**E-COMMERCE**

**UNIT-4**

**BCA-3rd Year**

**Common Legal Issues Faced By E-Commerce Businesses**

There are various legal issues associated with e-commerce as well. And if these issues are not taken care of in time, they can lead to serious problems for your business.

Described below are some of the common legal issues an e-commerce business faces.

**Incorporation Problem**

If you are a company operated merely via a website, not being incorporated is a crucial problem. Any purchase and selling activity related to your products will be considered illegal and you can’t claim your right in case of any fraud and corruption. Without incorporation, your business has no shelter.

**Trademark Security Problem**

Not getting your trademark protected is one of the main legal issues in the field of e-commerce. Since trademark is your company’s logo and symbol, the representation of your business all over the web, it must be protected. If you don’t secure it, it won’t take long before you’ll realize your trademark is being infringed upon. This is very common legal issue and can become a deadly threat to your e-business.

With the [hackers](https://study.com/academy/lesson/what-is-a-hacker-definition-lesson-quiz.html) on loose and cybercrime so common, trademark infringement of your business or by your business can be a serious legal matter and may hinder your business’s progress.

**Copyright Protection Issue**

While publishing content for your e-commerce website, using content of any other company can be a severe legal problem. This might mark an end to your e-business. There are many sites online which are royalty free and allow you to access their content and images. You may use those sites for creating web content for your business site.

Even if you unintentionally used copyrighted content, the other party can easily sue your business.

**Transaction Issues**

The Australian Consumer Law (ACL) governs all e-commerce transactions in Australia. Therefore, if you do not abide by the rules, you can get into serious law violation problems.

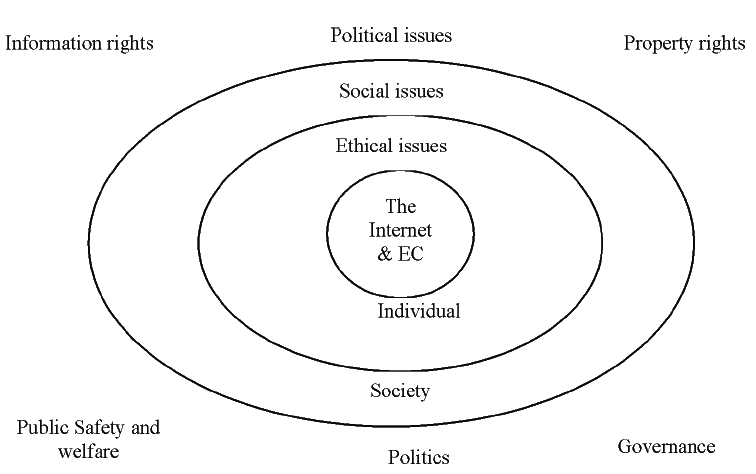
**Privacy Issues**

When it comes to online businesses, privacy is the major issue that can create problems both for the business and customers. Consumers share information with businesses online and they expect the sellers to keep their information confidential. By just one minor mistake and leakage of valuable information of a customer, you’ll not only lose your potential customer but your image and reputation will become a question mark. Moreover, you’ll be subjected to serious legal problems according to Australian privacy laws.

## Public Policy Issues in E commerce

The major ethical, social, and political issues that have developed around e commerce over the past seven to eight years can be loosely categorized into four major dimensions: **information rights, property rights, governance, and public safety and welfare**. Some of the ethical, social, and political issues raised in each of these areas include the following:

* **Information rights:**What rights to their own personal information do individuals have in a public marketplace, or in their private homes, when Internet technology make information collection so pervasive and efficient? What rights do individuals have to access information about business firms and other organizations?
* **Property rights:**How can traditional intellectual property rights be enforced in an internet world where perfect copies of protected works can be made and easily distributed worldwide in seconds?
* **Governance:**Should the Internet and e-commerce be subject to public laws? And if so, what law-making bodies have jurisdiction - state, federal, and/or international?
* **Public safety and welfare:**What efforts should be undertaken to ensure equitable access to the Internet and ecommerce channels? Should governments be responsible for ensuring that schools and colleges have access to the Internet? Is certain online content and activities - such as pornography and gambling - a threat to public safety and welfare? Should mobile commerce be allowed from moving vehicles?



