**Patent**

A patent is an exclusive right granted by law to make, use and sell an invention. In order to be patentable, the invention must be unique, genuine, and useful according to the prevalent technological standards.

**Trade mark and domain name conflicts**

A trade mark is that sign/symbol that associates the manufacturer or service provider with the manufactured goods or services, respectively. For instance, where the letter ‘u’ is written in a particular style (say in a circle) on the product packaging, it can be termed as a trade mark. A trade name is that name or brand under which a business carries on its business activity to become recognizable. Often, a trade name can be used as a part of the trade mark. A domain name is the user friendly name used to access a web site, such as ‘vu.edu’. Domain names are unique and global in nature which means that there cannot be two similar domain names. On the other hand, trade marks/trade names can be multiple and localized. Thus, same trade mark/trade name can be used in relation to the same product/service in different countries or geographical areas. Similarly, same trade mark/trade name can be used in relation to different products/services within the same geographical area. Based upon this distinction between trade marks/trade names and the domain names, the experts have **identified four areas of conflict as follows**:

1. **Cyber squatting**

The act of intentionally registering domain names containing trademarks/trade names of prominent companies to later blackmail or demand ransom from those companies is called cyber squatting. It is regarded as an offence in most countries. Assume there is a firm ‘Glory Enterprise’ and it wants to have its web site. It also wants to have the word ‘glory’ as a part of its domain name because for years it has been recognized in the physical world through this word. However, at the time of registration of its domain name it finds that a person Mr. ‘A’ who has nothing to do with the business of the firm or the word ‘glory’ has already registered a domain name containing this word as a part of it. Since there cannot be two similar domain names, the firm is forced to request Mr. ‘A’ to transfer that domain name to it. In response, if Mr. ‘A’ blackmails or claims ransom from the said firm, he would be said to have committed cyber squatting.

1. **Concurrent use**

This problem arises when two organizations have apparently legitimate claim to use the same domain name but cannot do so due to the uniqueness of domain names. Suppose, there is a company manufacturing electronic goods and another company selling French fries. Under the traditional trade mark law both these companies can have the same trade mark/trade name such as ‘frys’. The problem arises when both apply for the registration of a domain name containing the word ‘frys’

1. **Parasites**

Parasite domain names are variants on famous domain names, and are confusingly similar to them to gain business advantage. For instance, a software company may intentionally register a domain name as‘macrosoft.com’ (a variant of domain name of the famous company ‘Microsoft’) to take advantage of the reputation of ‘Microsoft’. The idea is that someone intending to reach the web site of ‘Microsoft’may mistype or misspell and reach the web site of ‘Microsoft’, instead. xyz.com vs. xyz.org This problem arises due to the fact that second level domain names can be assigned to multiple toplevel domains. For example, ‘whitehouse.org’ and ‘whitehouse.com’ are two valid domain names. The former may take you to the web site containing information about the residence of the American President, whereas the later may have been deliberately registered with the same second level domain but a different top-level domain to gain business advantage.

1. **Online Defamation**

A defamatory statement is a false statement that injures the reputation of on another person or company. If a statement injures the reputation of a product or service instead of a person, it is called product disparagement. Suppose, someone circulates a news item in the media about the reputation of a doctor, alleging him to be professionally incompetent and negligent. This doctor may then file a lawsuit against that person claiming that his reputation has been injured due to such an act. Often, in cases of defamation the plea taken by the defendant is that his statement is not false. Rather, it is a ‘fair comment’. In case defamation is done using the internet, it is termed as online defamation. In countries abroad, the courts are replete with cases of online defamation, mainly, because the person causing defamation can expect to remain anonymous due to the nature of internet technology. It is difficult to draw a clear line between justifiable criticism and defamation. So, commercial web sites should avoid making negative or critical statements about other persons or products. Similarly, web site designers should avoid any defamation liability when indulged in the alteration or modification of a picture or image of a person. They should not depict such person in derogatory or negative sense.

**Online Privacy**

Issue of online privacy is constantly evolving as internet grows as a tool of communication and commerce. Due to the nature of internet technology, it is possible for web sites to collect information about page viewing habits of visitors, product selection and demographic information (age, gender etc.) about the customers. This may threaten informational privacy rights of such visitors/customers. Cultural difference in different countries is the reason why there are different levels of expectations about privacy in different parts of the world. Many countries have, today, privacy laws such as Canada, European Union (EU) etc. Personal Information Protection and Electronic Documents Act, 2000 (PIPEDA) is the federal law in Canada in this regard. In 1998, the EU adopted a directive on the protection of personal data, which gave the form of law to different constitutional guarantees/rights about privacy existing in most European countries. This is applicable to all internet activities. The directive also prevents businesses from exporting personal data outside EU unless this data is protected in the exporting country according to the provisions of the directive. In the Unites States of America, the government has avoided to introduce any firm privacy regulations. Companies in the U.S.A. are entitled to make policies or devise mechanism to regulate privacy issues themselves. The companies have adopted two different approaches in this regard, that is, opt-out approach and opt-in approach. In more common opt-out approach, the company collecting information assumes that the customer does not object to a specific use of information unless the customer specifically denies the permission. Thus, the company may use the collected information for its own purpose, as well as, sell or rent it out to other firms or persons. In less common opt-in approach, the company collecting information assumes that it cannot use the information for any other purpose except the one for which it is collected. Accordingly, it cannot sell, market, or rent out this information to other firms/persons unless the customer specifically chooses to allow such a use. Experts have highlighted four guiding principles to form the basis of any privacy legislation. These are as follows: collected data may be used for improved customer service; sharing of personal data with outside firms/persons should not be allowed unless the customer consents to that; customers should have the right to receive information about what type of data has been collected from them and in what manner has it been used; customers should have the right to ask for the deletion of any of their data collected by the company.

**Cyber Crimes**

The use of internet technology has given rise to crimes which could not be conceived of a few years ago. Such crimes more suitably called cyber crimes include online fraud, online hate (spreading hatred against a community through internet), cyber-stalking (sending threatening messages using internet), online terrorism, using a computer for launching attacks on other computers etc. Today, many countries of the world are busy in either drafting new laws to deal with the issue of cyber crimes or making suitable amendments in existing criminal code. Again, the issue of territorial jurisdiction is critical in this behalf. For instance, where a Pakistani resident commits a cyber crime against a Canadian resident, the question arises whether or not the Canadian court can take an action against this Pakistani, particularly, where the act of Pakistani is not considered criminal under the Pakistani law.