I. FREEDOM OF EXPRESSION

Introduction

- The Internet enables a worldwide exchange of news, ideas, opinions, rumors, and information. Its broad accessibility, open discussions, and anonymity make the Internet a remarkable communications medium.
- It provides an easy and inexpensive way for a speaker to send a message to a large audience-potentially thousands or millions of people worldwide. In addition, given the right email addresses, a speaker can aim a message with laser accuracy at a select subset of powerful and influential people.

Bases of the Guarantee of the Right of FoE

Discovery of truth (free market of an idea)

- Public opinion
- Everyone can speak their minds out and compete in the free market place of ideas

For self-government

- As official acts, as well as the private life of a public servant are legitimate subjects of public comments.

Scope of the Freedom of Expression

Freedom from Prior Restraint or Censorship

- Prior restraint means official governmental restrictions on the press or other forms of expression in advance of actual publication or dissemination.

Freedom from Punishment

- The freedom from prior restraint would be set at naught if the citizen would hesitate to speak for fear of vengeance that he might suffer against the officials criticized.

TEST	CRITERION
Dangerous Tendency Test	There should be a rational connection between the speech and the evil apprehended
Clear and present danger Test	There should be a clear and present danger that the words when used under such circumstances are of such a nature as to create a CLEAR and PRESENT DANGER that they will bring about the substantive evils that the State has a right to prevent
Balancing of Interests Test	The courts should BALANCE the PUBLIC INTEREST served by legislation on or and the freedom of speech on the courts will then decide where the weight should be placed.

What is Libel?

- A libel is public and malicious imputation of a crime, or of a vice or defect, real or imaginary, or an act, omission, condition, status or circumstance tending to cause the dishonor, discredit, or contempt of a natural or judicial person, or to blacken the memory of one who is dead.
- Libel is punished by our Revised Penal Code Art 353.
- Libel is defamation committed by means of writing, printing, lithography, engraving, radio, phonograph, painting, theatrical exhibition, cinematographic exhibition, or any similar means
- Art. 354. Requirement for Publicity - every defamatory imputation is presumed to be malicious, even if it be true, if no good intention and justifiable motive for making it is shown, except in the following cases

  1. A private communication made by any person to another in the performance of any legal, moral or social duty; and

  2. A fair and true report

Exception (Absolute or Qualified Communication)

A person cannot be held liable for defamation if such is under privileged communication.

- Example - speeches or debate made by congressmen or senators

Private communications and fair and true report without any comments or remarks

Elements of Defamation

- There must be an imputation of a crime, or of vice or defect, real or imaginary, or any act, omission, condition, status, or circumstance.
- The imputation must be made publicly.
- It must be malicious.
- The imputation must be directed at a natural or juridical person, or one who is dead.
- The imputation must tend to cause the dishonor, discreet or contempt of the person defamed.

Reason for punishing defamation

Proverbs 19:1 says "Better is the poor who walks in his integrity than one who is perverse in his lips, and is a fool."

II. INTELECTUAL PROPERTY

Introduction

- Intellectual property is a term used to describe works of the mind-such as art, books, films, formulas, inventions, music, and processes
- Intellectual property is protected through copyright, patent, and trade secret laws.
- Copyright law protects authored works, such as art, books, film, and music; patent law protects inventions; and trade secret law helps safeguard information that is critical to an organization's success.
- Together, copyright, patent, and trade secret legislation form a complex body of law that addresses the ownership of intellectual property.
- Defining and controlling the appropriate level of access to intellectual property are complex tasks. Ex. Software - difficult to categorized under to the law

Limits to Intellectual Property

- Giving creators right to their inventions stimulates creativity
- Society benefits most when inventions in public domain
- Congress has struck compromise by giving authors and inventors rights for a limited time

Definition

- A copyright is the exclusive right to distribute, display, perform, or reproduce an original work

in copies or to prepare derivative works based on the work.
- Copyright infringement is a violation of the rights secured by the owner of a copyright. Infringement occurs when someone copies a substantial and material part of another's copyrighted work without permission.

