12.3: The Digital Millennium Copyright Act

As digital technologies have changed what it means to create, copy, and distribute media, a policy vacuum has been created. In 1998, the US Congress passed the Digital Millennium Copyright Act (DMCA), which extended copyright law to consider digital technologies, while limiting the liability of the providers of online services for copyright infringement by their users. An anti-piracy statute makes it illegal to duplicate digital copyrighted works and sell or freely distribute them. Two of the best-known provisions from the DMCA are the anti-circumvention provision and the "safe harbor" provision.

- The anti-circumvention provision makes it illegal to create technology to circumvent technology that has been put in place to protect a copyrighted work. This provision includes the creation of the technology and the publishing of information that describes how to do it. While this provision does allow for some exceptions, it has become quite controversial and has led to a movement to have it modified.
- The "safe harbor" provision limits online service providers' liability when someone using their services commits copyright infringement. This provision allows YouTube, for example, not to be held liable when someone posts a clip from a copyrighted movie. The provision does require the online service provider to take action when they are notified of the violation (a "takedown" notice). For an example of how takedown works, here's how YouTube handles these requests: YouTube Copyright Infringement Notification.

Here's a video overview of DMCA by CopyrightAlliance:

Many think that the DMCA goes too far and ends up limiting our freedom of speech. The Electronic Frontier Foundation (EFF) is at the forefront of this battle. For example, in discussing the anti-circumvention provision, the EFF states:

Yet, the DMCA has become a serious threat that jeopardizes fair use, impedes competition and innovation, chills free expression and scientific research, and interferes with computer intrusion laws. If you circumvent DRM [digital rights management] locks for non-infringing fair uses or create the tools to do so, you might be on the receiving end of a lawsuit.

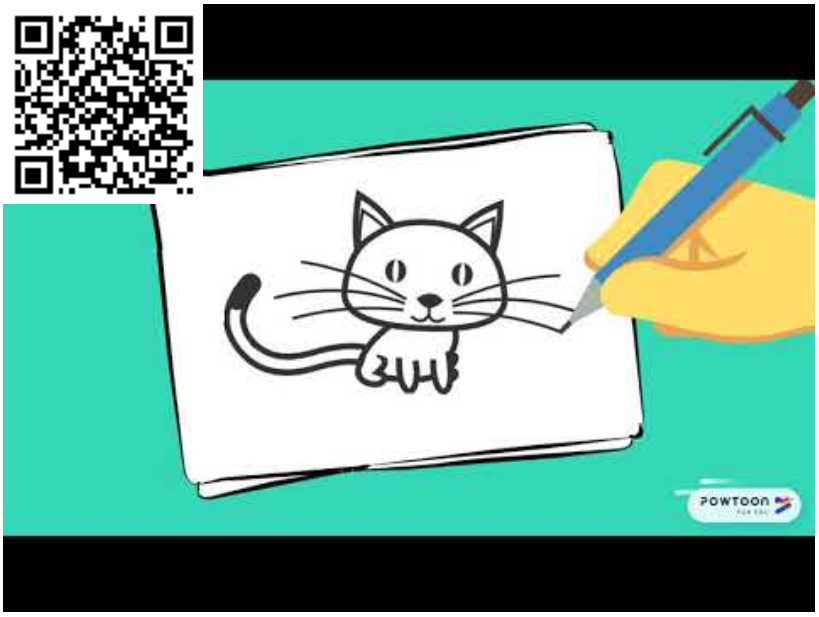
12.3.1: Creative Commons

In chapter 2, we learned about open-source software. Open-source software has few or no copyright restrictions; the software creators publish their code and make their software available for others to use and distribute for free. This is great for software, but what about other forms of copyrighted works? If an artist or writer wants to make their works available, how can they go about doing so while still protecting their work integrity? Creative Commons is the solution to this problem.

