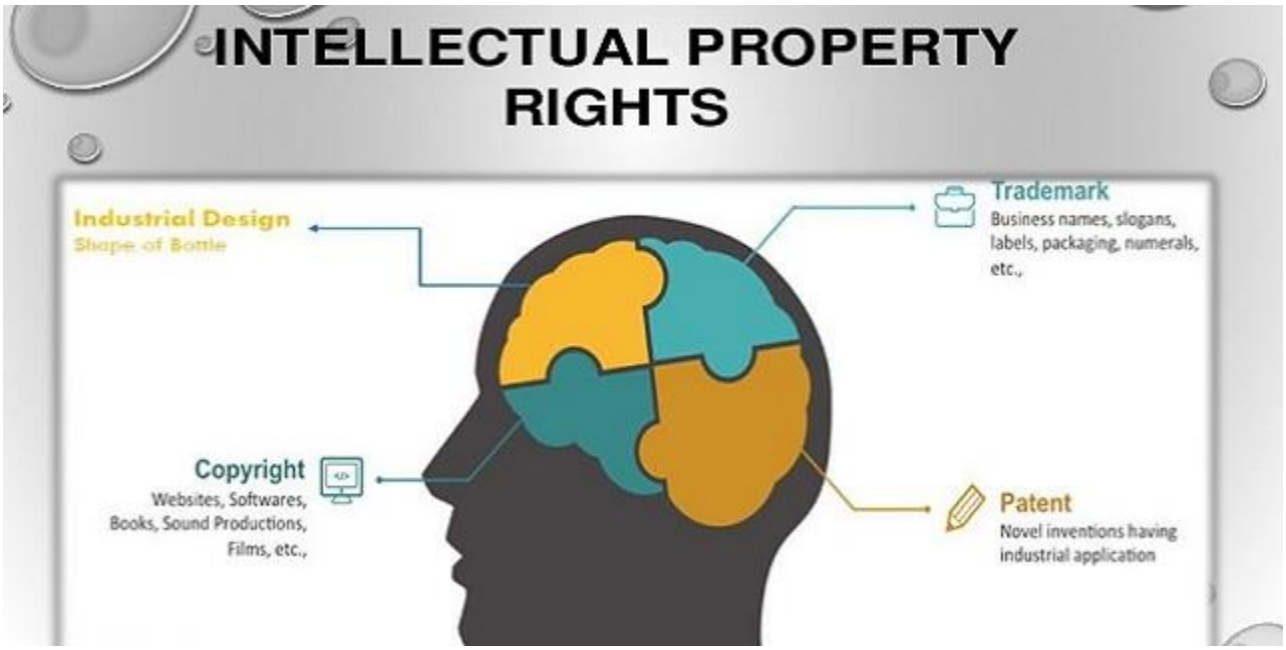
Unit IX: Contemporary Issues in E-Business

Intellectual Property Right Like Patent Right, Design right, Trademark, Copyright:

Intellectual property refers to creative work which can be treated as an asset or physical property. Intellectual property rights fall principally into four main areas; copyright, trademarks, design rights and patents. It is a term referring to creations of the intellect for which a monopoly is assigned to designated owners by law.



1. Patent Right:

A patent is a form of right granted by the government to an inventor, giving the owner the right to exclude others from making, using, selling, offering to sell, and importing an invention for a limited period of time, in exchange for the public disclosure of the invention. Patents apply to industrial processes and inventions and protect against the unauthorized implementation of the invention.

To get a patent, technical information about the invention must be disclosed to the public in a patent application. Patent is territorial and the protection is granted for a limited period, generally 20 years from the filing date of the application.

2. Industrial Design Right:

An **Industrial Design Right** protects the visual design of objects. An industrial design consists of the creation of a shape, configuration or composition of pattern or colour, or combination of pattern and colour in three-dimensional form containing aesthetic value.

