bookboon
The eBook company

Internet and Technology Law: A U.S. Perspective

Konnie G. Kustron

Konnie G. Kustron

Internet and Technology Law: A U.S. Perspective

Internet and Technology Law: A U.S. Perspective
1st edition

ISBN 978-87-403-0845-7

Note: Court cases, illustrations, and photographs used in this book have been taken primarily from United States federal government websites. They are public documents belonging to the United States Government (17 U.S.C. § 105), and as such, are not subject to U.S. copyright protection. Included documents are available at various websites including https://public.resource.org. Other documents have been included for educational purposes and discussion.

Content for this book has been taken in part from class lectures created by the author, and that have been used in her courses at Eastern Michigan University, in Ypsilanti, Michigan.

Images designated as "used with permission" are owned by the author.

Any errors or omissions are the sole responsibility of the author.

Contents

About the Author

Konnie Kustron is an attorney-educator. She is currently a professor in Paralegal Studies Program at Eastern Michigan University in Ypsilanti, Michigan.

Professor Kustron received her B.S. with honors in pre-law from Michigan State University, and her J.D. from the Michigan State University, College of Law. She is a member of the Michigan Bar and approved as a Veteran's Affairs attorney with United States Department of Veteran's Affairs. Professor Kustron is the recipient of an Eastern Michigan University Alumni Teaching Award as well as the Dean's Outstanding Faculty Award. Recently, she has been a contributor to the *Encyclopedia of Mathematics and Society* (Salem Press, 2011), which was described as the "Best Reference 2011," by the *Library Journal* – a leading reviewer of library materials in the United States. Professor Kustron is also a chapter author in the *Internet Guide for Michigan Lawyers*, a winner of the "Award of Excellence in the Best Publication" category awarded by the Association for Continuing Legal Education.

In 2013, Professor Kustron published her first Bookboon text, *Introduction to the American Legal System* available at http://bookboon.com/en/introduction-to-the-american-legal-system-ebook.

About the Contributing Reviewer

Christopher Bezak is an attorney specializing in intellectual property law at Sughrue Mion, PLLC, in Washington, D.C. Mr. Bezak received his B.S. with honors in Computer Engineering from the University of Michigan, Ann Arbor, and his J.D. with honors from the Michigan State University, College of Law.

1 Jurisdiction Defined

Objectives

After completing this chapter, the student should be able to:

- Define the concept of jurisdiction;
- Explain the difference between subject matter jurisdiction and personal jurisdiction;
- Define the four different types of personal jurisdiction;
- Describe the difference in interactivity between an active and a passive website; and

Understand the criteria necessary to obtain jurisdiction over an Internet business.

A Learning Story

K.T. Bird is a Michigan resident. She recently purchased a custom-made car online from Wheelz, Inc., an Indiana company. A month after delivery, certain defects appeared in the car, including doors that would not properly close, a radiator leak, as well as various mechanical problems. Estimated repair costs were $12,000. Bird's friends have told her she had a "lemon" on her hands.

The purchase price of the car was $31,033. The car was delivered directly to Bird's home by a car hauler and Bird paid for the car in full. Delivery was included in the purchase price. Bird wants to sue Wheelz. Because this was an Internet transaction involving residents from two different states, what options does Bird have? In other words, can she sue Wheelz in Michigan, or is she required to file a lawsuit against Wheelz in Indiana?

1.1 Overview

Technology and the Internet[1] have dramatically changed the way people interact with one another. The ability to electronically access, store, and transmit information presents people with many new ways to communicate. Email is now a standard business communication tool, and has also changed the way people conduct business. Technology has also created a new type of business called **electronic commerce,** which involves the purchase or sale of products and services over the Internet.

In 1995, less than 1% of the world's population had access to the Internet. However, it is estimated by the end of 2014 that the number of Internet users will reach 3 billion, or approximately 40% of the world's population.[2] With so many users online, disputes are inevitable. Social connections are made and crimes are committed online, just as they are in a face-to-face environment. Consumers increasingly make legal contracts on the Internet for services, such as travel arrangements. Estimates are that "the web will account for or influence 59% of U.S. retail purchases by 2018."[3]

All these communications can lead to disputes and potential litigation. These disagreements can involve not only individuals in the United States, but in other countries. How and where these disputes are resolved is not often clear.

Jurisdiction[4]

The legal authority of a court to decide a certain type of dispute. It is also used as a synonym for venue, meaning the geographic area over which the court has territorial jurisdiction to decide disputes.

Figure 1-1

Whenever there is a dispute between two or more parties, the parties can resolve their differences using a private agreement. If their conflict cannot be settled, then the individuals or companies involved have the option to sue each other in court. When the problem takes place with a face-to-face transaction, the law is clear which court has **jurisdiction**, namely the authority to hear the case. Typically, the **plaintiff** (the person or company suing) institutes a lawsuit where the transaction took place, or where the party being sued (the **defendant**) resides or does business. However, with disputes based on Internet transactions, it may not be clear where to sue.