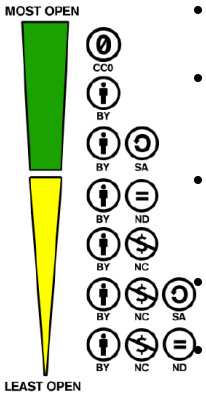
Creative Commons is an international nonprofit organization that provides legal tools for artists and authors around the world. The tools offered to make it simple to license artistic or literary work for others to use or distribute consistently with the creator's intentions. Creative Commons licenses are indicated with the symbol CC . It is important to note that Creative Commons and the

public domain are not the same. When something is in the public domain, it has absolutely no restrictions on its use or distribution. Works whose copyrights have expired, for example, are in the public domain.

Watch this video by U of G Library that introduces creative commons licensing to make copyright easier to understand.



By using a Creative Commons license, creators can control the use of their work while still making it widely accessible. By attaching a Creative Commons license to their work, a legally binding license is created. Creators can choose from the following six licenses with varying permissions from the least open to the most open license:



- **CCO**: allows creators to give up their copyright and put their works into the worldwide public domain. It allows others to distribute, remix, adapt and build upon in any medium or format with no conditions.
- **CC BY**: This is the least restrictive license. It lets others distribute, remix, adapt, and build upon the original work, in any medium or format, even commercially, as long as they give the author credit (attribution) for the original work.
- **CC-BY-SA**: This license restricts the distribution of the work via the “share-alike” clause. This means that others can freely distribute, remix, adapt and build upon the work, but they must give credit to the original author, and they must share using the same Creative Commons license.
- **CC-BY-NC**: NC stands for “non-commercial.” This license is the same as CC-BY but adds that no one can make money with this work - non-commercial purposes only.
- **CC-BY-NC-SA**: This license allows others to distribute, remix, adapt, and build upon the original work for non-commercial purposes, but they must give credit to the original author and share using the same license.
- **CC-BY-NC-ND**: This license is the same as CC-BY-NC and adds the ND restriction, which means that no derivative works may be made from the original.

Figure 12.3.1: Creative Commons licenses icons created by Creative Commons licensed under CC BY 4.0

This OER text book has been written under the Creative Commons license CC-BY. More than half a billion licensed works exist on the Web free for students and teachers to use, build upon, and share. Understanding the Creative Commons licenses and copyrights is important for making sure you're a respectful digital citizen.

Example 12.3.1

How well do you understand CC licensing? Suppose you find the following black and white image.

You would like to color it and then use it. Which licenses should the image have that allows you to do that?

CC BY

CC BY-SA

CC BY NC

CC BY-NC-SA

CC-BY-NC-ND

Solution

All except CC BY-NC-ND which does not allow derivative work. Coloring the image is considered a derivative work.

12.3.2: Patent

Another important form of intellectual property protection is the patent. A patent creates protection for someone who invents a new product or process. The definition of invention is quite broad and covers many different fields. Here are some examples of items receiving patents:

- circuit designs in semiconductors
- prescription drug formulas
- firearms
- locks
- plumbing
- engines
- coating processes and
- business processes.

Once a patent is granted, it provides the inventors with protection from others infringing on their patent. A patent holder has the right to “exclude others from making, using, offering for sale, or selling the invention throughout the United States or importing the invention into the United States for a limited time in exchange for public disclosure of the invention when the patent is granted.”

As with copyright, patent protection lasts for a limited period of time before the invention or process enters the public domain. In the US, a patent lasts twenty years. This is why generic drugs are available to replace brand-name drugs after twenty years.

Example

In 1935, a patent application was submitted for a board game called Monopoly. The Patent Office initially rejected it, stating that the game was too similar to previous games. However, after appeal, a patent was eventually granted in 1935, protecting this now famous board game.

12.3.3: Obtaining Patent Protection

Unlike copyright, a patent is not automatically granted when someone has an interesting idea and writes it down. In most countries, a patent application must be submitted to a government patent office. A patent will only be granted if the invention or process being submitted meets certain conditions:

- It must be original. The invention being submitted must not have been submitted before.
- It must be non-obvious. You cannot patent something that anyone could think of. For example, you could not put a pencil on a chair and try to get a patent for a pencil-holding chair.
- It must be useful. The invention being submitted must serve some purpose or have some use that would be desired.