The design when applied to a product gives the product a unique appearance. An industrial design can be a two- or three-dimensional pattern used to produce a product, industrial commodity or handicraft.

3. Trademark:

A **Trademark** can be a name, word, slogan, design, symbol or other unique sign that identifies a product or organization. Trademarks are registered at a national or territory level with an appointed government body and may take anywhere between 6 and 18 months to be processed.

Registering in countries such as the US, the UK, Japan, etc. will protect the mark in that country only but within the European Union, there now exists a Community Trade Mark (CTM) which covers the mark in all EU countries.

Registered trademarks may be identified by the abbreviation **TM** (Unregistered), or the **®** (Registered) symbol.

There is also the Madrid System that provides a facility to submit trademarks applications to many countries at the same time. Trademarks are used to distinguish the goods and services of one trader from those of another.

Trademark rights may be used to prevent others from using a confusingly similar mark, but not to prevent others from making the same goods or from selling the same goods or services under a clearly different mark.

4. Copyright:

Copyright is a form of protection provided to the authors of "original works of authorship" including literary, dramatic, musical, artistic, and certain other intellectual works, both published and unpublished. **It** is a legal right created by the law of a country that grants the creator of an original work exclusive rights to its use and distribution, usually for a limited time.
The 1976 Copyright Act generally gives the owner of copyright the exclusive right to reproduce the copyrighted work, to prepare derivative works, to distribute copies or phone-records of the copyrighted work, to perform the copyrighted work publicly, or to display the copyrighted work publicly.

The copyright protects the form of expression rather than the subject matter of the writing. Copyrights are *territorial*. Typically, the *duration* of copyright is the author's life plus 50 to 100 years (that is, copyright typically expires 50 to 100 years after the author dies, depending on the country).

Electronic Transaction/Cyber Law:

Electronic Transaction:

An electronic transaction is the sale or purchase of goods or services between businesses, households, individuals, governments, and other public or private organizations, conducted over computer-mediated networks. The goods and services are ordered over those networks, but the payment and the ultimate delivery of the good or service may be conducted on or off-line. *Uniform Electronic Transactions Act (UETA) developed in 1999 prepares the ETA (Electronic Transactions Act).*

Since the transaction relies on the network as the media, insecurity in the network leads to the disclosure or defacement of the transaction details. For example, online details

transferred for credit card payments may be captured by hackers to make other fake transactions. So, security issues have become a major issue in all electronic transactions. For its security, Electronic Transaction Acts are made with different obligations.

Secure Electronic Transaction (SET) is a system for ensuring the security of financial transactions on the Internet. It is supported by Mastercard, Visa, Microsoft, Netscape, and others. With SET, a user is given an *electronic wallet* (digital certificate) and a transaction is conducted and verified using a combination of digital certificates and digital signatures among the purchaser, a merchant, and the purchaser's bank in a way that ensures privacy and confidentiality.