Eligible Works Title 17 of the US Code:
- architecture, art, audiovisual works, choreography, drama, graphics, literature, motion pictures, music, pantomimes, pictures, sculptures, sound recordings, and other intellectual works
- To be eligible: a work must fall within one of the preceding categories, and it must be original.

Fair Use Doctrine
- The fair use doctrine allows portions of copyrighted materials to be used without permission under certain circumstances; four factors:
    1. purpose and character of the use
    2. nature of the copyrighted work
    3. portion of the copyrighted work used in relation to the work as a whole
    4. effect of the use on the value of the copyrighted work

Software Copyright Protection
- Infringement: a software manufacturer can observe the operation of a competitor's copyrighted program and then create a program that accomplishes the same result and performs in the same manner.
- No infringement: two software manufacturers conceivably developed a separate but nearly identical programs for a simple game without any knowledge of the existing program.

Definition
- A patent is a grant of a property right issued by the USPTO to an inventor.
- A patent permits its owner to exclude the public from making, using, or selling a protected invention, and it allows for legal action against violators.
- Unlike a copyright, a patent prevents independent creation as well as copying.

Patent Infringement
- For an invention to be eligible for a patent, it must fall into one of three statutory classes of items that can be patented: It must be useful; it must be novel; and it must not be obvious to a person having ordinary skill in the same field.
- Patent infringement, or the violation of the rights secured by the owner of a patent, occurs when someone makes unauthorized use of another's patent.

Software Patents
- A software patent claims as its invention some feature or process embodied in instructions executed by a computer. Application software, business software, expert systems, and system software were patented
- Big names on patent battles:
    1. Oracle vs Google
    2. Apple vs Samsung
    3. Google vs Apple

Cross-Licensing Agreements
- Many large software companies have cross-licensing agreements in which each party agrees not to sue the other over patent infringements. For example, Apple and HTC battled for several years over various mobile phone-related patents, which eventually led to the U.S. International Trade Committee banning imports of two models of the HTC mobile phone. The two companies eventually agreed to a 10-year cross-licensing agreement that permits each party to license the other's current and future patents.

Definition
- A business information that represents something of economic value, has required effort or cost to develop, has some degree of uniqueness or novelty, is generally unknown to the public, and is kept confidential.
- Trade secret protection begins by identifying all the information that must be protected-from undisclosed patent applications to market research and business plans- and developing a comprehensive strategy for keeping the information secure.

Eligible Works
- To qualify as a trade secret, information must have economic value and must not be readily ascertainable. In addition, the trade secret's owner must have taken steps to maintain its secrecy.
- Trade secret laws do not prevent someone from using the same idea if it was developed independently or from analyzing an end product to figure out the trade secret behind it.

Advantages over Patents & Copyrights
1. There are no time limitations on the protection of trade secrets, unlike patents and copyrights;
2. There is no need to file any application or otherwise disclose a trade secret to outsiders to gain protection; and
3. There is no risk that a trade secret might be found invalid in court.

Definition
- A trademark is a logo, package design, phrase, sound, or word that enables a consumer to differentiate one company's products from another's.
- Consumers often cannot examine goods or services to determine their quality or source, so instead they rely on the labels attached to the products.
- The Lanham Act of 1946 - The law gives the trademark's owner the right to prevent others from using the same m or a confusingly similar mark on a product's label.
- Ultimately, the goal of trademarking is to protect the consumer by creating clear brand identification so they can easily identify the source of the products they are purchasing.

Key Intellectual Property Issues
1. **Plagiarism**
    - Plagiarism is the act of stealing someone's ideas or words and passing them off as one's own. Plagiarism detection systems enable people to check the originality of documents and manuscripts.
2. **Reverse Engineering**
    - Reverse engineering is the process of taking something apart in order to understand it, build a copy of it, or improve it. Reverse

engineering was originally applied to computer hardware but is now commonly applied to software as well.
- Reverse engineering of software involves analyzing it to create a new representation of the system in a different form or at a higher level of abstraction.

