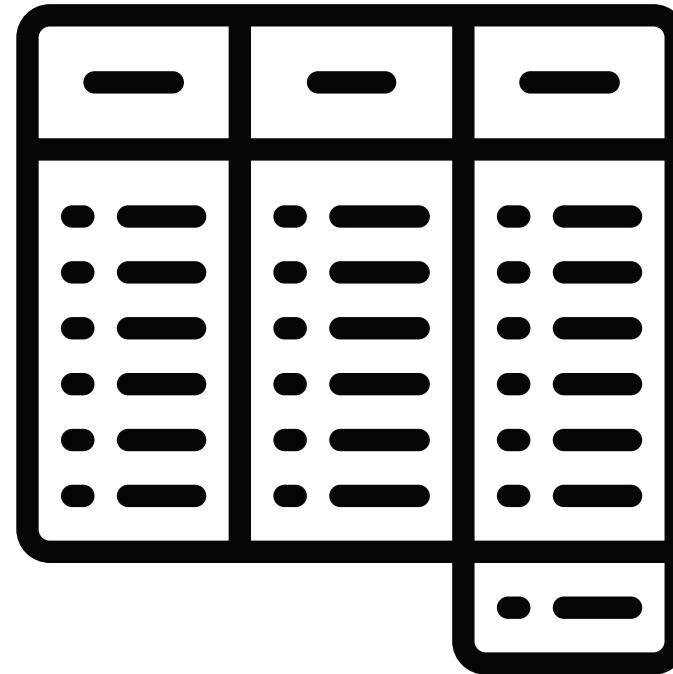
Length compatible with fair practice

Existence in the public domain



IsCopyrightTables

```
CREATE PROCEDURE uspCopyrights
AS
BEGIN
    SELECT * FROM IPs
    ORDER BY creation_date;
END;
```



$$f(x)$$





Part 4: Patents / Utility Models/ Industrial Designs

Industrial protection



Patents

A patent is an **exclusive right** granted for an invention, which is a product or a process that provides, in general, a **new way of doing something**, or offers a **new technical solution** to a problem.



Patents

Patents are **legal instruments** intended to **encourage innovation** by providing a **limited monopoly** to the inventor (or their assignee) in return for the **disclosure** of the invention.



Patentability

Novelty

Is the solution new?

Inventive Step

Is the solution obvious?

Industrial Applicability

Is the solution usable and reproducible?



Non-Patentability

- Discoveries
- Scientific theories
- Mathematical methods
- Schemes, rules and methods of -performing mental acts
 - playing games
 - doing business
 - programs for computers
- Aesthetic creations
- Anything which is contrary to public order or morality



Utility Model

A registrable utility model (UM) is any technical solution to a problem in any field of human activity which is new and industrially applicable. It may or may not have an inventive step.

Has 7 years of protection and non-renewable



Industrial Design

An industrial design constitutes the ornamental aspect of an article.

5 years renewable for 2 consecutive terms of 5 years

Industrial Design

An industrial design may consist of three dimensional features, such as the shape of an article,

or two dimensional features, such as patterns, lines or color.



