WHAT IS 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. Intellectual property 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 legislation 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.

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.

COPYRIGHTS

Copyright and patent protection was established through the U.S. Constitution.

This passage discusses copyright law in the United States, rooted in the Constitution. Here's a summary with explanations and key highlights:

What is Copyright?

A copyright is a legal right granted to creators of original works. It gives them exclusive control over how their work is used, including:

- **Distribution:** Selling or giving away copies of the work.
- **Display:** Publicly showing the work.
- **Performance:** Publicly performing the work (e.g., a play, music).

- **Reproduction:** Making copies of the work.
- **Derivative Works:** Creating new works based on the original (e.g., a movie based on a book).

Copyright protects "original works of authorship" in any tangible form, whether it's written, recorded, or exists in a digital format. The creator can transfer these rights to others. As technology advances, copyright protection has been extended to new forms of expression, like audiovisual works and computer programs.

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 willful infringement.

Copyright Term (How Long Does Protection Last?):

The length of copyright protection has been extended numerous times. The current rules, largely defined by the Sonny Bono Copyright Term Extension Act, are complex and depend on when the work was created:

- **Works created after January 1, 1978:** Life of the author plus 70 years. This means the copyright lasts for the author's entire lifetime, plus 70 years after their death.
- **Unpublished/Unregistered works created before January 1, 1978:** Life of the author plus 70 years, but in no case expires earlier than December 31, 2004.
- **Works created before 1978 (and still under copyright):** 95 years from the date the original copyright was secured.

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. **The fair use doctrine allows portions of copyrighted materials to be used without permission under certain circumstances.**

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:

• The purpose and character of the use (such as commercial use or nonprofit, educational purposes)
• The nature of the copyrighted work
• The portion of the copyrighted work used in relation to the work as a whole
• The effect of the use on the value of the copyrighted work

Idea vs. Expression:

The concept that an idea cannot be copyrighted but the expression of an idea can be is key to understanding copyright protection.

An idea itself cannot be copyrighted, but the *expression* of that idea can be. For example, two authors could write about the same historical figure, but they can't copy each other's specific wording. Independent creation of similar works is not infringement, but proving independent creation can be difficult.

HathiTrust Case:

The HathiTrust case illustrated "transformative use" within fair use. HathiTrust created a searchable database of books. The court ruled this was fair use because creating the index was a *transformative* act, adding a new purpose to the original works.

Software Copyright:

Software copyright is complex. Simply creating a program that performs the same function as another is not necessarily infringement. 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.

Tetris Case:

The Tetris case demonstrates that while basic game rules and functionality are not protectable, *other* elements, like the specific design and presentation, *are* subject to copyright. Xio Interactive copied too many elements of Tetris, even if it didn't copy the core gameplay, and thus infringed on the Tetris copyright.

PRO-IP Act, GATT, the WTO, and the TRIPS Agreement, all of which strengthen intellectual property protection, particularly copyright, on both domestic and international levels.

PRO-IP Act of 2008:(Prioritizing resources and organization for Intellectual Property)

This U.S. law significantly increased penalties for copyright and trademark infringement. For example, fines for infringing a 10-song album were dramatically raised. It also established the Office of the United States Intellectual Property Enforcement Representative and the CHIP (Computer Hacking and Intellectual Property) program, a network of specialized federal prosecutors focusing on computer and intellectual property crimes. Essentially, the PRO-IP Act aimed to get tougher on IP theft.

General Agreement on Tariffs and Trade (GATT):

GATT was a major international trade agreement. The Uruguay Round of GATT negotiations led to an agreement among many nations and also created the World Trade Organization (WTO). Critically, **GATT includes a section specifically addressing copyrights: the Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS)**, which is discussed below. U.S. law was brought in line with GATT through acts like the Uruguay Round Agreements Act and the Sonny Bono Copyright Term Extension Act. However, it's important to note that copyright protection still varies across countries, making expert consultation necessary for international use of intellectual property.