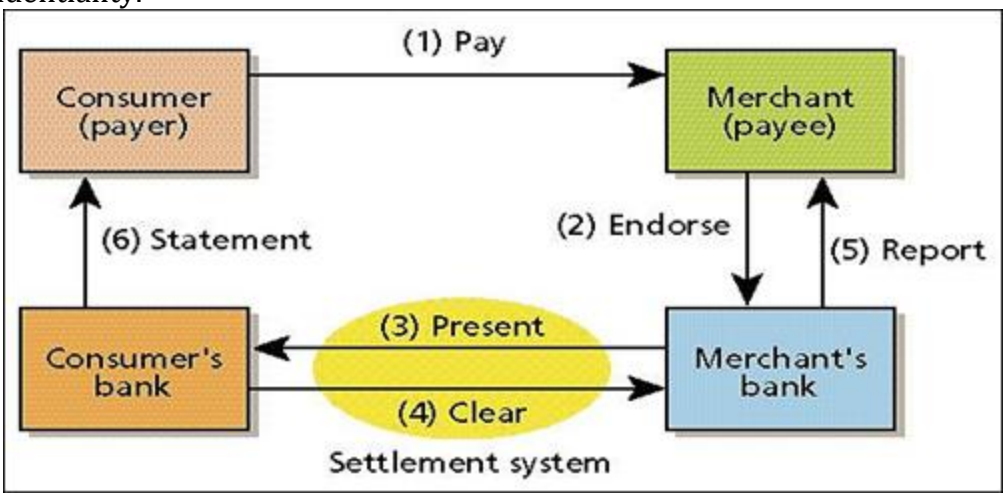
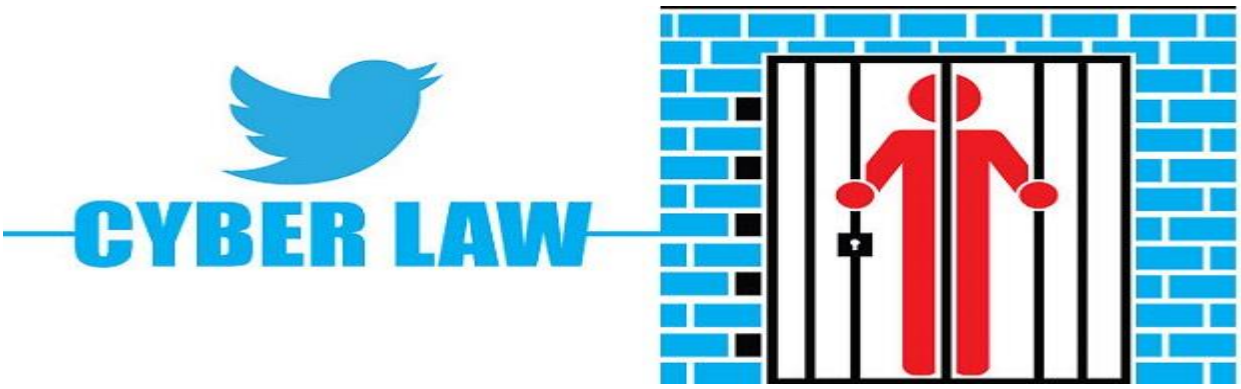


Fig: Secure Electronic Transaction

Cyber Law:

The Internet has its wide usage in all sorts of Businesses with its varying applications from personal use to agriculture to large scale enterprises, government sectors, etc. on one hand, while on the other hand, it has opened up many possibilities for the intruders to access the network and breach authentication to create defacement to the information base.



Cyber-crimes (Crimes that are committed over the internet) such as hacking, piracy, copyright violation, fraudulent and all other deceitful activities have now become major issues widely practiced on the internet. Cyberlaw is much about the legal issue of computing.

Cyberlaw or **Internet law** is a term that encapsulates the legal issues related to using of the Internet. It is less a distinct field of law than intellectual property or contract law, as it is a domain covering many areas of law and regulation. Some leading topics include internet access and usage, privacy, freedom of expression, and jurisdiction.

The Internet has opened up many opportunities for the world. It has given tremendous market access that anyone from any corner of the world can offer their products and services to any part of the world.

Types of Cyber Crimes:

Cyberlaw refers to all the legal and regulatory aspects of Internet and the World Wide. Besides, providing protection against new types of infringements of the business/consumer privacy rights, confidentiality of business information and other regulatory aspects, cyber law provides a legal framework to promote and conduct commerce along with the rapid development of new applications, thus build the necessary trust to use new applications.

The government of Nepal (House of Representatives) has approved the Electronic Transaction Act-2063 on 4th December 2006. According to Cyber Law in Nepal if an individual is found in such cybercrime like hacking the intellectual property of others, he or she will be punished for a minimum of 6 months to 3 years in prison and has to pay minimum of 50 thousand to max 3 lakhs.

