Module 5: Lecture Guide Part I

Overview:

Businesses that shift their operations and transactions online may, frequently without their knowledge, find themselves subject to new rules and regulations. Online settings continue to lack precise definitions for several fundamental legal notions, such as jurisdiction. The factors of authority, impact, legitimacy, and notice form the basis of the link between physical limits and legal boundaries. Although these factors have contributed to the development of the notion of jurisdiction by governments in the physical world, they take on slightly different shapes online, therefore the jurisdiction norms that are effective in the physical world are not always applicable there.

Client devices may be at danger from active content in browser plugins, attacks (such as viruses, Trojan horses, and worms) sent through email or Web browsing, assaults launched from other devices connected to the same network, or any combination of these threats. A crucial component in the safety of client computers is antivirus software.

For online businesses, the use and protection of intellectual property are crucial challenges. These businesses must take care to prevent trademark, copyright, or patent infringement as well as defamation and the violation of privacy or publicity rights. An international administrative process that essentially eliminates the need for litigation to settle domain name disputes. Given the subjective nature of defamation and product disparagement, online firms must avoid suggesting relationships that do not exist and providing negative evaluations of entities, even when genuine.

Unfortunately, some people use the Internet to commit crimes, support terrorism, and even start wars. Governments are working to develop sufficient defenses for internet conflict and terrorism since law enforcement authorities have found it difficult to resist many sorts of online crime.

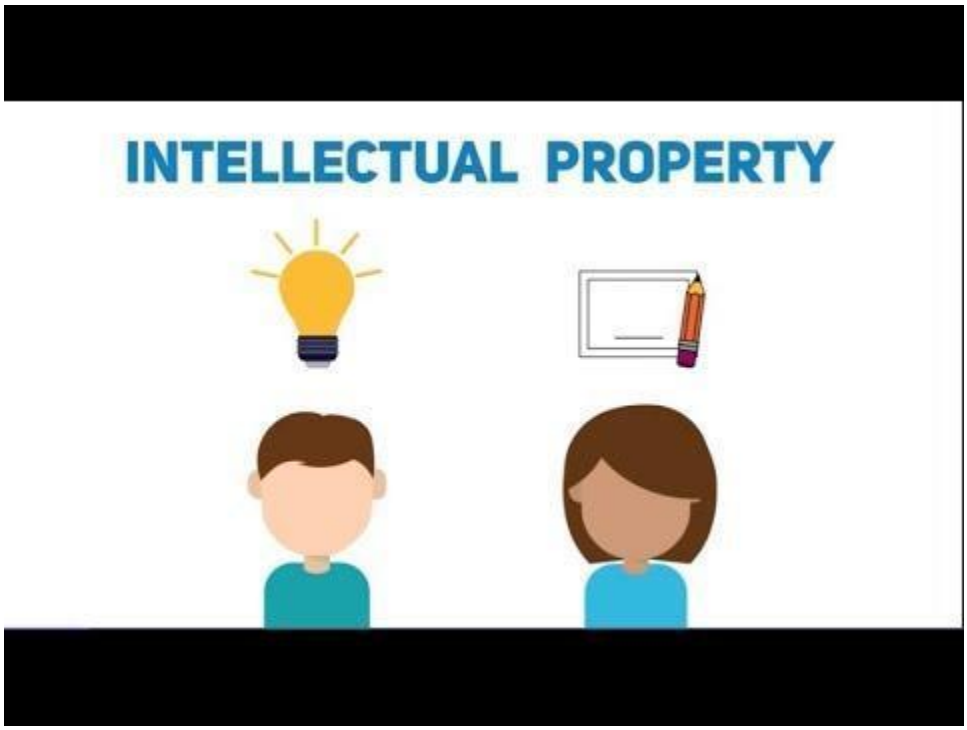
It is simple for internet firms to track client information, including online behavior, and the use of this data has sparked ethical debates over online privacy. Some nations have significantly tighter restrictions on the collecting of information than do others. Businesses that gather personal data may utilize either an opt-in or an opt-out policy. Customers' privacy rights are better protected by opt-in procedures. Many businesses have increased security and threat testing because of the rise in data breaches that expose consumer and employee data. When interacting with minors online, companies must exercise caution. Most nations' laws mandate that parental approval must be acquired before collecting any data from children under the age of 13.

