Unit 4: Intellectual Property

Syllabus:

Unit 4: Intellectual Property (8 Hrs.)
Intellectual Property, Copyright; Patient; Trade Secrets; Intellectual Property Issues: Plagiarism, Reverse Engineering, Open Source Code, Competitive Intelligence, Trademark Infringement, and Cybersquatting

==========

Intellectual Property

Intellectual property is a term used to describe works of the mind—such as art, books, films, formulas, inventions, music, and processes—that are distinct and owned or created by a single person or group. It 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 laws form a complex body of law that addresses the ownership of intellectual property. Such laws can also present potential ethical problems for IT companies and users—for example, some innovators believe that copyrights, patents, and trade secrets stifle creativity by making it harder to build on the ideas of others. Meanwhile, the owners of intellectual property want to control and receive compensation for the use of their intellectual property. Should the need for ongoing innovation or the rights of property owners govern how intellectual property is used?

Defining and controlling the appropriate level of access to intellectual property are complex tasks. For example, protecting computer software has proven to be difficult because it has not been well categorized under the law. Software has sometimes been treated as the expression of an idea, which can be protected under copyright law. In other cases, software has been treated as a process for changing a computer's internal structure, making it eligible for protection under patent law. At one time, software was even judged to be a series of mental steps, making it inappropriate for ownership and ineligible for any form of protection.

Copyright

Copyright and patent protection was established through the U.S. Constitution, Article I, section 8, clause 8, which specifies that Congress shall have the power "to promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Rights to their respective Writings and Discoveries."

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 protection is granted to the creators of "original works of authorship in any tangible medium of expression, now known or later developed, from which they can be perceived, reproduced, or otherwise communicated, either directly or with the aid of a machine or device."

The author may grant this exclusive right to others. As new forms of expression develop, they can be awarded copyright protection. For example, in the Copyright Act of 1976, audio-visual works were given protection, and computer programs were assigned to the literary works category.

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. The courts have a wide range of discretion in awarding damages—from $200 for innocent infringement to $100,000 for wilful infringement.

The Copyright Term Extension Act, also known as the Sonny Bono Copyright Term Extension Act (after the legislator, and former singer/entertainer, who was one of the cosponsors of the bill in the House of Representatives), signed into law in 1998, and established the following time limits:

- For works created after January 1, 1978, copyright protection endures for the life of the author plus 70 years.
- For works created but not published or registered before January 1, 1978, the term endures for the life of the author plus 70 years, but in no case expires earlier than December 31, 2004.
- For works created before 1978 that are still in their original or renewable term of copyright, the total term was extended to 95 years from the date the copyright was originally secured.

These extensions were primarily championed by movie studios concerned about retaining rights to their early films. Opponents argued that extending the copyright period made it more difficult for artists to build on the work of others, thus stifling creativity and innovation. The Sonny Bono Copyright Term Extension Act was legally challenged by Eric Eldred, a bibliophile who wanted to put digitized editions of old books online. The Eldred v. Ashcroft case went all the way to the Supreme Court, which ruled the act constitutional in 2003.8

Eligible Works

The types of work that can be copyrighted include architecture, art, audio-visual works, choreography, drama, graphics, literature, motion pictures, music, pantomimes, pictures, sculptures, sound recordings, and other intellectual works, as described in Title 17 of the U.S. Code.

To be eligible for a copyright, a work must fall within one of the preceding categories, and it must be original. Copyright law has proven to be extremely flexible in covering new technologies; thus, software, video games, multimedia works, and web pages can all be protected.

Fair Use Doctrine

Copyright law tries to strike a balance between protecting an author's rights and enabling public access to copyrighted works. The fair use doctrine was developed over the years as courts worked to maintain that balance. It allows portions of copyrighted materials to be used without permission under certain circumstances. Title 17, Section 107, of the U.S. Code established that courts should consider the following four factors when deciding whether a particular use of copyrighted property is fair and can be allowed without penalty:

1. The purpose and character of the use (such as commercial use or non-profit, educational purposes)
2. The nature of the copyrighted work
3. The portion of the copyrighted work used in relation to the work as a whole
4. The effect of the use on the value of the copyrighted work.