1. Cyber-Stalking:

Cyber-stalking is a crime in which the attacker harasses a victim using electronic communication, such as e-mail or instant messaging (IM), or messages posted to a Web site or a discussion group. A cyber-stalker relies upon the anonymity afforded by the Internet to allow them to stalk their victim without being detected. Cyber-stalking messages differ from ordinary spam in that a cyber-stalker targets a specific victim with often threatening messages, while the scammer targets a multitude of recipients with simply annoying messages.

2. Fraud:

Fraud is a general term used to describe a cybercrime that intends to deceive a person in order to gain important data or information. Fraud can be done by altering, destroying, stealing, or suppressing any information to secure an unlawful or unfair gain.

3. Hacking:

Hacking involves the partial or complete acquisition of certain functions within a system, network, or website. It also aims to access to important data and information, breaching privacy. Most "hackers" attack corporate and government accounts. There are different types of hacking methods and procedures.

4. Identity Theft:

Identify theft is a specific form of fraud in which cybercriminals steal personal data, including passwords, data about the bank account, credit cards, debit cards, social security, and other sensitive information. Through identity theft, criminals can steal money. According to the

U.S. Bureau of Justice Statistics (BJS), more than 1.1 million Americans are victimized by identity theft.

5. Scamming:

The scam happens in a variety of forms. In cyberspace, scamming can be done by offering computer repair, network troubleshooting, and IT support services, forcing users to shell out hundreds of monies for cyber problems that do not even exist. Any illegal plans to make money falls to scamming.

6. Computer Viruses:

Most criminals take advantage of viruses to gain unauthorized access to systems and steal important data. Mostly, highly-skilled programs send viruses, malware, and Trojan, among others to infect and destroy computers, networks, and systems. Viruses can spread through removable devices and the internet.

7. Ransomware:

Ransomware is one of the most destructive malware-based attacks. It enters our computer network and encrypts files and information through public-key encryption. In 2016, over 638 million computer networks are affected by ransomware. In 2017, over $5 billion is lost due to global ransomware.

8. DDoS Attack:

DDoS or the Distributed Denial of Service attack is one of the most popular methods of hacking. It temporarily or completely interrupts servers and networks that are successfully running. When the system is offline, they compromise certain functions to make the website unavailable for users. The main goal is for users to pay attention to the DDoS attack, giving hackers the chance to hack the system.

9. Botnets:

Botnets are controlled by remote attackers called “bot herders” in order to attack computers by sending spams or malware. They usually attack businesses and governments as botnets specifically attack the information technology infrastructure. There are botnet removal tools available on the web to detect and block botnets from entering our system.

10. Spamming:

Spamming uses electronic messaging systems, most commonly emails in sending messages that host malware, fake links of websites, and other malicious programs. Email spamming is very popular. Unsolicited bulk messages from unfamiliar organizations, companies, and groups are sent to large numbers of users. It offers deals, promos, and other attractive components to deceive users.

11. Phishing:

Phishers act like a legitimate company or organization. They use “email spoofing” to extract confidential information such as credit card numbers, social security number, passwords, etc. They send out thousands of phishing emails carrying links to fake websites. Users will believe these are legitimate, thus entering their personal information.

12. Social Engineering:

Social engineering is a method in which cybercriminals make a direct contact with us through phone calls, emails, or even in person. Basically, they will also act like a legitimate company as well. They will be our friend to earn our trust until we provide our important information and personal data.

13. Malvertising:

Malvertising is the method of filling websites with advertisements carrying malicious codes. Users will click these advertisements, thinking they are legitimate. Once they click these ads,

they will be redirected to fake websites or a file carrying viruses and malware will automatically be downloaded.

14. Cyberstalking:

Cyberstalking involves following a person online anonymously. The stalker will virtually follow the victim, including his or her activities. Most of the victims of cyberstalking are women and children being followed by men and paedophiles.