## Protecting Intellectual Property in E Commerce

**Types of Intellectual Property Protection**

There are three main types of intellectual property protection:

* Copyright,
* Patent and
* Trademark law.

**Copyright: The Problem of Perfect Copies and Encryption**

In the United States, **copyright**law protects original forms of expression such as writings (books, periodicals, and lecture notes), art, drawings, photographs, music, motion pictures, performances, and computer programs from being copied by others for a minimum of 50 years. Copyright does not protect ideas -just their expression in a tangible medium such as paper, cassette tape, or handwritten notes.

Copyrights, like all rights, are not absolute. There are situations where strict copyright observance could be harmful to society, potentially inhibiting other rights such as the right to freedom of expression and thought. As a result the doctrine of fair use has been created. The **doctrine of fair use**permits teachers and writers. to use copyrighted materials without permission under certain circumstances. The fair use doctrine draws upon the First Amendment’s protection of freedom of speech (and writing). Journalists, writers, and academics must be able to refer to, and cite from, copyrighted works in order to criticize or even discuss copyrighted works. Professors are allowed to clip a contemporary article just before class, copy it, and hand it out to students as an example of a topic under discussion.

**Patents: Business Methods and Processes**

A patent grants the owner an exclusive monopoly to the ideas behind an invention for 20 years. The congressional intent behind patent law was to ensure that inventors of new machines, devices, or industrial methods would receive the full financial and other rewards of their labor and yet still makes widespread use of the invention possible by providing detailed diagrams for those wishing to use the idea under license from the patent’s owner. Patents are obtained from the United States Patent and trademark Office (USPTO), created in 1812. Obtaining a patent is much more difficult and time-consuming than obtaining copyright protection (which is automatic with the creation of the work). Patents must be formally applied for, and the granting of a patent is’ determined by ‘Patent Office examiners who follow a set of rigorous rules. Ultimately, federal courts decide when patents are valid and when infringement occurs.

Patents are very different from copyrights because patents protect the ideas themselves and not merely the expression of ideas.

There are four types of inventions for which patents are granted under patent law:**machines, man-made products, compositions of matter, and processing methods**.

**Trademarks: Online Infringement and Dilution**

Trademark law is a form of intellectual property protection for trademarks - a mark used to identify and distinguish goods and indicates their source. Trademark protections exist at both the federal and state levels in the United States. The purpose of trademark law is twofold. First, the trademark law protects the public in the market-place by ensuring that it gets what it pays for and wants to receive. Second, trademark law protects the owner - who has spent time, money, and energy bringing the product to the marketplace - against piracy and misappropriation.

‘Trademarks have been extended from single words to pictures, shapes, packaging, and colors”. Some things may not be trademarked: common words that are merely descriptive (“clock”), flags of states and nations, immoral or deceptive marks, or marks belonging to others. Federal trademarks are obtained, first, by use in interstate commerce, and second, by registration with the U.S. Patent and ‘Trademark Office (USPTO). ‘Trademarks are granted for a period of ten years, and can be renewed indefinitely.

Disputes over federal trademarks involve establishing infringement. The test for infringement is twofold: **market confusion and bad faith**. Use of a trademark that creates confusion with existing trademarks, causes consumers to make market mistakes, or misrepresents the origins of goods is an infringement.

# Electronic commerce and free speech

For commercial purveyors of digital speech, information and entertainment, the biggest threat posed by the Internet isn't the threat of piracy, but the threat posed by free speech -- speech that doesn't cost any money. Free speech has the potential to squeeze out expensive speech. A glut of high quality free stuff has the potential to run companies in the business of selling speech out of business. We haven't had to worry about this before, because speaking in a meaningful way to a large audience was expensive, and people couldn't afford to do serious mass speaking for free for very long. The Internet has made it much cheaper. It doesn't take much to give out information to the whole world, every day, for free, for years. And people do. If we are trying to increase the abundant dissemination of information, free speech is good. If we are trying to increase commerce in information, free speech is arguably bad, in that it competes with pay speech.