The concept that an idea cannot be copyrighted but the expression of an idea can be key to understanding copyright protection. For example, an author cannot copy the exact words that someone else used to describe his feelings during a skirmish with terrorists, but he can convey the sense of horror that the other person expressed. Also, there is no copyright infringement if two parties independently develop a similar or even identical work. For example, if two writers happened to use the same phrase to describe a key historical figure, neither would be guilty of infringement. Of course, independent creation can be extremely difficult to prove or disprove.

Since 2004, Google has scanned and converted into machine readable form over 20 million books as part of a project to create an electronic searchable database of books. Users of the Google Books service can enter search queries and view full pages from books in which the search terms appear, provided that either the book is out of copyright or the copyright owner has given permission for the work to be included in the database. If the book is still under copyright, a user sees "snippets" of text around the queried search terms. The Authors Guild, a professional organization that advocates for authors on issues of copyright, fair contracts, and free speech, sued Google saying that serving up search results from scanned books infringes on publishers' copyrights. In April 2016, the Supreme Court let stand a lower court decision that rejected the writers' claims on the basis that such usage represented no infringing fair use. The ruling allows Google to continue with its scanning project and may encourage other digitization projects.

Software Copyright Protection

The use of copyrights to protect computer software raises many complicated issues of interpretation. For example, 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.

To prove infringement, the copyright holder must show a striking resemblance between its software and the new software that could be explained only by copying. However, if the new software's manufacturer can establish that it developed the program on its own, without any knowledge of the existing program, there is no infringement. For example, two software manufacturers could conceivably develop separate but nearly identical programs for a simple game such as tic-tac-toe without infringing the other's copyright.

The Prioritizing Resources and Organization for Intellectual Property Act of 2008

The Prioritizing Resources and Organization for Intellectual Property (PRO-IP) Act of 2008 created the position of Intellectual Property Enforcement Coordinator within the Executive Office of the President. It also increased trademark and copyright enforcement and substantially increased penalties for infringement. One of its programs, called Computer Hacking and Intellectual Property (CHIP), is a network of over 150 experienced and specially trained federal prosecutors who focus on computer and intellectual property crimes.

General Agreement on Tariffs and Trade

The General Agreement on Tariffs and Trade (GATT) was a multilateral agreement governing international trade. There were several rounds of negotiations addressing various trade issues. The Uruguay Round, completed in December 1993, resulted in a trade agreement among 117 countries. This agreement also created the World Trade Organization (WTO) in Geneva, Switzerland, to enforce compliance with the agreement.

GATT includes a section covering copyrights called the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS). The U.S. intellectual property law was amended to be essentially consistent with GATT through both the Uruguay Round Agreements Act of 1994 and the Sonny Bono Copyright Term Extension Act of 1998. Despite GATT, however, copyright protection varies greatly from country to country, and an expert should be consulted when considering international usage of any intellectual property.

The World Intellectual Property Organization Copyright Treaty (1996)

The World Intellectual Property Organization (WIPO), headquartered in Geneva, Switzerland, is an agency of the United Nations established in 1967. WIPO is dedicated to "**the use of intellectual property as a means to stimulate innovation and creativity."** It has 185 member nations and administers 25 international treaties. Since the 1990s, WIPO has strongly advocated for the interests of intellectual property owners. Its goal is to ensure that intellectual property laws are uniformly administered.

Patents

A patent is a grant of a property right issued by the U.S. Patent and Trademark Office (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. Even if someone else invents the same item independently and with no prior knowledge of the patent holder's invention, the second inventor is excluded from using the patented device without permission of the original patent holder. The rights of the patent are valid only in the United States and its territories and possessions.

There are six types of patents, with the two of main concern to information technology firms being the utility patent and the design patent.

A utility patent is "issued for the invention of a new and useful process, machine, manufacture, or composition of matter, or a new and useful improvement thereof, it generally permits its owner to exclude others from making, using, or selling the invention for a period of up to twenty years from the date of patent application filing, subject to the payment of maintenance fees." According to the USPTO, approximately 90 percent of the patent documents issued in recent years have been utility patents.

A design patent, which is "issued for a new, original, and ornamental design embodied in or applied to an article of manufacture," permits its owner to exclude others from making, using, or selling the design in question.

Design patents issued from applications filed on or after May 13, 2015, are granted for a term of 15 years from the date of grant. Design patents issued from applications filed before May 13, 2015, were granted for a term of 14 years from the date of grant.

Leahy-Smith America Invents Act (2011)

Under this law, the U.S. patent system changed from a "first-to-invent" to a "first-inventor-to-file" system effective from March 16, 2013. That means if two people file for a patent application on the same invention at approximately the same time, the first person to file with the USPTO will receive the patent, not necessarily the person who actually invented the item first.