The rules and taxes that apply to offline businesses also apply to online firms, but because of the nature of doing business online, organizations may be subject to many more regulations and

taxes earlier and in unexpected ways. The global reach of all online commerce can make a company's tax duties more challenging. Online businesses must be aware of the potential risks associated with doing business with clients in those jurisdictions because there are so many governmental entities with the authority to tax and exercise jurisdiction over them.

Online Business Uses and Protects Intellectual Property

Intellectual property must be used with care by online firms. All creations of the human mind are included in the broad category of intellectual property. These goods may be physical or abstract. The protections provided by governments to people and businesses through the issuance of copyrights, patents, and the registration of trademarks and service marks are referred to as intellectual property rights. People may have the limited right to control how their name, appearance, likeness, or other identifying characteristics are used for commercial purposes depending on where they live. Although this right is recognized in the majority of US states, it is constrained by the First Amendment of the US Constitution.



Online companies must exercise caution when employing unlicensed content on their websites or in their domain names to prevent unfair trade practices, misleading advertising claims, defamation or product disparagement, and intellectual property rights violations. The content of Web pages on websites that conduct electronic commerce may give rise to a number of legal difficulties. The use of intellectual property that is covered by copyrights, patents, trademarks, and service marks belonging to other people is the most frequently raised concern.

The video below goes into deeper with IP:

Domain Names and Intellectual Property Issues

Regarding intellectual property rights and Internet domain names, there is a great deal of debate. The process of registering a domain name that is a trademark of another person or business is known as "cybersquatting," and it is done in the hopes that the owner would pay a hefty sum of money to get the URL. Successful cybersquatters can also charge hefty advertising charges due to their huge site traffic. It is not cybersquatting to register a generic domain name like Wine.com in the hopes that it may one day be worth anything. It is entirely permissible to speculate.

When someone registers purposefully misspelled variations of well-known domain names, a related issue known as name altering (also known as typosquatting) arises. These variations occasionally seduce customers who enter URLs incorrectly. For instance, typing Nikke.com instead of Nike.com is a simple way for someone to go on a fake Web page.

Since 1999, the U.S. Anticybersquatting Consumer Protection Act has prohibited third parties from registering the trademarked names of companies as domain names. The statute allows for up to $100,000 in damages per trademark. Damages might reach $300,000 if the unauthorized domain name registration is shown to have been "willful."

The World Intellectual Property Organization resolves disputes that emerge when one person registers a domain name that is a brand or corporate name that already exists (WIPO). Under its Uniform Domain Name Dispute Resolution Policy, WIPO started resolving domain name disputes in 1999. (UDRP). Due to issues with international jurisdiction, it was difficult and

ineffective to enforce laws through national courts. Being a worldwide body, WIPO is able to provide decisions that are applicable in a multi-national online commercial context.

When a company uses a common phrase in its trademark, disputes may result. The owner of the trademark must file a complaint with WIPO if someone manages to register a domain name using that widely used term. WIPO rules in favor of the trademark owner in more than 90% of its disputes, although a victory is never guaranteed.

Online Crime, Terrorism, and Warfare

Although the Internet has had some positive effects, such as making it possible for individuals who are separated by distance to contact and get to know one another better and opening up new economic opportunities, it has also been abused. The Internet has been used by some people in our world to commit crimes, carry out terrorism, and even wage war.

Take some time and read the following the article, "Cyber Security To Safeguard Cyber Attacks" and be ready to discuss in small groups or a whole class discussion.

Ethical Issues:

Businesses that use websites to conduct electronic trade should uphold the same moral principles that other companies do. If they do not, they will experience the same problems that all businesses do: a tarnished reputation, a sustained loss of trust, and maybe a reduction in business. Any advertising or promotion on the Web should only contain factual assertions and avoid any information that can deceive potential customers or incorrectly affect how they perceive a product or service. When the advertisement omits essential connected facts, even factual statements have been found to be deceptive. Verifiable data should always be used to support any product comparisons.