# Internet censorship

# Internet censorship is the [control or suppression](https://en.wikipedia.org/wiki/Censorship) of what can be accessed, published, or viewed on the [Internet](https://en.wikipedia.org/wiki/Internet) enacted by regulators, or on their own initiative. Individuals and organizations may engage in [self-censorship](https://en.wikipedia.org/wiki/Self-censorship) for moral, religious, or business reasons, to conform to societal norms, due to intimidation, or out of fear of legal or other consequences.

# The extent of Internet censorship varies on a country-to-country basis. While most democratic countries have moderate Internet censorship, other countries go as far as to limit the access of information such as news and suppress discussion among citizens. Internet censorship also occurs in response to or in anticipation of events such as elections, protests, and riots. An example is the increased censorship due to the events of the [Arab Spring](https://en.wikipedia.org/wiki/Arab_Spring). Other types of censorship include the use of copyrights, defamation, harassment, and obscene material claims as a way to suppress content.

## Taxation and Encryption Policies

**The Future for Ecommerce Taxation**

The Commission on Electronic Commerce, created by the ITFA legislation, has not been able to make any headway in the taxation debate, but several members have voice support for Internet taxes, provided the tax is simple to calculate for businesses. This could mean a uniform tax rate agreed to by all the states, or technological advances that would allow businesses to calculate the sales tax simply and without a large investment in time and resources.

Unfortunately, the current state and local tax systems, which number close to 7,500 throughout the U.S., are notoriously parochial minded when it comes to defending their jurisdiction. In Texas alone, there are more than 1,300 separate sales tax jurisdictions. These numbers could be significantly increased if states and local jurisdictions were allowed to tax Ecommerce.

Small businesses would be buried in costly paperwork attempting to comply with all these rules. That is precisely why the commerce clause in the Constitution prohibits taxes and is an undue burden on interstate commerce.

**Encryption policy:**

Encryption is a technique for hiding data. The encrypted data can be read only by those users for whom it is intended. Nowadays various encryption techniques are available. One of the available techniques commonly used for encryption is Public Key. In Public Key encryption system, RSA Data Security of Redwood City offers the most popular and commercially available algorithm.

In a Public Key encryption system each user has two keys-public key and private key. The encryption and decryption algorithms are designed in a way so that only the private key can decrypt data that is encrypted by the public key. And the public key can decrypt data, encrypted by the private key. Therefore, one can broadcast the public key to all users.

Computer encryption is based on the science of cryptography, which has been used throughout history. Before the digital age, the biggest users of cryptography were governments, particularly for military purposes.

Most computer encryption systems belong in one of two categories. Broadly speaking, there are two types of encryption methods:

* Secret-key cryptography
* Public-key cryptography

**Data Encryption Standard (DES)**

A widely-adopted implementation of secret-key cryptography is Data Encryption Standard (DES). The actual software to perform DES is readily available at no cost to anyone who has access to the Internet. DES was introduced in 1975 by IBM, the National Security Agency (NSA), and the National Bureau of Standards (NBS) (which is now called NIST). DES has been extensively researched and studied over the last twenty years and is definitely the most well-known and widely used cryptosystem in the world. DES is secret-key, symmetric cryptosystem: When used for communication, both sender and receiver must know the same secret key, which is used both to encrypt and decrypt the message. DES can also be used for single user encryption, for example, to store files on a hard disk in encrypted form. In a multi-user environment, however, secure-key distribution becomes difficult; public-key cryptography, discussed in the next subsection, was developed to solve this problem.

DES operates on 64-bit blocks with a 56-bit secret key. Designed for hardware implementation, it operation is relatively fast and works well for large bulk documents or encryption. Instead of defining just one encryption algorithm, DES defines a whole family of them. With a few exceptions, a different algorithm is generated for each secret key. This means that everybody can be told about the algorithm and your message will still be secure. You just need to tell others your secret key a number less than 256. The number 256 is also large enough to make it difficult to break the code using a brute force attack (trying to break the cipher by using all possible keys). DES has withstood the test of time. Despite the fact that its algorithm is well known, it is impossible to break the cipher without using tremendous amounts of computing power.