Software Patents

A software patent claims as its invention some feature or process embodied in instructions executed by a computer. The courts and the USPTO have changed their attitudes and opinions on the patenting of software over the years. Prior to 1981, the courts regularly turned down requests for such patents, giving the impression that software could not be patented.

In the 1981 Diamond v. Diehr case, the Supreme Court granted a patent to Diehr, who had developed a process control computer and sensors to monitor the temperature inside a rubber mold. The USPTO interpreted the court's reasoning to mean that just because an invention used software did not mean that the invention could not be patented. Based on this ruling, courts have slowly broadened the scope of protection for software-related inventions.

As a result, during the 1980s and 1990s, the USPTO granted thousands of software-related patents per year. Application software, business software, expert systems, and system software were patented, along with such software processes as compilation routines, editing and control functions, and operating system techniques. Many patents were granted for business methods implemented in software.

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, eventually leading the U.S. International Trade Committee (ITC) to ban imports of two models of the HTC mobile phone. Following that ruling by the ITC, the two companies agreed to a 10-year cross-licensing agreement that permits each party to license the other's current and future patents.

In 2016, IBM entered into cross-licensing arrangements with Western Digital covering some 100 patents in the area of distributed storage systems and nonvolatile memory devices. In 2014, Twitter acquired 900 IBM patents, and in 2011, Google acquired more than 2,000 IBM patents in cross-licensing deals.

TRADE SECRETS

A trade secret is defined as 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.

Trade secret law protects only against the misappropriation of trade secrets. If competitors come up with the same idea on their own, it is not misappropriation; in other words, the law doesn't prevent someone from using the same idea if it was developed independently.

Trade secret laws protect more technology worldwide than patent laws do, in large part because of the following key advantages:

- There are no time limitations on the protection of trade secrets, as there are with patents and copyrights.
- There is no need to file an application, make disclosures to any person or agency, or disclose a trade secret to outsiders to gain protection. (After the USPTO issues a patent, competitors can obtain a detailed description of it.) Hence, no filing or application fees are required to protect a trade secret.
- Although patents can be ruled invalid by the courts, meaning that the affected inventions no longer have patent protection, this risk does not exist for trade secrets.

Trade Secret Laws

Trade secret protection laws vary greatly from country to country. For example, the Philippines provides no legal protection for trade secrets. In some European countries, pharmaceuticals, methods of medical diagnosis and treatment, and information technology cannot be patented.

Many Asian countries require foreign corporations operating there to transfer rights to their technology to locally controlled enterprises. (Coca-Cola reopened its operations in India in 1993 after halting sales for 16 years to protect the "secret formula" for its soft drink, even though India's vast population represented a huge potential market.)

Uniform Trade Secrets Act

The Uniform Trade Secrets Act (UTSA) was drafted in the 1970s to bring uniformity to all the United States in the area of trade secret law. The UTSA defines a trade secret as "information, including a formula, pattern, compilation, program, device, method, technique, or process, that:

- Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by, persons who can obtain economic value from its disclosure or use, and
- Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy."

Under these terms, computer hardware and software can qualify for trade secret protection by the UTSA.

The Economic Espionage Act

The Economic Espionage Act (EEA) of 1996 imposes penalties of up to $10 million and 15 years in prison for the theft of trade secrets. Before the EEA, there was no specific criminal statute to help law enforcement agencies pursue economic espionage; the FBI was investigating nearly 800 such cases in 23 countries when the EEA was enacted.

Defend Trade Secrets Act of 2016

The Defend Trade Secrets Act of 2016 (DTSA) amended the EEA to create a federal civil remedy for trade secret misappropriation. Prior to its enactment, civil claims for trade secret misappropriation were primarily governed by state law. In one such case, Sergey Aleynikov was found guilty under New York state law of theft of trade secrets.

Aleynikov—a Goldman Sachs programmer who left the firm in 2007 to take a job paying $1.2 million annually with Teza Technologies, a group of widely recognized experts in quantitative trading—admitted copying Goldman's high frequency trading code before he resigned but claimed the files were intended only as research for his new job.