World Trade Organization (WTO) and TRIPS (Trade-Related Aspects of Intellectual Property Rights) Agreement:

The WTO is a global organization overseeing international trade. It has many member nations and aims to facilitate trade. Recognizing the growing importance of intellectual property in global trade, the WTO created the TRIPS Agreement. TRIPS sets *minimum* standards of intellectual property protection that all WTO member governments must provide. It mandates that member countries have laws that enforce intellectual property rights and impose strong penalties for infringement. Essentially, TRIPS tries to level the playing field and ensure stronger IP protection worldwide. The passage also mentions a table summarizing copyright, patent, and trade secret protection under TRIPS.

TABLE 6-1 Summary of the WTO TRIPS Agreement

Form of intellectual property	Key terms of agreement
Copyright	Computer programs are protected as literary works. Authors of computer programs and producers of sound recordings have the right to prohibit the commercial rental of their works to the public.
Patent	Patent protection is available for any invention—whether a product or process—in all fields of technology without discrimination, subject to the normal tests of novelty, inventiveness, and industrial applicability. It is also required that patents be available and patent rights enjoyable without discrimination as to the place of invention and whether products are imported or locally produced.
Trade secret	Trade secrets and other types of undisclosed information that have commercial value must be protected against breach of confidence and other acts that are contrary to honest commercial practices. However, reasonable steps must have been taken to keep the information secret.

Source Line: World Trade Organization, "Overview: The TRIPS Agreement," www.wto.org/english/tratop_e/trips_e/intel2_e.htm.

World Intellectual Property Organization (WIPO):

WIPO is a United Nations agency dedicated to promoting intellectual property (IP) to stimulate innovation and creativity. It has many member nations and controls numerous international treaties. WIPO advocates for IP owners and aims for uniform administration of IP laws globally.

WIPO Copyright Treaty (1996):

This treaty provides additional copyright protections for electronic media. It specifically protects computer programs as literary works and the arrangement of material in databases. It also gives authors control over the rental and distribution of their work and prohibits circumventing

technical protection measures. The WIPO Copyright Treaty is implemented in U.S. law through the DMCA.

Digital Millennium Copyright Act (DMCA) (1998):

The DMCA implements the WIPO Copyright Treaty and another WIPO treaty in U.S. law. It has five main sections:

- **Title I:** Implements the WIPO treaties, prohibits circumventing technological protection measures, and prohibits tampering with copyright management information. It also adds civil and criminal penalties for violations. This is a key part of the DMCA.
- **Title II (Online Copyright Infringement Liability Limitation Act):** Provides "safe harbors" for website operators that allow user-generated content, limiting their liability for copyright infringement if they follow certain procedures (like "notice and takedown").
- **Title III (Computer Maintenance Competition Assurance Act):** Allows copying a computer program for maintenance/repair purposes.
- **Title IV:** Clarifies the Copyright Office's authority.
- **Title V (Vessel Hull Design Protection Act):** Protects original vessel hull designs.

DeCSS Case:

The DeCSS case, involving software that could break DVD encryption, demonstrated the DMCA's anticircumvention provisions in action. Courts ruled that distributing DeCSS violated the DMCA.

Title II (Safe Harbors and Notice and Takedown):

Title II provides safe harbors for ISPs, protecting them from liability for user-generated content if they are unaware of infringement or if they act quickly to remove infringing material ("notice and takedown"). Copyright holders can issue subpoenas to ISPs to identify infringers. The "notice and takedown" process involves the copyright holder notifying the ISP, the ISP notifying the uploader, and the ISP removing the content if there's no counter-notice.

Viacom v. YouTube Case:

This case explored the limits of DMCA safe harbor protection. Viacom argued that YouTube's "general awareness" of infringement should disqualify it from safe harbor. The courts considered whether YouTube had specific knowledge of infringing content. The case highlighted the complexities of applying the DMCA to user-generated content platforms.

Criticisms of the DMCA:

Some argue the DMCA is essential for the internet's growth, protecting ISPs from excessive liability for user content. Others argue it grants too much power to copyright holders, especially regarding subpoenas and the "notice and takedown" process, potentially chilling free speech and innovation.

PATENTS

A patent is a grant of a property right issued by the United States 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.

Patent Application Process:

Obtaining a patent requires a strict application process with the USPTO. The USPTO searches for "prior art" (existing knowledge in the field) to ensure the invention is truly new. Despite having many examiners, the patent process is slow, often taking over two years, and there's a large backlog of applications. This delay can be costly, so patent applications are often prepared by specialists, not the inventors themselves.