A new technique for improving the security of DES is triple encryption (Triple DES), that is, encrypting each message block using three different keys in succession. Triple DES, thought to be equivalent to doubling the key size of DES, to 112 bits, should prevent decryption by a third party capable of single-key exhaustive search. Of course, using triple-encryption takes three times as long as single encryption DES. If you use DES three times on the same message with different secret keys, it is virtually impossible to break it using existing algorithms. Over the past few years several new, faster symmetric algorithms have been developed, but DES remains the most frequently used.

**Customer’s Trust Online**

***Presentation***

The look of a site conveys a sense of personality and influences the degree to which visitors are prepared to trust the site owner. If an organisation already has a corporate identity then the site should be consistent with this. On-screen design and copy styles should reflect existing printed literature. A company’s colours may need re-working online, to a new palette that is fast to download to the computer screen. Developing a brand to work online is a new task. The internet is tactile - web pages should look, sound and move in ways that reinforce the company’s existing image.

***Navigation***

If customers walk into a new high street shop they can usually find their way around. There are conventions for laying out a shop and customers unconsciously understand and follow them. Online conventions are still being developed. Therefore, some judgement will be needed to make first-time visits successful.

The challenge is to create enticement – to explore the store - without customers getting lost. On the home page a site’s purpose must be clear to the first-time visitor. Use simple words to describe the site’s content and make it easy for visitors to find what they are looking for by giving clear instructions.

***Fulfilment***

Goods have now been selected and your customer has made it to the checkout. At this point most shopping carts are abandoned. Websites can keep customers’ trust by taking them through a transparent transaction process. At all times customers should know where they are in the checkout process and they should be able to find out what happens later. It must be easy to see: How orders are to be processed The company’s returns policy. Online and offline customer support services. The company’s security policy for personal information. If you have shops on the high street, give customers the option to return goods there. And remember to train your staff to handle returned online orders.

***Familiar Names & Logos***

Names that we know and trust are familiar and friendly. If we see them on a website we trust the website more. Customers trust sites where they can see the familiar logos of credit card brands, major software companies and web security organizations. If your company is trusted by these organizations, don’t hide it. Should your company have a familiar name, use it to build customer expectation of the site’s content, the quality of products and the level of service support. Web customers will have higher service expectations than offline customers. They may expect service delivered in real time, with transparency and, above all, with consistency.

***Technology***

Too much technology can be daunting. Use technology as a transparent aid to navigation and activity. Aim for graphics and functions in proportion to your customer’s needs. These needs will change with your customer’s experience. Are you handling visitors new to the web trade or devotees?

* Newcomers need signposts and easy navigation.
* Old hands need quick routes to every part of the site.

**E-commerce and the new legal framework**  
  
The use of the Internet and the general development of communication technology have raised the issue of the elimination of legal barriers for contractual relationships conducted through electronic means. The Albanian legislation, which is based on traditional civil law, contains obstacles to the development of information society services, since the concept of creation, validity and extinguishment of contractual relationships is traditionally linked to paper documents.  
  
In order to provide for the necessary legal framework regulating business activities performed through electronic means, Parliament approved the E-commerce Law on May 11 2009.[(1)](https://www.internationallawoffice.com/Newsletters/Tech-Data-Telecoms-Media/Albania/Hoxha-Memi-Hoxha/E-commerce-and-contracts-concluded-by-electronic-means#1) In particular, the law establishes the basic rules for performing business activities through electronic instruments by ensuring protection for persons, entities and consumers, and determines the responsibilities of services providers.  
  
The law is based on the principles of equity, free will, contractual freedom, free movement of goods and services within Albania and free entrepreneurship. Under the law, information society services may be offered by any entrepreneur or company registered with the National Registration Centre[(2)](https://www.internationallawoffice.com/Newsletters/Tech-Data-Telecoms-Media/Albania/Hoxha-Memi-Hoxha/E-commerce-and-contracts-concluded-by-electronic-means#2) without the need for specific authorisation or a permit. Exceptions to this rule are made for service providers offering financial or insurance services and other specific cases foreseen by law.  
  
In addition, the law does not apply to legal relationships in the field of taxation, protection of personal data, questions related to practice and agreements regulated by competition law, activities of notaries and other similar activities (eg, **gambling** activities) directly related to the exercise of public authority.