His initial convictions under the EEA were reversed after Aleynikov spent a year in federal prison; however, new charges brought in New York state court resulted in Aleynikov being found guilty of the unlawful use of secret scientific material under New York's penal code . Aleynikov could be sentenced to up to four years in prison. Although Aleynikov was found guilty under New York state law, the wide variety in state statues governing trade secret misappropriation prior to the passage of DTSA created great uncertainty in the application of trade secret law across the United States.

DTSA broadly defines misappropriation to include disclosure or use of a trade secret without express or implied consent or acquisition of a trade secret by anyone with reason to know the trade secret was acquired by theft, bribery, misrepresentation, breach or inducement of a breach of duty to maintain secrecy, or espionage through electronic or other means. However, reverse engineering and independent derivation are not considered improper. The act also allows for seizure of property under certain conditions to prevent dissemination of the misappropriated trade secret.

Employees and Trade Secrets

Employees are the greatest threat to the loss of company trade secrets—they might accidentally disclose trade secrets or steal them for monetary gain. Organizations must educate employees about the importance of maintaining the secrecy of corporate information. Trade secret information should be labelled clearly as confidential and should only be accessible by a limited number of people. Most organizations have strict policies regarding nondisclosure of corporate information.

Because organizations can risk losing trade secrets when key employees leave, they often try to prohibit employees from revealing secrets by adding nondisclosure clauses to employment contracts. Thus, departing employees cannot take copies of computer programs or reveal the details of software owned by the firm.

Defining reasonable nondisclosure agreements can be difficult, as seen in the following example involving Apple. In addition to filing hundreds of patents on iPhone technology, the firm put into place a restrictive nondisclosure agreement to provide an extra layer of protection. Many iPhone

developers complained bitterly about the tough restrictions, which prohibited them from talking about their coding work with anyone not on the project team and even prohibited them from talking about the restrictions themselves. Eventually, Apple admitted that its nondisclosure terms were overly restrictive and loosened them for iPhone software that was already released.

Employers can also use noncompete agreements to protect intellectual property from being used by competitors when key employees leave. A noncompete agreement prohibits an employee from working for any competitors for a period of time, often one to two years. When courts are asked to settle disputes over noncompete agreements, they must weigh several factors. First, they must consider the reasonableness of the restriction and how it protects confidential and trade secret information of the former employer. Second, they must weigh the employee's right to work and seek employment in the area where the employee has gained skill, experience, and business contacts. The courts also consider geographic area and the length of time of the restriction in relation to the pace of change in the industry.

Most states only enforce such noncompete agreements to the extent required to shelter the employer's legitimate confidential business interests. However, there is a wide range of treatment on noncompete agreements among the various states. For example, Ohio is highly supportive of former employers enforcing noncompete agreements while noncompete agreements are not as strictly enforced in California.

Current Intellectual Property Issues

Here we discuss several issues that apply to intellectual property and information technology are…

1. Plagiarism
2. Reverse engineering
3. Open source code
4. Competitive intelligence
5. Trademark infringement, and
6. Cybersquatting.

Plagiarism

Plagiarism is the act of stealing someone's ideas or words and passing them off as one's own. The explosion of electronic content and the growth of the web have made it easy to cut and paste paragraphs into term papers and other documents without proper citation or quotation marks. To compound the problem, hundreds of online "paper mills" enable users to download entire term papers. Although some sites post warnings that their services should be used for research purposes only, many users pay scant heed. As a result, plagiarism has become an issue from elementary schools to the highest levels of academia. Plagiarism also occurs outside academia. Popular literary authors, playwrights, musicians, journalists, and even software developers have been accused of it.

Turnitin, a software product developed by California-based iParadigms, supports 15 languages and is used by over 10,000 educational institutions around the world. It uses three primary databases for content matching with over 58 billion web pages, some 570 million archived student papers, and 150 million articles from over 110,000 journals, periodicals, and books. iThenticate is available from the same company that created Turnitin, but it is designed to meet the needs of members of the information industry, such as publishers, research facilities, legal firms, government agencies, and financial institutions.

The following list shows some of the actions that schools can take to combat student plagiarism:

- Help students understand what constitutes plagiarism and why they need to cite sources properly.
- Show students how to document web pages and materials from online databases.
- Schedule major writing assignments so that portions are due over the course of the term, thus reducing the likelihood that students will get into a time crunch and be tempted to plagiarize to meet the deadline.
- Make clear to students that instructors are aware of Internet paper mills.
- Ensure that instructors both educate students about plagiarism detection services and make them aware that they know how to use these services.
- Incorporate detection software and services into a comprehensive antiplagiarism program.