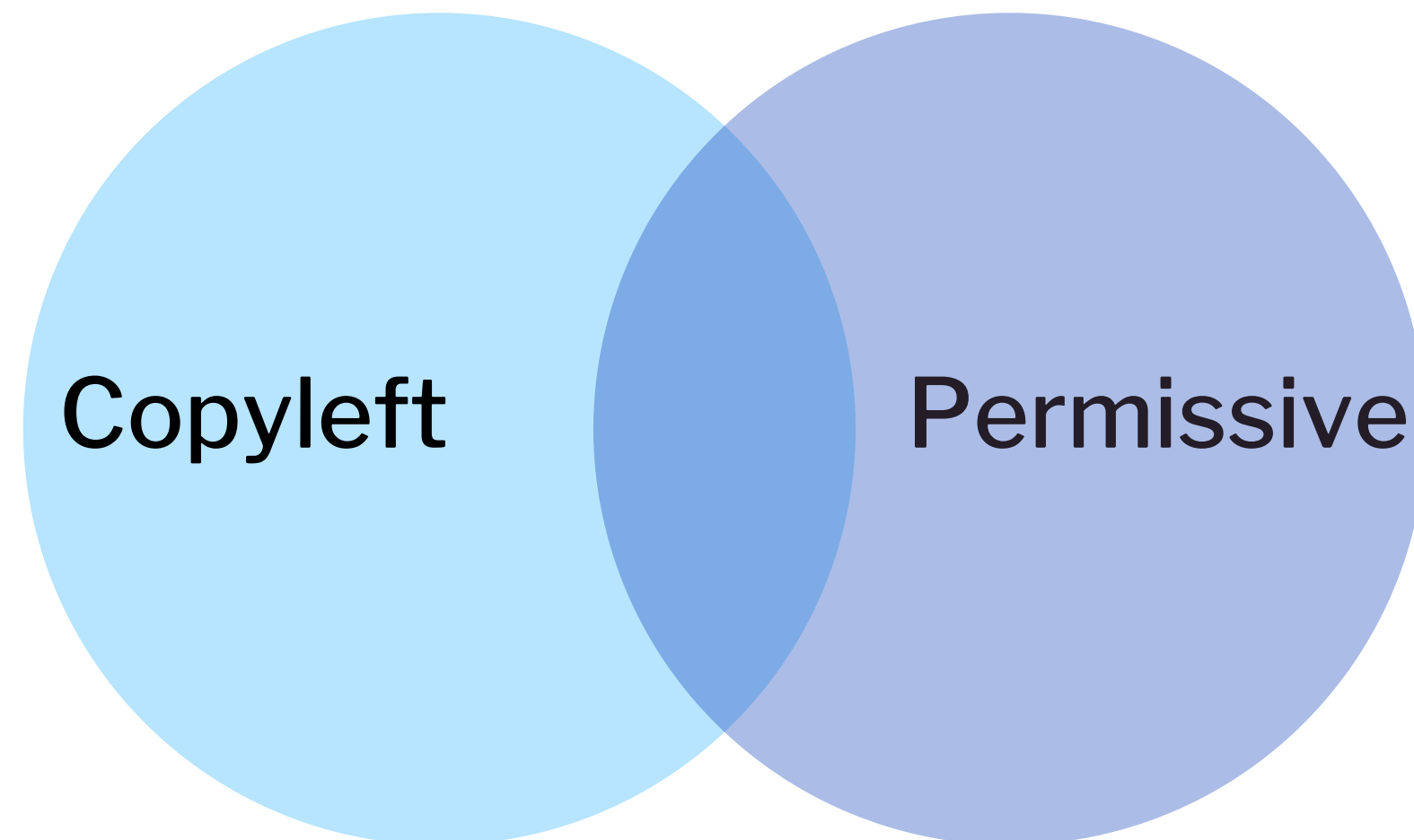


Part 4: Open Source IP

Industrial protection

Free and Open Source Software

Free to use does not mean IP-free





Freedoms of the Free Software Foundation

The freedom to run the program, for any purpose
(freedom 0)

The freedom to study how the program works, and adapt to your
needs
(freedom 1)

The freedom to redistribute copies
(freedom 2)

The freedom to improve the program and publish your
improvements
(freedom 3)



Copyleft

Mechanism to ensure all users have freedoms

- use the same free license on redistributing the software + modifications, and
- provide access to the source code of the original and modified software program. No longer possible to make the software “proprietary”



Permissive

“academic” origin

No substantive restrictions on use

Main requirement is to maintain the copyright notice and disclaimer



FOSS License Types

License Type	Scope	Example
Permissive	Few restrictions on reuse / redistribution Derivative or composed works may be closed	BSD, MIT, Apache Software License v2
“Weak” copyleft	Copyleft only on the original work, not on extensions or composed works using the work	LGPL, MPL, CPL
Strong copyleft	Copyleft on all the redistributed work, including new derivative and composed works incorporating the work	GPL2, GPL3, EUPL



Creative Commons

For copyright-protected works, a special form of license is available, the Creative Commons (CC) license. Works made available under a CC license can be freely distributed.

Creative Commons

Attribution

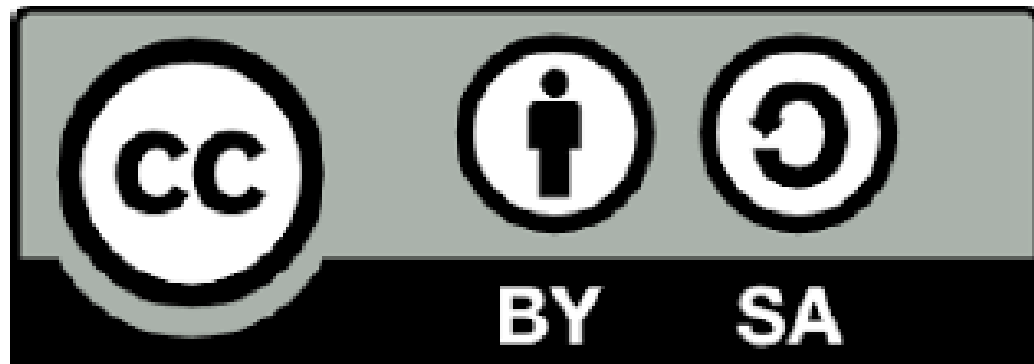


Licensees must give appropriate credit or attribution to the creator.