**E-contracts**  
  
The law recognises that contracts may be concluded by electronic means in accordance with the provisions of the Civil Code and the specific requirements on consumer protection.[(3)](https://www.internationallawoffice.com/Newsletters/Tech-Data-Telecoms-Media/Albania/Hoxha-Memi-Hoxha/E-commerce-and-contracts-concluded-by-electronic-means#3) The law applies to the provision of information society services to individuals and legal entities, excluding the conclusion of contracts that by law must be executed in the form of material deeds (ie, real estate contracts), grant representation powers for court procedures and/or other similar procedures (ie, administrative appeals), as well as gambling transactions. Moreover the law does not apply to transactions relating to tax issues, protection of personal data as well as other transactions that may fall under the scope of competition law.  
  
The law appears to be in line with the principles set out in EU Directive 2000/31/EC, especially referring to Section 3, Article 9 on legal validity and effectiveness of contracts concluded by electronic means.  
  
**Conclusion of e-contracts**  
  
Based on the law, an e-contract is concluded when the recipient receives an electronic message containing confirmation and acceptance of the offer. The order and the acceptance of the order by the parties, due to their e-commerce legal relationship, are deemed to be received when the parties to which they are addressed can access them. In addition, the service provider must render a summary of the general and specific terms of the e-contract, and confirm without delay receipt of the order by the recipient, except when non-consumer parties agree otherwise.

**Consumer protection in e-commerce**

The Indian Consumer Protection laws, backed by the International guidelines are able to protect consumers in e-commerce even in the absence of explicit laws concerning online transactions. In this respect, the person making the purchase or transaction online would qualify as the consumer and would be able to bring a suit against any online shopping portal as the dealer under any of the above mentioned grounds.

The court to which a consumer is supposed to apply depends on the amount of claim and the geographical position as follows:

1. **Amount of claim:**

 1.If the amount is less than Rs. 20 Lakh – **District Consumers Forum**;

2. If the amount is more than Rs. 20 Lakh & upto Rs One crore – **Consumer Disputes Redressal Commission** of the concerned State;

3. If the amount is more than Rs. One crore – **National Consumer Disputes Redressal Commission** New Delhi.

B. **The area of jurisdiction**:

When applying to a District Forum, the court should have local jurisdiction over either :

1. The **place of residence** of one of the opposite parties;
2. The **area of business** of one of the opposite parties;
3. The **place where the cause of action arises**.

Since most shopping portals have offices in all cities, the consumer, in this case, would have to apply to the court with jurisdiction where the cause of action arose.

The new**Consumer Protection Bill, 2015** provides for new laws related to e-commerce and hence will be of great assistance to consumers, once adopted, as they would have explicit and concrete laws to rely on for their protection of rights as a consumer along with their safety and privacy.

**Precautions to be taken by consumers**

In addition to the laws protecting consumers, consumers themselves ought to be careful and take some precautionary measures while making transactions and purchases online. A few examples are as follows:

1. Be well informed about the dealer before making an online purchase;
2. Read up on the privacy policy of the online portal or the dealer;
3. Never make purchases from unknown online retailers;
4. Read reviews before making a purchase;
5. Monitor your bank account from where you make the online transactions regularly. Prefer using credit cards for online purchases instead of debit cards.

**Conclusion**

In the new era of digitalization, e-commerce has revolutionized the Indian market. It is a great opportunity for both dealers and consumers, but only if the transactions are regulated and monitored to make sure that there are no unfair practices plaguing the market which would prove to be detrimental. Protecting consumer rights is of the utmost importance as they are the backbone of any economy and everyone is a consumer in one way or the other. With new advancements and technology, the laws need to be up to date to ensure smooth functioning of business and a stable economy. Issues like international e-commerce not falling under the jurisdiction of local consumer forums, promised free services not being protected under the current consumer law, and no proper consumer law mechanism ensuring and enforcing privacy of sensitive personal information shared online for transactions need to be tackled immediately. Either the proposed Bill needs to be passed urgently or separate law for the consumer protection of e-consumers, as present in the UK, needs to be brought into existence as soon as possible.

**Reference**

Consumer Protection Act, 1986