3. **Open-Source Code**
   - Open-source code is any program whose source code is made available for use or modification, as users or other developers see fit. The basic premise behind open-source code is that when many programmers can read, redistribute, and modify a program's code, the software improves.
   - Programs with open-source code can be adapted to meet new needs, and bugs can be rapidly identified and fixed. Open-source code advocates believe that this process produces better software than the traditional closed model.
4. **Competitive Intelligence**
   - A legally obtained information that is gathered to help a company gain an advantage over its rivals.
   - Requires the continual gathering, analysis, and evaluation of data with controlled dissemination of useful information to decision makers.
   - Is integrated into a company's strategic plan and executive decision making.
   - Competitive Intelligence # Industrial Espionage
5. **Trademark Infringement**
   - Trademark infringement is the unauthorized use of a trademark or service mark on or in connection with goods and/or services in a manner that is likely to cause confusion, deception, or mistake about the source of the goods and/or services. (USPTO)
6. **Cybersquatting**
   - Cybersquatting is registering, trafficking in, or using an Internet domain name with bad faith intent to profit from the goodwill of a trademark belonging to someone else. (Wikipedia)
   - It generally refers to the practice of buying up domain names that use the names of existing businesses with the intent to sell the names for a profit
   - Practice of registering as Internet domains identical or similar to a third-party company name or trade mark, in hope of reselling them at a profit.

III. CYBERCRIME

- **Introduction**
  Crime committed using a computer and the internet
  Computer is used as a means of a crime
  Refers to any and all illegal activities carried out using
  technology.
  Most cybercrime is an attack on information about individuals, corporations, or governments.

History

- 1834 — French Telegraph System — A pair of thieves hack the French Telegraph System and steal financial market information, effectively conducting the world's first cyberattack.
- 1870 — Switchboard Hack — A teenager hired as a switchboard operator is able to disconnect and redirect calls and use the line for personal usage.
- 1940 — First Ethical Hacker — Rene Carmille, a member of the Resistance in Nazi-occupied France and a punch-card computer expert who owns the machines that the Vichy government of France uses to process information, finds out that the Nazis are using punch-card machines to process and track down Jews, volunteers to let them use his, and then hacks them to thwart their plan.
- 1957 — Joybubbles — Joe Engressia (Joybubbles), a blind, 7-year-old boy with perfect pitch, hears a high-pitched tone on a phone line and begins whistling along to it at a frequency of 2600Hz, enabling him to communicate with phone lines and become the U.S.'s first phone hacker or "phone phreak."
- 1962 — Allan Scherr — MIT sets up the first computer
  passwords, for student privacy and time limits. Student Allan Scherr makes a punch card to trick the computer into printing off all passwords and uses them to log in as other people after his time runs out. He also shares passwords with his friends, leading to the first computer "troll." They hack into their teacher's account and leave messages making fun of him.
- 1969 — RABBITS Virus — An anonymous person installs a program on a computer at the University of Washington Computer Center. The inconspicuous program makes copies of itself (breeding like a rabbit) until the computer overloads and stops working. It is thought to be the first computer virus.
- 1970-1995 — Kevin Mitnick — Beginning in 1970, Kevin Mitnick penetrates some of the most highly-guarded networks in the world, including Nokia and Motorola, using elaborate social engineering schemes, tricking insiders into handing over codes and passwords, and using the codes to access internal computer systems. He becomes the most- wanted cybercriminal of the time.
- 1971 — Steve Wozniak and Steve Jobs — When Steve
  Wozniak reads an article about Joybubbles and other phone phreaks, he becomes acquainted with John "Captain Crunch" Draper and learns how to hack into phone systems. He builds a blue box designed to hack into phone systems, even pretending to be Henry Kissinger and prank-calling the Pope. He starts mass-producing the device with friend Steve Jobs and selling it to classmates.
- 2010 — The Stuxnet Worm — A malicious computer virus called the world's first digital weapon is able to target control systems used to monitor industrial facilities. It is discovered in nuclear power plants in Iran, where it knocks out approximately one-fifth of the enrichment centrifuges used in the country's nuclear program.
- 2010 — The Stuxnet Worm — A malicious computer virus called the world's first digital weapon is able to target control systems used to monitor industrial facilities. It is discovered in nuclear power plants in Iran, where it knocks out approximately one-fifth of the enrichment