The United States Patent and Trademark Office(USPTO) is the federal agency that grants U.S patents and registering trademarks. It reviews patent applications to ensure that the item being submitted meets these requirements. This is not an easy job: USPTO processes more than 600,000 patent applications and grants upwards of 300,000 patents each year. It took 75 years to issue the first million patents. The last million patents took only three years to issue; digital technologies drive much of this innovation.

The cost of preparing and filing a patent application can vary dramatically based on such factors as the technology of the invention, the skill and experience of the attorney or agent preparing the application, and the involvement of the inventor in the process. Simple mechanical patent applications can be prepared for less than 10,000 dollars in many cases, while some drug related applications might exceed $30,000 or 40,000 dollars to prepare and file. Patents are not inexpensive, so why should companies get patents? Patents provide a competitive advantage by

- enabling limited monopolies for their owners
- protect the invention from leaving the business - ex-employees, customers, competitors cannot market their own competing products
- and provide a tangible measure of research and product development output.

Sidebar: What is a Patent Troll?

The advent of digital technologies has led to a large increase in patent filings and, therefore, many patents being granted. Once a patent is granted, it is up to the patent owner to enforce it; if someone is found to be using the invention without permission, the patent holder has the right to sue to force that person to stop and collect damages.

The rise in patents has led to a new form of profiteering called patent trolling. A patent troll is a person or organization who gains the rights to a patent but does not actually make the invention that the patent protects. Instead, the patent troll searches for illegally using the invention in some way and sues them. In many cases, the infringement being alleged is questionable at best. For example, companies have been sued for using Wi-Fi or for scanning documents, technologies that have been on the market for many years.

Recently, the US government has begun taking action against patent trolls. Several pieces of legislation are working their way through Congress that will, if enacted, limit the ability of patent trolls to threaten innovation. You can learn a lot more about patent trolls by listening to a detailed investigation titled *When Patents Attack* conducted by the radio program This American Life.

12.3.4: Trademark

A trademark is a word, phrase, logo, shape, or sound that identifies a source of goods or services. For example, the Nike “Swoosh,” the Facebook “f,” and Apple’s apple (with a bite taken out of it) Kleenex(facial tissue brand) are all trademarked. The concept

behind trademarks is to protect the consumer. Imagine going to the local shopping center to purchase a specific item from a specific store and finding that there are several stores all with the same name!

Two types of trademarks exist – a common-law trademark and a registered trademark. As with copyright, an organization will automatically receive a trademark if a word, phrase, or logo is being used in the normal course of business (subject to some restrictions, discussed below). A common-law trademark is designated by placing "TM" next to the trademark. A registered trademark has been examined, approved, and registered with the trademark office, such as the Patent and Trademark Office in the US. A registered trademark has the circle-R (®) placed next to the trademark.

While most any word, phrase, logo, shape, or sound can be trademarked, there are a few limitations.

A trademark will not hold up legally if it meets one or more of the following conditions:

1. The trademark is likely to confuse with a mark in a registration or prior application.
2. The trademark is merely descriptive for the goods/services. For example, trying to register the trademark "blue" for a blue product you sell will not pass muster.
3. The trademark is a geographic term.
4. The trademark is a surname. You will not be allowed to trademark "Smith's Bookstore."
5. The trademark is ornamental as applied to the goods. For example, a repeating flower pattern that is a design on a plate cannot be trademarked.

As long as an organization uses its trademark and defends it against infringement, the protection afforded by it does not expire. Thus, many organizations defend their trademark against other companies whose branding even only slightly copies their trademark. For example, Chick-fil-A has trademarked the phrase "Eat Mor Chikin" and has vigorously defended it against a small business using the slogan "Eat More Kale." Coca-Cola has trademarked its bottle's contour shape and will bring legal action against any company using a bottle design similar to theirs. As an example of trademarks that have been diluted and have now lost their protection in the US are "aspirin" (originally trademarked by Bayer), "escalator" (originally trademarked by Otis), and "yo-yo" (originally trademarked by Duncan).