15. Software Piracy:

The internet is filled with torrents and other programs that illegally duplicate original content, including songs, books, movies, albums, and software. This is a crime as it translates to copyright infringement. Due to software piracy, companies and developers encounter huge cut down in their income because their products are illegally reproduced.

16. Child Pornography:

Porn content is very accessible now because of the internet. Most countries have laws that penalize child pornography. Basically, this cybercrime involves the exploitation of children in the porn industry. Child pornography is a $3-billion-a-year industry. Unfortunately, over 10,000 internet locations provide access to child porn.

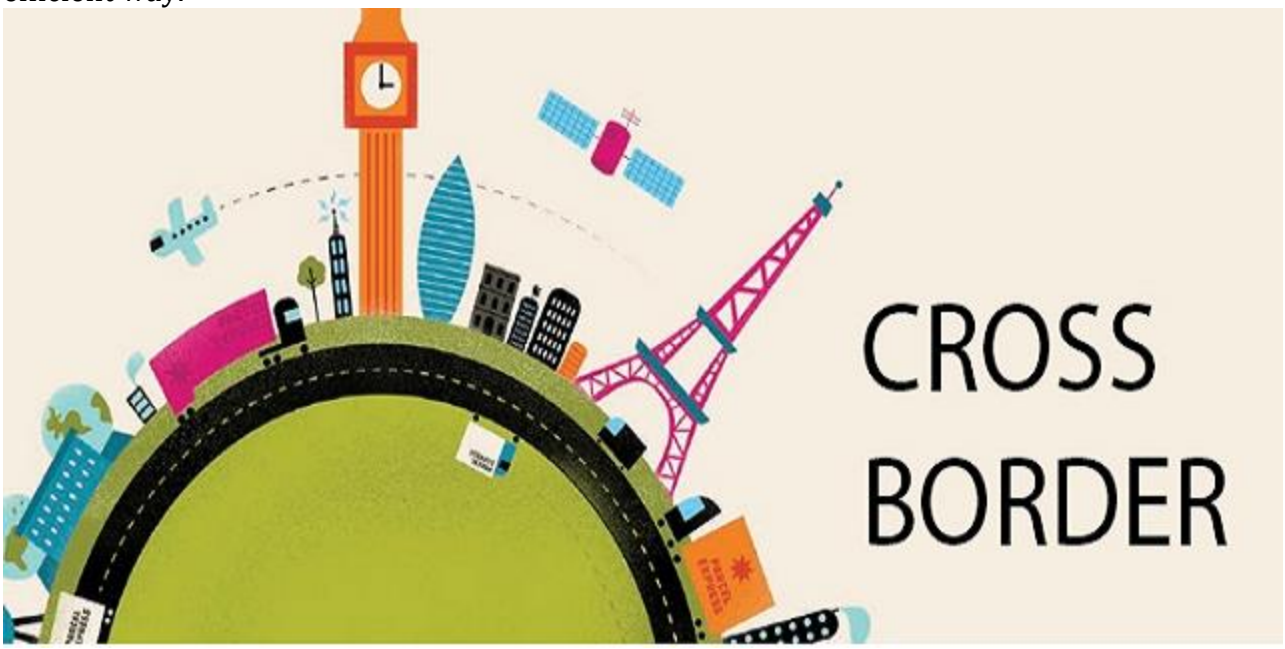
17. Cyberbullying:

Cyberbullying is one of the most rampant crimes committed in the virtual world. It is a form of bullying carried over to the internet. On the other hand, global leaders are aware of this crime and pass laws and acts that prohibit the proliferation of cyberbullying.

Cross-Border Legal Issues:

As cross-border business transactions are nowadays routine matters for business entities all over the world, the related legal aspects are becoming more and more complex. The success

of an M&A (Mergers & Acquisition) transaction lies with the common commercial operation principles along with the anticipation of potential legal issues, and careful structuring to navigate potential legal obstacles and to achieve the commercial objectives in a feasible and efficient way.