Plagiarism can also be an issue in the field of software development. Measure of Software Similarity (MOSS) is software used to measure the similarities among computer programs written in languages such as Ada, C, C++, Java, Lisp, and Paschal. MOSS is used to detect plagiarism in computer programming classes and commercial software.

Reverse Engineering

Reverse engineering is the process of taking something apart in order to understand it, build a copy of it, or improve it. It was originally applied to computer hardware but is now commonly applied to software as well. Reverse engineering of software involves analysing it to create a new representation of the system in a different form or at a higher level of abstraction. Often, reverse engineering begins by extracting design-stage details from program code. Design-stage details about an information system are more conceptual and less defined than the program code of the same system. Microsoft has been accused repeatedly of reverse engineering products—ranging from the Apple Macintosh user interface to many Apple operating system utility features that were incorporated into DOS (and later Windows), to early word-processing and spreadsheet programs that set the design for Word and Excel, to Google's methods for improving search results for its Bing search engine.

One frequent use of reverse engineering for software is to modify an application that ran on one vendor's database so that it can run on another's (e.g., from Access to Oracle). Database management systems use their own programming language for application development. As a result, organizations that want to change database vendors are faced with rewriting existing applications using the new vendor's database programming language. The cost and length of time required for this redevelopment can deter an organization from changing vendors and deprive it of the possible benefits of converting to an improved database technology.

Using reverse engineering, a developer can use the code of the current database programming language to recover the design of the information system application. Next, code-generation tools can be used to take the design and produce code (forward engineer) in the new database programming language. This reverse-engineering and codegenerating process greatly reduces the time and cost needed to migrate the organization's applications to the new database management system. No one challenges the right to use this process to convert applications developed in-house. After all, those applications were developed and are owned by the companies using them. It is quite another matter, however, to use this process on a purchased software application developed and licensed by outside parties. Most IT managers would consider this action unethical because the software user does not actually own the right to the software. In addition, a number of intellectual property issues would be raised, depending on whether the software was licensed, copyrighted, or patented.

A compiler is a language translator that converts computer program statements expressed in a source language (such as Java, C, C++, and COBOL) into machine language (a series of binary codes of 0s and 1s) that the computer can execute. When a software manufacturer provides a customer with its software, it usually provides the software in machine-language form. Tools called reverse-engineering compilers, or decompilers, can read the machine language and produce the source code. For example, Reverse Engineering Compiler (REC) is a decompiler that reads an executable, machine-language file and produces a C-like representation of the code used to build the program.

Decompilers and other reverse-engineering techniques can be used to reveal a competitor's program code, which can then be used to develop a new program that either duplicates the original or interfaces with the program. Thus, reverse engineering provides a way to gain access to information that another organization may have copyrighted or classified as a trade secret.

The courts have ruled in favor of using reverse engineering to enable interoperability. In the early 1990s, video game maker Sega developed a computerized lock so that only Sega video cartridges would work on its entertainment systems. This essentially shut out competitors from making software for the Sega systems. Sega Enterprises Ltd. v. Accolade, Inc. dealt with rival game maker Accolade's use of a decompiler to read the Sega software source code. With the code, Accolade could create new software that circumvented the lock and ran on Sega machines. An appeals court ultimately ruled that if someone lacks access to the unprotected elements of an original work and has a "legitimate reason" for gaining access to those elements, disassembly of a copyrighted work

is considered to be a fair use under section 107 of the Copyright Act. The unprotected element in this case was the code necessary to enable software to interoperate with the Sega equipment. The court reasoned that to refuse someone the opportunity to create an interoperable product would allow existing manufacturers to monopolize the market, making it impossible for others to compete. This ruling had a major impact on the video game industry, allowing video game makers to create software that would run on multiple machines.

Software license agreements increasingly forbid reverse engineering. As a result of the increased legislation affecting reverse engineering, some software developers are moving their reverse-engineering projects offshore to avoid U.S. rules.

The ethics of using reverse engineering are debated. Some argue that its use is fair if it enables a company to create software that interoperates with another company's software or hardware and provides a useful function. This is especially true if the software's creator refuses to cooperate by providing documentation to help create interoperable software. From the consumer's standpoint, such stifling of competition increases costs and reduces business options. Reverse engineering can also be a useful tool in detecting software bugs and security holes.