The work may be copied, distributed, displayed, performed, used for commercial purposes and even used to derive other works from it, as long as the creator is given credit.

Creative Commons

Share-Alike



Licensees **may distribute work** derived from licensed content, but they **must distribute the derived work under licensing terms** identical to those posed on the original work.

Creative Commons

Non-commercial



Licensees **may copy, distribute, display and derive** other works as long as it is done for non-commercial purposes only. Non-commercial works are **not intended for or directed toward commercial use** or monetary compensation.

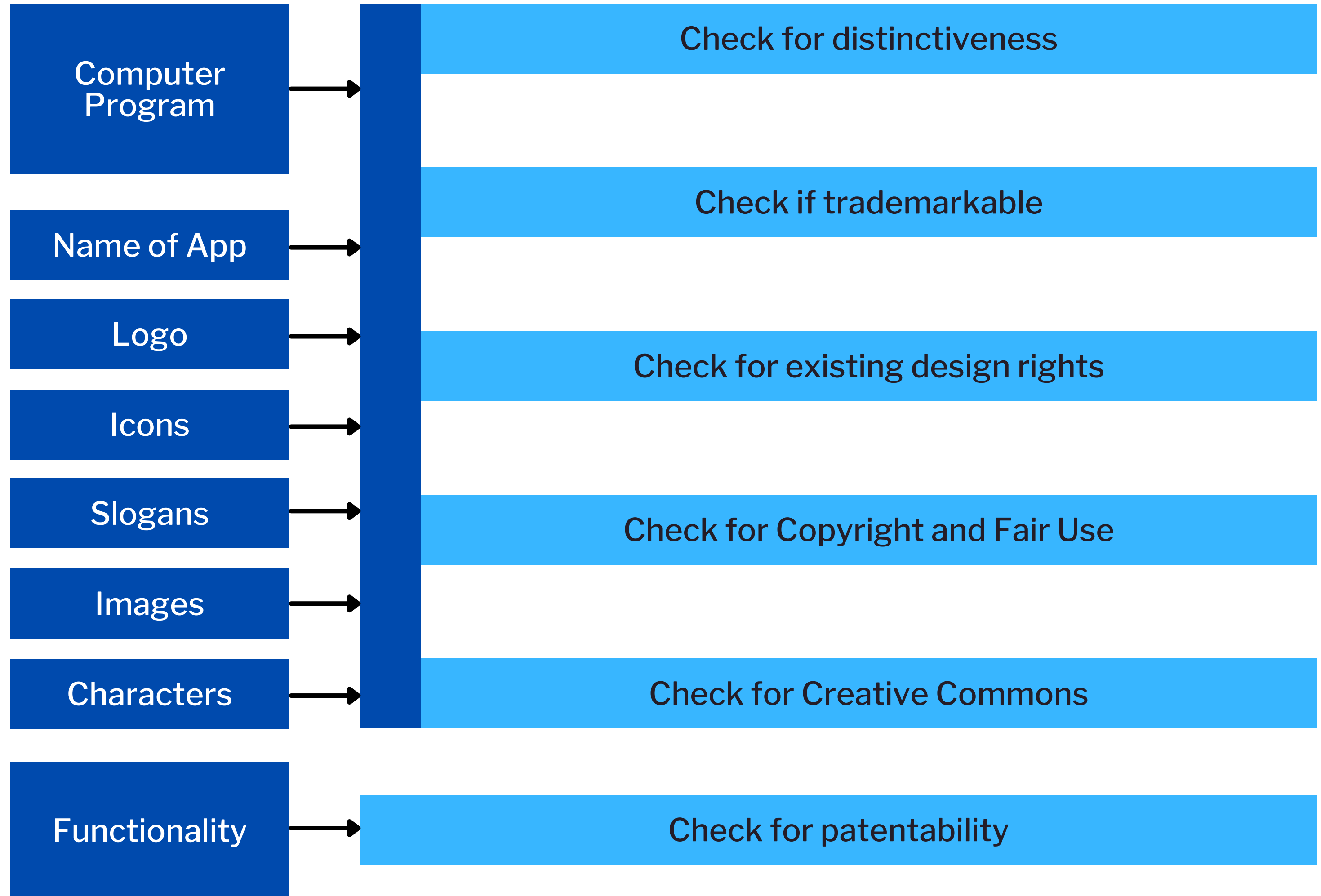
Creative Commons

No Derivative



Licensees may copy, distribute and display verbatim copies of the work, but they cannot make derivative works based on it.

App





Thank you