centrifuges used in the country's nuclear program.
- 2014-2018 — Marriott International — A breach occurs on systems supporting Starwood hotel brands beginning in 2014. Attackers remain in the system after Marriott acquires Starwood in 2016 and aren't discovered until September 2018. The thieves steal data on approximately 500 million customers. Marriott announces it in late 2018.
- 2017 — WannaCry — WannaCry, the first known example of ransomware operating via a worm (viral software that replicates and distributes itself), targets a vulnerability in older versions of Windows OS. Within days, tens of thousands of businesses and organizations across 150 countries are locked out of their own systems by WannaCry's encryption. The attackers demand $300 per computer to unlock the code.

Cybercriminals
- Attackers are individuals or groups who attempt to exploit vulnerability for personal or financial gain. Attackers are interested in everything, from credit cards to product designs and anything with value.
- Children & adolescents between 6-18yrs old.
- Dissatisfied employees
- Professional hackers
- Organized hackers

Attack Modes & Manners
- Unauthorized access to computer systems or networks
- Theft of information contained in electronic form
- Data diddling
- DoS/DDoS Attack
- Trojan Attacks
- Web Jacking
- Email bombing

Categories
1. **Cybercrimes against persons**
   - Harassment via emails
   - **Cyber-stalking –** following person's movements across the internet
   - **Email spoofing –** misrepresents its origin
2. **Cybercrimes against IP**
   - **Computer vandalism –** damaging or destroying data
   - Transmitting malware
     1. Ransomware
     2. Trojan horse
     3. Virus
     4. Worm
3. **Cybercrimes against government**
   - **Cyber Terrorism –** by DDoS, hate websites/emails, attacks on networks, etc.
   - **Hacktivists –** make political statements to create awareness to issues that are important to them.
   - **State-sponsored –** attackers gather intelligence or commit sabotage on behalf of their government. These attackers are usually highly trained and well-funded, and their attacks are focused on specific goals that are beneficial to their government.
4. **Cybercrimes against nation**
   - **Cyberwarfare –** an Internet-based conflict that involves the penetration of computer systems and networks of other nations. These attackers have the resources and expertise to launch massive Internet-based attacks against other nations to cause damage or disrupt services, such as shutting down a power grid.

Types of Cybercrime
1. Child Pornography – use of computer networks to create, distribute, or access materials that sexually use underage children.
2. Cyber Contraband – transferring illegal items through the internet (such as encryption technology) that is barred in some locations.
3. Cyber Laundering – electronic transfer of illegally-obtained money with the goal of hiding its source and possible its destination.
4. Cyber Stalking – threats that creates fear through the use of computer technology such as emails, phones, text messages, webcams, websites or videos.
5. Cyber Theft – using a computer to steal. Activities such as breaking & entering, unlawful appropriation, identify theft, fraud, malicious hacking & piracy.
6. Cyber Trespass – unauthorized access of someone else's computer or network resources but does not alter, disturb, misuse or damage the data or system.

Cybersecurity
- Cybersecurity involves protection of sensitive personal and business information through prevention, detection, and response to different online attacks
- Cybersecurity protects your personal information by responding, detecting and preventing the attacks.
- Sets of strategies that prevents unauthorized access to organizational assets & maintains the integrity and confidentiality of sensitive information, blocking the access of hackers.