Patent Law:

Patent law is primarily found in Title 35 of the U.S. Code. Key sections include:

- **Section 101:** Defines what can be patented (new and useful processes, machines, etc.).

- **Section 102:** Defines "novelty" and describes prior art.
- **Section 103:** Describes "nonobviousness" – the invention must not be obvious to someone skilled in the relevant field.

What Can and Cannot be Patented:

The Supreme Court has ruled that abstract ideas, laws of nature, and natural phenomena cannot be patented. Mathematical formulas, like Pythagoras' theorem, are also not patentable. While the law doesn't explicitly mention software, gene sequences, or genetically modified bacteria, these *have* been determined to be patentable by courts.

Patent Infringement:

Patent infringement is the unauthorized use of a patented invention. Unlike copyright infringement, there's no set limit on monetary penalties. Courts can award up to *three times* the damages claimed if infringement is deemed intentional. Common defenses against infringement claims include challenging the validity of the patent itself or arguing that not every element of the patent claim was infringed. The patent holder must prove both infringement *and* damages.

Software Patents:

Software patents cover features or processes embodied in computer instructions. The patentability of software has been a complex issue. Initially, courts were reluctant to grant software patents. However, the *Diamond v. Diehr* case in 1981 marked a turning point. The Supreme Court granted a patent for a process control system that used a computer, establishing that software-related inventions *could* be patented. This led to a surge in software patents in the 80s and 90s, covering various types of software and software processes. More recently, courts have become more restrictive on software patents. Some argue that too many software patents are being granted, hindering innovation. Software patent litigation is common and expensive, as illustrated by several high-profile cases involving companies like Oracle, Google, Apple, and Mformation.

Cross-Licensing Agreements:

Many large software companies use cross-licensing agreements, where they agree not to sue each other for patent infringement. This allows them to avoid costly and protracted legal battles. For example, Apple and HTC settled a patent dispute with a cross-licensing agreement.

However, smaller companies often don't have the leverage to negotiate such agreements with larger firms. This puts small businesses at a disadvantage, as they face the full cost and risk of patent litigation. Large companies can also use multiple patent suits to overwhelm smaller competitors, forcing them to settle even if the suits are without merit. Patent lawsuits are very expensive, making it difficult for small businesses to defend their patents against large corporations.

TRADE SECRETS

A trade secret can be 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. 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.

International Variation in Trade Secret Protection:

Trade secret laws differ significantly from country to country. Some countries, like the Philippines, offer no legal protection at all. Others may have restrictions on what can be patented (e.g., pharmaceuticals in some European countries). Some countries may even require foreign companies to transfer technology rights to local entities. The example of

Coca-Cola illustrates the importance of trade secret protection, even if it means sacrificing market share. Businesses operating internationally must be aware of these legal variations.

Uniform Trade Secrets Act (UTSA):

The UTSA was created to standardize trade secret law across the United States. Many states have adopted it. The UTSA defines a trade secret as information (including formulas, patterns, programs, etc.) that:

1. Has economic value because it's not generally known and not easily discoverable.
2. Is subject to reasonable efforts to maintain secrecy.

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

Economic Espionage Act (EEA) (1996):

The EEA criminalizes the theft of trade secrets, with penalties of up to $10 million and 15 years in prison. It was enacted because there was previously no specific federal law against economic espionage. The FBI was investigating numerous cases of economic espionage at the time. The cost of economic espionage, including intellectual property theft, is estimated to be very high.

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 labeled 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.

Another option for preserving trade secrets is to have an experienced member of the Human Resources Department conducts an exit interview with each departing employee. A key step in the interview is to review a checklist that deals with confidentiality issues. At the end of the interview, the departing employee is asked to sign an acknowledgment of responsibility not to divulge any trade secrets.

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. Courts evaluating noncompete agreements consider several factors:

- Reasonableness of the restriction and its protection of confidential information.
- Employee's right to work and use their skills and experience.
- Geographic scope and duration of the restriction, considering the industry's pace of change.

KEY INTELLECTUAL PROPERTY ISSUES

This section discusses several issues that apply to intellectual property and information technology, including plagiarism, reverse engineering, open source code, competitive intelligence, trademark infringement, and cybersquatting.