How an organization controls the use of the e-mail addresses and associated information is a crucial ethical dilemma that businesses have when they gather email addresses from website users. Few businesses made any commitments to users who gave this information in the early days of the Web. The majority of websites today make their protection of visitor information policies clear, however many do not. Organizations are not required by law to restrict how they utilize the data they gather on their websites in the United States. They are free to use the data however they see fit, even selling it to other businesses. Many people and privacy rights supporters are concerned about the lack of government regulation that would protect visitor information.

The issue of online privacy is continuing to evolve as the Internet and the Web grow in importance as tools of communication and commerce. Many legal and privacy issues remain unsettled and are hotly debated in various forums.

In the United States, a number of laws have been enacted that address online privacy issues, but none have survived constitutional challenges.

Because laws have not kept up with the expansion of the Internet and the Web, ethical concerns are important in the realm of online privacy. The type and extent of personal information that websites may gather about users' product preferences, page browsing patterns, and demographic data may pose a danger to users' right to privacy. This is especially true when businesses lose control of the client data they acquire (and other people). Numerous businesses have garnered media attention over the years for allowing the dissemination of private information about individuals without their consent.

The incidence of security lapses resulting in the loss of personal data keeps rising.

Because it enables anyone, wherever in the world, to gather data online in numbers that were previously unthinkable, the Internet has also challenged conventional beliefs about privacy. For instance, in the United States, real estate transactions are public information. For many years, these transactions were recorded in county records and were accessible to anyone who chose to visit the office of the county recorder and spend hours poring through massive books filled with handwritten data. A researcher can now review thousands of real estate transaction records in hours without visiting a single county office because many counties have made these documents online accessible. Many privacy experts see this change in the ease of data access to be an important shift that affects the privacy rights of those who participate in real estate transactions. Because the Internet makes such data more readily available to a wider range of people, the privacy previously afforded to the participants in those transactions has been reduced.

A prime example of this is in the following article: Black couple sues after they say home valuation rises nearly $300,000 when shown by White colleague

Different expectations on privacy in electronic commerce have arisen as a result of cultural diversity around the world. For instance, most people in Europe anticipate that the information they give to a commercial Web site would only be used for the intended purpose. Numerous European nations have regulations that forbid businesses from sharing customer data without the customer's express consent.

Opt-in versus opt-out is one of the most contentious privacy issues in the US today. The majority of businesses that collect personal information while conducting business online would like to be permitted to utilize that information anyway they see fit. Some businesses would also appreciate the option of renting or selling that information to other businesses. Currently, no regulation in the United States restricts how these data are used by businesses. Additionally, businesses are typically free to sell or rent client information. A growing number of American businesses do provide customers the option to limit how their personal information is used. The opt-out strategy is currently the most often adopted policy in American businesses. If a consumer explicitly chooses to withhold consent, the firm collecting the information will assume that the customer does not object to the company's use of the information (that is, to opt out of having their information used). The less popular opt-in approach prohibits the entity collecting the information from using the data for any other purposes (or from selling or renting the data) unless the client expressly agrees to do so (that is, to opt in and grant permission for the use).

The following article by Fletcher (2022) emphasizes the importance on privacy concerns: Why-the-ethical-use-of-data-and-user-privacy-concerns-matter. Be prepared to discuss the article in small groups or as a whole class discussion.

Communications with Children

When children visit websites and communicate with such websites in any way, a new set of privacy issues come into play. Adults who use websites have the ability to read privacy policies and decide for themselves whether or not to give the site their personal information. A crucial component of doing electronic commerce is the exchange of private information, such as credit card numbers, shipping addresses, and other details. Children are considered to be less capable than adults in judging information sharing and transaction risks by the majority of legislation and ethical frameworks. As a result, rules in the real world restrict or prohibit youngsters from signing documents, getting married, operating motor vehicles, and going into specific locations.

Children are thought to be less able (or incapable) to weigh the dangers of various activities while making decisions. Similar to this, many people worry about kids' capacity to read, assess, and subsequently consent to supplying personal information to Web sites. The majority of social media platforms employ software that checks each user's registration information against a database of known sex offenders and deletes any matches. Despite these protections, most experts concur that nothing technological will ever offer the same level of security as parental monitoring of their children's online activity.