Protecting your Privacy
- Privacy Policy
- Evidence that your information is being encrypted
- Keep software up to date
- Use good passwords
- Disable remote connectivity

Cybercrimes covered in Republic Act 10175

Types of Cybercrime	Penalty
1. Illegal access Unauthorized access (without right) to a computer system or application	Prision mayor (imprisonment of 6 12 yrs) or a fine of at least P200,000 up to a maximum amount commensurate to the damage incurred or BOTH.
2. Illegal interception Unauthorized interception of any non-public transmission of computer data to, from, or within a computer system.	- same as above
3. Data Interference Unauthorized alteration, damaging, deletion or	- same as above

deterioration of computer data, electronic document, or electronic data message, and including the introduction or transmission of viruses	
4. System Interference Unauthorized hindering or interference with the functioning of a computer or computer network by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data or program, electronic document, or electronic data messages, and including the introduction or transmission of viruses.	- same as above
5. Misuse of devices The unauthorized use, possession, production, sale, procurement, importation, distribution, or otherwise making available, of devices, computer program designed or adapted for the purpose of committing any of the offenses stated in Republic Act 10175.	- same as above except fine should be no more than Five hundred thousand pesos (P500,000).
6. Cyber-squatting Acquisition of domain name over the Internet in bad faith to profit, mislead, destroy reputation, and deprive others from the registering the same. This includes those existing trademark at the time of registration; names of persons other than the registrant; and acquired with intellectual property interests in it	- same as above
7. Computer-related Forgery Unauthorized input, alteration, or deletion of computer data resulting to inauthentic 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	Prision mayor (imprisonment of 6 12 yrs) or a fine of at least P200,000 up to a maximum amount commensurate to the damage incurred or BOTH
8. Computer-related Fraud Unauthorized input, alteration, or deletion of computer data or program or interference in the functioning of a computer system, causing damage thereby with fraudulent intent.	- same as above Provided, That if no damage has yet been caused, the penalty imposed shall be one (1) degree lower.
9. Computer-related Identity Theft Unauthorized acquisition, use, misuse, transfer, possession, alteration or deletion of identifying information belonging to another, whether natural or juridical.	- same as above
10. Cybersex There is a discussion on this matter if it involves “couples” or “people in relationship” who engage in cybersex. For as long it is not done for favor or consideration, I don’t think it will be covered. However, if one party (in a couple or relationship) sues claiming to be forced to do cybersex, then it can be covered.	Prision mayor (imprisonment of six years and 1 day up to 12 years) or a fine of at least Two hundred thousand pesos (P200,000) but not exceeding One million pesos (P1,000,000) or BOTH.
11. Child Pornography 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.	Penalty to be imposed shall be one (1) degree higher than that provided for in Republic Act 9775, if committed through a computer system.
12. Unsolicited Commercial Communications (SPAMMING) The transmission of commercial communication with the use of computer system which seek to advertise sell, or offer for sale products and services are prohibited unless:	Imprisonment of arresto mayor (1 month and one day to 6 months) or a fine of at least Fifty thousand pesos (P50,000) but not exceeding Two hundred fifty thousand pesos (P250,000) or both.
13. Libel Unlawful or prohibited acts of libel as defined in Article355 of the Revised Penal Code, as amended committed through a computer system or any other similar means which may be devised in the future.	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.
14. Aiding or Abetting in the commission of cybercrime – Any person who willfully abets or aids in the commission of any of the offenses enumerated in this Act shall be held liable.	Imprisonment of one (1) degree lower than that of the prescribed penalty for the offense or a fine of at least One hundred thousand pesos (P100,000) but not exceeding Five hundred thousand pesos (P500,000) or both.
15. **Attempt in the commission of cybercrime** Any person who willfully attempts to commit any of the offenses enumerated in	- same as above

this Act shall be held liable.	
16. 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.	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.

Understanding the Cybercrime Prevention Law in the Philippines (RA 10175)

1. You shall only say nice things on the Internet
2. You cannot tell the TRUTH, whether joking or seriously, if it hurts someone
3. What you say can be held against you forever
4. What you like can also be held against you
5. The government now has the power to take down your Internet
6. Your Internet is required to compile evidence against you
7. You can be punished more harshly for online crimes than for real life crimes
8. You must trust the government to do the right thing in implementing the law
9. The law shall apply to all Filipinos wherever they are
10. The law doesn't really protect you

Conclusion:

1. Cybercrime is indeed getting the recognition it deserves.
2. However, it is not going to restricted that easily.
3. In fact, it is highly likely that cybercrime and its hackers will continue developing and upgrading to stay ahead of the law.
4. So, to make us a safer we must need cyber security.