Plagiarism

Plagiarism is stealing someone else's ideas or words and presenting them as your own. The internet has made it easier to copy and paste content without proper citation. Online "paper mills" further contribute to the problem. Plagiarism is an issue across all levels of education and even in professional fields.

Why Does Plagiarism Occur?

Despite ethical codes and penalties, many students don't fully understand what constitutes plagiarism. Some mistakenly believe online content is in the public domain. Others plagiarize due to pressure to achieve high grades, laziness, or time constraints. Surveys indicate

plagiarism is increasing, even with efforts to combat it. Even online course platforms have struggled with plagiarism among students.

How is Plagiarism Detected?

Instructors may recognize plagiarism by noticing inconsistencies in a student's writing style. Plagiarism detection systems are also widely used. These systems, like Turnitin and iThenticate, compare documents against massive databases of web pages, student papers, and published works to identify matching text.

Turnitin and iThenticate:

Turnitin is used by many educational institutions. It checks submitted papers against billions of web pages, millions of student papers, and numerous articles. iThenticate, from the same company, is designed for professionals in publishing, research, law, government, and finance.

How Can Schools Combat Plagiarism?

The passage suggests several actions schools can take:

- Educate students about plagiarism and proper citation.
- Show students how to document online sources.
- Break down large writing assignments into smaller parts to avoid time crunches.
- Make students aware of internet paper mills and their knowledge of them.
- Educate students about plagiarism detection software and make it clear that instructors use these tools.
- Incorporate detection software into a comprehensive anti-plagiarism program.

Reverse Engineering

Reverse engineering is the process of taking something apart in order to understand it, build a copy of it, or improve it. Reverse engineering was originally applied to computer hardware but is now commonly applied to software as well. **Reverse engineering of software involves analyzing 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.

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 (for example, 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.

Legal Aspects of Reverse Engineering:

Courts have ruled in favor of reverse engineering for the purpose of achieving interoperability. The *Sega v. Accolade* case established that reverse engineering a copyrighted work is fair use if it's necessary to access unprotected elements (like code needed for interoperability) and there's a legitimate reason for access. This ruling significantly impacted the video game industry. However, software license agreements often explicitly prohibit reverse engineering, and some developers are moving projects offshore to avoid legal restrictions.

Ethical Considerations:

The ethics of reverse engineering are debated. Some argue it's justified when it enables interoperability, especially if the software creator refuses to provide necessary documentation. They argue that restricting interoperability stifles competition and harms consumers. Reverse engineering can also be valuable for identifying bugs and security vulnerabilities. Others argue that reverse engineering unfairly exploits the work of software developers, reducing their incentive to create new software. They claim it allows competitors to copy designs developed at great expense.

Open Source Code

Open source code refers to any program whose source code is freely available for use, modification, and redistribution. The philosophy behind it is that making code accessible to

many programmers leads to better software through collaborative improvement. Users can adapt the software to new needs, and bugs can be quickly identified and fixed.

Prevalence of Open Source Code:

Open source code is widely used, powering much of the internet infrastructure. Every time you access a web page or use a social media platform, you're likely interacting with open source software. It's also commonly used for data migration, extraction, transformation, and loading (ETL) into databases, and in mobile applications. Common reasons for choosing open source software include better solutions for specific problems and lower cost.

TABLE 6-4 Commonly used open source software

Open source software	Purpose
7-Zip	File compression
Ares Galaxy	Peer-to-peer file sharing
Audacity	Sound editing and special effects
Azureus	Peer-to-peer file sharing
Blender 3D	3D modeling and animation
eMule	Peer-to-peer file sharing
Eraser	Erasing data completely
Firefox	Internet browsing
OpenOffice	Word processing, spreadsheets, presentations, graphics, and databases
Video Dub	Video editing

Source Line: Course Technology/Cengage Learning.

Motivations for Creating Open Source Code:

Several reasons drive individuals and companies to create open source code:

- **Recognition:** Sharing well-crafted code can earn respect and recognition within the programming community.
- **Reciprocity:** Those who have benefited from open source code may feel obligated to contribute back to the community.

- **Business Strategy:** A company might release code as open source to promote its expertise, attract clients, or secure maintenance contracts. They may be paid for the development time, not the software itself.
- **Altruism:** A company might develop useful code but be unwilling to license and market it, choosing to donate it to the public instead.