Others argue strongly against the use of reverse engineering, saying it can uncover software designs that someone else has developed at great cost and taken care to protect. Opponents of reverse engineering contend it unfairly robs the creator of future earnings and significantly reduces the business incentive for software development.

Open Source Code

Historically, the makers of proprietary software have not made their source code available, but not all developers share that philosophy. 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.

A considerable amount of open source code is available, and an increasing number of organizations use open source code. For example, much of the Internet runs on open source code; when you access a web page, send a text, or post a status update, you are likely using an open source program such as Linux, Apache HTTP, PHP, Perl, Python, or Ruby.

TABLE 6-3 Commonly used open source software

Open source web browsers	Open source database management systems	Open source accounting applications
Chrome	MySQL	GnuCash
Firefox	PostgreSQL	SQL Ledger
Opera	SQLite	X Tuple PostBooks
Chromium	MongoDB	Compiere
Midori	Cubrid	Turbo Cash
QupZilla	MariaDB	KashFlow

Reasons that firm or individual developers create open-source code, even though they do not receive money for it, include the following:

- Some people share code to earn respect for solving a common problem in an elegant way.
- Some people have used open-source code that was developed by others and feel the need to pay back by helping other developers.
- A firm may be required to develop software as part of an agreement to address a client's problem. If the firm is paid for the employees' time spent to develop the software rather than for the software itself, it may decide to license the code as open source and use it either to promote the firm's expertise or as an incentive to attract other potential clients with a similar problem.
- A firm may develop open source code in the hope of earning software maintenance fees if the end user's needs change in the future.
- A firm may develop useful code but may be reluctant to license and market it, and so might donate the code to the general public.

There are various definitions of what constitutes open-source code, each with its own idiosyncrasies. The GNU General Public License (GPL) was a precursor to the open-source code defined by the Open-Source Initiative (OSI). GNU is a computer operating system comprised entirely of free software; its name is a recursive acronym for GNUs Not Unix. The GPL is intended to protect GNU software from being made proprietary, and it lists terms and conditions for copying, modifying, and distributing free software. The OSI is a non-profit organization that advocates for open source and certifies open source licenses. Its certification mark, "OSI Certified," may be applied only to software distributed under an open source license that meets OSI criteria, as described at its website, www .opensource.org.

A software developer could attempt to make a program open source simply by putting it into the public domain with no copyright. This would allow people to share the program and their improvements, but it would also allow others to revise the original code and then distribute the

resulting software as their own proprietary product. Users who received the program in the modified form would no longer have the freedoms associated with the original software. Use of an open-source license avoids this scenario.

Competitive Intelligence

Competitive intelligence is legally obtained information that is gathered to help a company gain an advantage over its rivals. For example, some companies have employees who monitor the public announcements of property transfers to detect any plant or store expansions of competitors. An effective competitive intelligence program requires the continual gathering, analysis, and evaluation of data with controlled dissemination of useful information to decision makers.

Competitive intelligence is often integrated into a company's strategic plan and executive decision making. Competitive intelligence is not the same as industrial espionage, which is the use of illegal means to obtain business information not available to the general public. In the United States, industrial espionage is a serious crime that carries heavy penalties.

Almost all the data needed for competitive intelligence can be collected from examining published information or interviews, as outlined in the following list:

- 10-K or annual reports
- An SC 13D acquisition—a filing by shareholders who report owning more than five percent of common stock in a public company
- 10-Q or quarterly reports
- Press releases
- Promotional materials
- Websites
- Analyses by the investment community, such as a Standard & Poor's stock report
- Interviews with suppliers, customers, and former employees
- Calls to competitors' customer service groups
- Articles in the trade press
- Environmental impact statements and other filings associated with a plant expansion or construction
- Patents

Trademark Infringement

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 (also known as the Trademark Act, Title 15, of the U.S. Code) defines the use of a trademark, the process for obtaining a trademark from the USPTO, and the penalties associated with trademark infringement. The law gives the trademark's owner the right to prevent others from using the same mark or a confusingly similar mark on a product's label.

The United States has a federal system that stores trademark information; merchants can consult this information to avoid adopting marks that have already been taken. Merchants seeking trademark protection apply to the USPTO if they are using the mark in interstate commerce or if they can demonstrate a true intent to do so. Trademarks can be renewed forever—as long as a mark is in use.

It is not uncommon for an organization that owns a trademark to sue another organization over the use of that trademark in a website or a domain name. The court rulings in such cases are not always consistent and are quite difficult to judge in advance.