Since each nation have their own procedures for business transactions, cross border deal may be different and implementation of the business issues will greatly depend on the facts, dynamics, scale and the geographic scope of the particular situation.

Mergers and acquisitions (M&A) is the area of corporate finances, management and strategy dealing with purchasing and/or joining with other companies. In a **merger**, two organizations join forces to become a new business, usually with a new name.

Mergers and acquisitions (**M&A**) are transactions in which the ownership of companies, other business organizations or they're operating units are transferred or combined. As an aspect of strategic management, M&A can allow enterprises to grow, shrink, change the nature of their business or improve their competitive position.

Some of the key considerations that should be taken into account when embarking on any cross-border M&A transaction are as follows:

1. Deal Structure:

The deal structure depends on, among other things, the commercial objectives of the acquirer, and the financial, tax, and legal and regulatory considerations.

2. Due Diligence:

Due diligence is an essential part of the M&A process. In addition to the usual legal, financial and tax investigations, it is crucial in cross-border M&A transactions to be aware of the political, regulatory, currency, and infrastructure risks and other local issues.

3. Political Considerations:

Identifying and evaluating the actual or potential political implications should be accomplished in advance of initiating any M&A or strategic investment transaction. It may play a key part in M&A transactions involving politically-sensitive industries, such as defence, security and energy. In certain jurisdictions, advance notification and consultation with labour unions and other employees' representatives may be required.

4. Cultural and Communication Obstacles:

Cross-border transactions in-bound or out-bound present a unique set of issues that are compounded by the scale and geographic scope of the deal in which the cultural background, language requirements should also be considered.

Similarly, other related issues are:

a. Protection Of Intellectual Property Rights And Technology Transfer
b. Corporate Governance And Corporate Social Responsibility (CSR);

c. Letters Of Intent, Heads Of Agreement, Confidentiality And Exclusivity Agreements;
d. Insurance Policies;
e. Employment Law;
f. Anti-Trust Issues
g. Anti-Corruption Legislation

Ethical and Other Public Policy Issues:

1. Ethics:

It is Branch of philosophy that involves systematizing, defending, and recommending concepts of right and wrong conduct. But Right and wrong may not always be clear. Consider examples of unethical activities such as:
a. The company sells profiles of customers with information collected through cookies
b. The company allows personal use of the Web but secretly monitors activity
c. The company knowingly sells tax software with bugs

2. Web Spoofing:

Web spoofing is an electronic **deception relates to the Internet**. It occurs when **the attacker sets up a fake website** which almost totally same with the original website in order to lure consumers to give their credit card number or other personal information.

3. Privacy Invasion:

This issue is related to the consumer. **The privacy invasion occurs when the personal details belonging to consumers are exposed to the unauthorized party**.

4. Online Piracy:

The online piracy can be defined as **unauthorized copyright of electronic intellectual property such as e-books, music or videos**.

5. Email Spamming:

E-mail spamming, also known as unsolicited commercial e-mail (UCE) involves **using e-mail to send or broadcast unwanted advertisement or correspondence over the Internet**.

6. Poor Service:

Online sellers can ship damaged or counterfeit goods to customers, or fail to ship any goods at all. They may refuse returns or fail to give credit to the customer who in good faith returns the purchase.

7. Typosquatting:

Purchasing a domain name that is a variation on a popular domain name with the expectation that the site will get traffic off of the original sight because of a user's misspelling of the name.

For example, registering the domain names webapedia.com or yahooo.com in the hopes that someone making a typo will get to that site unexpectedly.

8. Bait and Switch:

Sellers often advertise amazing deals on the latest gadgets, such as laptops, flat-screen televisions and cellphones, and then divert the curious customers to sites that don't sell those goods at all, or may place a set of strict conditions such as providing a lot of personal information on the purchase.

Example: Ad claims $10 laptop (while supplies last) there was one a while ago that was 10 years old, but that ad wasn't lying, however, it was misleading and it got the customer onto their site.