Sidebar: What is the difference between Copyright, Trademark, and Patent?

Each of the legal rights Copyright, Trademark and Patent provides a person or company with the ability to exploit or protect a particular form of intellectual property. While patents tend to be very distinct from the other two categories, how copyright and trademark are distinguished can often be difficult for people to understand. This video compares Copyright vs. Trademark vs. Patent

Examples: Lost Protection

Examples of trademarks that lost protection due to becoming widely used generic terms include aspirin, escalator, and yo-yo. All were originally protected brand names that are now just common names for the related products.

12.3.5: Information Systems and Intellectual Property

The rise of information systems has forced us to rethink how we deal with intellectual property. From the increase in patent applications swamping the government's patent office to the new laws that must be put in place to enforce copyright protection, digital technologies have impacted our behavior.

12.3.6: Privacy

The term privacy has many definitions, but privacy will mean the ability to control information about oneself for our purposes. Our ability to maintain our privacy has eroded substantially in the past decades due to information systems.

12.3.6.1: Personally Identifiable Information(PII)

Information about a person that can uniquely establish that person's identity is called personally identifiable information, or PII. This is a broad category that includes information such as:

- name;
- social security number;
- date of birth;
- place of birth;
- mother's maiden name;
- biometric records (fingerprint, face, etc.);
- medical records;
- educational records;
- financial information; and
- employment information.

Organizations that collect PII are responsible for protecting it. The Department of Commerce recommends that "organizations minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission." They go on to state that "the likelihood of harm caused by a breach involving PII is greatly reduced if an organization minimizes the amount of PII it uses, collects, and stores." 4 Organizations that do not protect PII can face penalties, lawsuits, and loss of business. In the US, most states now have laws requiring organizations that have had security breaches related to PII to notify potential victims, as does the European Union.

Just because companies are required to protect your information does not mean they are restricted from sharing it. In the US, companies can share your information without your explicit consent (see sidebar below), though not all do so. The FTC urges companies that collect PII to create a privacy policy and post it on their website. California requires a privacy policy for any website that does business with a resident of the state.

While the US's privacy laws seek to balance consumer protection with promoting commerce, in the European Union, privacy is considered a fundamental right that outweighs the interests of commerce. This has led to much stricter privacy protection in the EU and makes commerce more difficult between the US and the EU.

Example: Facebook

Facebook faced a $5 billion penalty in 2019 for failing to protect user privacy after the Cambridge Analytica scandal revealed the private data of millions of users had been misused without consent.

12.3.7: Non-Obvious Relationship Awareness (NORA)

Digital technologies have given us many new capabilities that simplify and expedite the collection of personal information. Every time we come into contact with digital technologies, information about us is being made available. From our location to our web-surfing habits, our criminal record, to our credit report, we are constantly being monitored. This information can then be aggregated to create profiles of every one of us. While much of the information collected was available in the past, collecting it and combining it took time and effort. Today, detailed information about us is available for purchase from different companies. Even information not categorized as PII can be aggregated so that an individual can be identified.

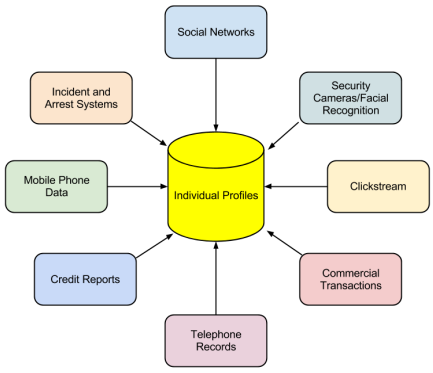


Figure 12.3.2 Non-obvious relationship awareness(NORA). Image by David Bourgeois, Ph.D. is licensed CC-By-NC-SA 4.0

First commercialized by big casinos looking to find cheaters, NORA is used by both government agencies and private organizations, and it is big business. In some settings, NORA can bring many benefits, such as in law enforcement. By identifying potential criminals more quickly, crimes can be solved more quickly or even prevented before they happen. But these advantages come at a price: our privacy.