Nominative fair use is a defense often employed by the defendant in trademark infringement cases in which a defendant has used a plaintiff's mark to identify the plaintiff's products or services in conjunction with its own product or services. To successfully employ this defence, the defendant must show three things:

- that the plaintiff's product or service cannot be readily identifiable without using the plaintiff's mark,
- that it uses only as much of the plaintiff's mark as necessary to identify the defendant's product or service, and
- that the defendant does nothing with the plaintiff's mark that suggests endorsement or sponsorship by the plaintiff.

This defence was first applied to websites in Playboy Enterprises, Inc. v. Terri Welles. Welles was the Playboy™ Playmate of the Year™ in 1981. In 1997, she created a website to offer free photos of herself, advertise the sale of additional photos, solicit memberships in her photo club, and promote her spokeswoman services. Welles used the trademarked terms and Playmate of the Year to describe herself on her website. The Ninth Circuit Court of Appeals determined that the former Playboy model's use of trademarked terms was permissible, nominative use. By using the nominative fair use defense, Welles avoided a motion for preliminary injunction, which would have restrained her from continuing to use the trademarked terms on her website.

Cybersquatting

Companies that want to establish an online presence know that the best way to capitalize on the strengths of their brand names and trademarks is to make the names part of the domain names for their websites. When websites were first established, there was no procedure for validating the legitimacy of requests for website names, which were given out on a first-come, first-served basis. And in the early days of the web, many cybersquatters registered domain names for famous trademarks or company names to which they had no connection, with the hope that the trademark's owner would eventually buy the domain name for a large sum of money.

The main tactic organizations use to circumvent cybersquatting is to protect a trademark by registering numerous domain names and variations as soon as the organization knows it wants to develop a web presence (e.g., UVXYZ.com, UVXYZ.org, and UVXYZ.info). In addition, trademark owners who rely on non-English-speaking customers often register their names in multilingual form. Registering additional domain names is far less expensive than attempting to force cybersquatters to change or abandon their domain names.

Other tactics can also help curb cybersquatting. For example, the **Internet Corporation for Assigned Names and Numbers (ICANN)** is a non-profit corporation responsible for managing the Internet's domain name system. Prior to 2000, eight generic top-level domain names were in existence: .com, .edu, .gov, .int, .mil, .net, .org, and .arpa.

In 2000, ICANN introduced seven more: .aero, .biz, .coop, .info, .museum, .name, and .pro. In 2004, ICANN introduced .asia, .cat, .mobi, .tel, and .travel. The generic top-level domain .xxx was approved in 2011. With each new round of generic top-level domains, current trademark holders are given time to assert rights to their trademarks in the new top-level domains before registrations are opened up to the general public. As of March 2016, there were 882 top-level domain names, which can be found at http://blog.europeandomaincentre .com/list-of-domain-extensions/#.

ICANN also has a Uniform Domain-Name Dispute-Resolution Policy, under which most types of trademark-based domain name disputes must be resolved by agreement, court action, or arbitration before a registrar will cancel, suspend, or transfer a domain name.

The ICANN policy is designed to provide for the fast, relatively inexpensive arbitration of a trademark owner's complaint that a domain name was registered or used in bad faith.

The Anticyber squatting Consumer Protection Act (ACPA), enacted in 1999, allows trademark owners to challenge foreign cyber squatters who might otherwise be beyond the jurisdiction of U.S. courts. Also under this act, trademark holders can seek civil damages of up to $100,000 from cybersquatters that register their trade names or similar-sounding names as domain names. The act also helps trademark owners challenge the registration of their trademark as a domain name even if the trademark owner has not created an actual website.

In 1994, a reporter bought the mcdonalds.com domain for a story he was writing for Wired magazine about the value of domain names. At this very early stage of the Internet, nobody at McDonald's saw any value to being online. Eventually McDonald's realized their mistake and wanted to use the domain name. So the author persuaded the company to make a charitable contribution of $3,500 to a public school to provide computers and Internet access in exchange for returning the domain name to McDonalds.

========== End of Unit-4 ==========

Unit 4: Intellectual Property (8 Hrs.)

Intellectual Property, Copyright; Patient; Trade Secrets; Intellectual Property Issues: Plagiarism, Reverse Engineering, Open Source Code, Competitive Intelligence, Trademark Infringement, and Cybersquatting