Defining Open Source:

Several definitions of open source exist.

- **GNU General Public License (GPL):** A precursor to the Open Source Initiative's definition. GNU is a free operating system, and the GPL aims to keep GNU software free by specifying terms for copying, modifying, and distributing it.
- **Open Source Initiative (OSI):** A non-profit organization that advocates for and certifies open source licenses. Its "OSI Certified" mark guarantees that software meets its open source criteria.

Protecting Open Source Freedom:

Simply placing code in the public domain without copyright allows others to modify it and then distribute the modified version as proprietary software, stripping away the freedoms associated with the original open source code. Using an open source license prevents this from happening, ensuring that users retain their freedoms to use, modify, and share the software.

Trademark

A trademark is a symbol (logo, design, phrase, sound, word) that distinguishes one company's products from another's. Consumers rely on trademarks to identify quality and source. The Lanham Act (Trademark Act) defines trademark use, the application process with the USPTO, and penalties for infringement. **Trademark owners have the right to prevent others from using identical or confusingly similar marks.**

Trademark Registration:

The U.S. has a federal trademark database. Merchants can search this database to avoid using existing marks. To obtain a trademark, applicants must file with the USPTO, demonstrating use

in interstate commerce or a genuine intent to do so. Trademarks can be renewed indefinitely as long as the mark remains in use.

Trademark Infringement on the Web:

Lawsuits over trademark use in websites and domain names are common, but court rulings are often inconsistent and unpredictable.

Nominative Fair Use:

Nominative fair use is a legal defense in trademark infringement cases. It allows a defendant to use a plaintiff's mark to identify the plaintiff's products or services in relation to the defendant's own offerings. To successfully claim nominative fair use, the defendant must prove:

1. The plaintiff's product/service is not readily identifiable without using the plaintiff's mark.
2. Only as much of the mark is used as necessary for identification.
3. The defendant's use does not suggest endorsement or sponsorship by the plaintiff.

Example: *Playboy Enterprises, Inc. v. Terri Welles*

Terri Welles, a former Playmate of the Year, used "Playboy model" and "Playmate of the Year" on her website. The court ruled this was permissible nominative use, as she was using the terms to accurately identify herself.

Example: IGB Eletronica and Apple's iPhone:

IGB, a Brazilian company, obtained trademark rights to the name "iPhone" in Brazil *before* Apple's iPhone was released. IGB then launched its own "Gradiente iPhone." Apple sued IGB over trademark infringement, leading to a lengthy legal battle. This case highlights the complexities of trademark law, especially in international contexts and when prior registration exists.

What is Cybersquatting?

Cybersquatting is the practice of registering domain names that contain famous trademarks or company names with no connection to the registrant. The goal is often to sell the domain name to the trademark owner for a profit. In the early days of the web, domain

names were assigned on a first-come, first-served basis, making it easy for cybersquatters to exploit this system.

How to Combat Cybersquatting:

Organizations use several strategies to mitigate the risks of cybersquatting:

- **Defensive Registration:** Registering numerous domain names and variations of their trademarks (e.g., .com, .org, .info, multilingual versions) as soon as they plan to establish a web presence. This is often cheaper than fighting cybersquatters.
- **ICANN's Role:** The Internet Corporation for Assigned Names and Numbers (ICANN) manages the internet's domain name system. The introduction of new generic top-level domains (gTLDs) (like .xxx) allows trademark holders to assert their rights in these new domains before general registration opens.
- **Uniform Domain Name Dispute Resolution Policy (UDRP):** ICANN's UDRP offers a fast and inexpensive way to resolve trademark-based domain name disputes through arbitration.
- **Anticybersquatting Consumer Protection Act (ACPA) (1999):** This act allows trademark owners to sue foreign cybersquatters, even if they are outside U.S. jurisdiction. It also allows for damages of up to $100,000 per domain name and enables trademark holders to challenge domain name registrations even if they haven't yet created a website.

Example: Ally Financial Case:

Ally Financial sued a man under the ACPA for registering domain names similar to Ally's. The man initially tried to leverage the domain names into a business venture with Ally, and then redirected traffic to Ally's competitor. Ally is seeking damages. This case illustrates how the ACPA can be used to protect trademark owners from cybersquatting.