Example: NORA

NORA technology allowed law enforcement to identify an anonymous serial killer in Louisiana known as the Riddler, who had sent cryptic notes to police. By analyzing writing samples through NORA, a suspect was identified.

12.3.8: Restrictions on Data Collecting

Information privacy or data protection laws provide legal guidelines for obtaining, using, and storing data about its citizens. The European Union has had the General Data Protection Regulation(GDPR) in force since 2018. The US does not have a comprehensive information privacy law but has adopted sectoral laws. 9

12.3.8.1: Children's Online Privacy Protection Act (COPPA)

Websites collecting information from children under the age of thirteen are required to comply with the Children's Online Privacy Protection Act (COPPA), which is enforced by the Federal Trade Commission (FTC). To comply with COPPA, organizations must make a good-faith effort to determine the age of those accessing their websites. If users are under thirteen years old, they must obtain parental consent before collecting any information.

Note

In 2022, T-Mobile paid $19 million to settle claims it violated COPPA by selling location data from children's phones to third party companies, failing to obtain parental consent.

12.3.8.2: Family Educational Rights and Privacy Act (FERPA)

The Family Educational Rights and Privacy Act (FERPA) is a US law that protects student education records' privacy. In brief, this law specifies that parents have a right to their child's educational information until they reach either the age of eighteen or begin

attending school beyond the high school level. At that point, control of the information is given to the child. While this law is not specifically about the digital collection of information on the Internet, the educational institutions collecting student information are at a higher risk for disclosing it improperly because of digital technologies. This became especially apparent during the Covid-19 pandemic when all face-to-face classes at educational institutions transitioned to online classes. Institutions need to have policies in place that protect student privacy during video meetings and recordings.

12.3.8.3: Health Insurance Portability and Accountability Act (HIPAA)

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) is the law that specifically singles out records related to health care as a special class of personally identifiable information. This law gives patients specific rights to control their medical records, requires health care providers and others who maintain this information to get specific permission to share it, and imposes penalties on the institutions that breach this trust. Since much of this information is now shared via electronic medical records, the protection of those systems becomes paramount.

If you key in the data in the US, you own the right to store and use it even if the data was collected without permission except regulated by laws and rules such as above. Very few states recognize an individual's right to privacy; California is the exception. The California Online Privacy Protection Act of 2003(OPPA) requires operators of commercial websites or online services that collect personal information on California residents through a website to post a privacy policy on the site conspicuously.

Sidebar: Do Not Track

When it comes to getting permission to share personal information, the US and the EU have different approaches. In the US, the "opt-out" model is prevalent; in this model, the default agreement is that you have agreed to share your information with the organization and explicitly tell them that you do not want your information shared. No laws prohibit sharing your data (beyond some specific categories of data, such as medical records). In the European Union, the "opt-in" model is required to be the default. In this case, you must give your explicit permission before an organization can share your information.

To combat this sharing of information, the Do Not Track initiative was created. As its creators explain 3 :

Do Not Track is a technology and policy proposal that enables users to opt-out of tracking by websites they do not visit, including analytics services, advertising networks, and social platforms. At present, few of these third parties offer a reliable tracking opt-out, and tools for blocking them are neither user-friendly nor comprehensive. Much like the popular Do Not Call registry, Do Not Track provides users with a single, simple, persistent choice to opt-out of third-party web tracking.

12.3.9: References

EFF. *Unintended consequences - 16 years under DCMA (2014)*. Retrieved November 10, 2020, from https://www.eff.org/wp/unintended-consequences-16-years-under-dmca

EFF. *Do not track*. Retrieved November 10, 2020, from http://donottrack.us/

Guide to Protecting the Confidentiality of Personally Identifiable Information (PII). National Institute of Standards and Technology. US Department of Commerce Special Publication 800-122. http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf

US Patent and Trademark Office, *"What is a patent?"* Retrieved November 10, 2020, from www.uspto.gov/patents/