With an Internet contract, the answer to the question where to sue if often found on a company's website under a section called "**terms of use**" (also called terms of service or terms and conditions), which specifies how disputes are handled. Consumers do not often realize, but consumers agree to these terms when they make a purchase. The agreement may also include a "**forum selection clause**" or "**choice of law clause**" that states who can sue whom and in what court. Typically, the consumer agrees to the "terms of use" as a condition to purchasing the product or services. These types of agreements often favor the seller rather than the consumer, and usually require lawsuits to be filed in the state where the vendor is located. Many of these agreements also include an **arbitration** provision that is mandatory in many online contracts.

Sample Terms of Use Language

You agree to resolve any dispute you have with Wheelz Inc. in a state or federal court located in Battle Ground, Indiana, and to submit to the personal jurisdiction of the courts located in Tippecanoe County, Indiana for litigating all such disputes.

Figure 1-2

Absent an agreement how a dispute is to be handled, statutes or laws determine where a lawsuit can be filed and in which court. As noted earlier, jurisdiction is the *authority of a court* to hear a controversy and render a decision to resolve a disagreement.

The United States has two main court systems: federal and state. However, each state also has their own court system. When considering the District of Columbia and the U.S. territories (U.S. Virgin Islands, Guam, the Commonwealth of Puerto Rico, Northern Mariana Islands, and American Samoa), there are well over 50 court systems[5] in the United States.

Two elements are involved with jurisdiction and the Internet: **subject matter jurisdiction** and **jurisdiction over the person (personal jurisdiction)**.[6] The discussion of these two concepts will clarify and answer the question how to determine where to file a lawsuit in an Internet based dispute.

1.2 Subject Matter Jurisdiction

Subject matter jurisdiction is the authority of a *specific* court to hear a particular type of dispute. Often times, the law is very clear and only one type of court can hear a case. This is referred to as a court having **exclusive jurisdiction** over a matter. For example, only federal courts resolve patent and bankruptcy disputes.

A federal trial court will also handle any dispute involving a federal statue, the U.S. Constitution, or a treaty. In addition, federal courts can review any dispute over $75,000 when there is **diversity of citizenship**. Diversity of the citizenship means the plaintiff and the defendant reside or do business in different states. Diversity of citizenship also applies to parties outside the United States.[7] If a dispute does not meet the criteria for federal court jurisdiction, a lawsuit should be filed in a state court.

Sometimes, both the federal and a state court will have **concurrent jurisdiction** over a matter. In that case, the attorney for the plaintiff must determine which court location would be more beneficial to his or her client. For example, a court in close proximity to the plaintiff's home or business would be more convenient and cost effective for the client as well as his or her attorney.

Subject Matter Jurisdiction for the Federal Court system	**Subject Matter Jurisdiction for the State Court system**
• Cases that deal with the constitutionality of a law; • Cases involving the laws and treaties of the U.S.; • Ambassadors and public ministers; • Disputes between two or more states; • Admiralty law; • Patent law; and • Bankruptcy.	• Most criminal cases, probate (involving wills and estates); and • Most contract cases, tort cases (personal injuries), family law (marriages, divorces, and adoptions), etc. State courts are the final arbiters of state laws and constitutions. Their interpretation of federal law or the U.S. Constitution may be appealed to the U.S. Supreme Court. The Supreme Court may choose to accept or refuse such appeals.

Figure 1-3[8]

1.3 Personal Jurisdiction

Personal jurisdiction is known as "jurisdiction over the person." In other words, a court that has personal jurisdiction over a person or company can require that party to appear in its court.

When the both parties live or do business in the same state, that state has personal jurisdiction over the litigants and the authority to require their appearance in court. A person can also consent to be subject to the personal jurisdiction of a state court. When the parties live in different states, (or different countries), the question as to what court has personal jurisdiction becomes more complex. In the federal courts, Rule 4 of the Federal Rules of Civil Procedure, which requires a federal court to follow the state law on personal jurisdiction where the court is located,[9] governs personal jurisdiction.

When the dispute is with an electronic business (e-business), courts look at the characteristics of the company's website to determine whether it "operates" within the state's boundaries. In addition to physical presence within a state, a court may acquire personal jurisdiction over a non-resident defendant based on the state's **long arm statute**, which will be discussed below.

1.4 Long Arm Statute

A long arm statute is a state law that allows a court to claim personal jurisdiction over an out of state party *who performs an act or transaction within the state*. State laws differ, but the concept is the same: allow the local court to acquire personal jurisdiction over a non-resident defendant based on the defendant's contacts within the state.

For example, in Michigan, state law Michigan Compiled Laws (MCL) 600.705 provides jurisdiction over an individual when any of the following relationships exist:

1) The transaction of any business within the state.
2) The doing or causing an act to be done, or consequences to occur, in the state resulting in an action for tort.
3) The ownership, use, or possession of real or tangible personal property situated within the state.
4) Contracting to insure a person, property, or risk located within this state at the time of contracting.
5) Entering into a contract for services to be rendered or for materials to be furnished in the state by the defendant.
6) Acting as a director, manager, trustee, or other officer of a corporation incorporated under the laws of, or having its principal place of business within this state.
7) Maintaining a domicile in this state while subject to a marital or family relationship which is the basis of the claim for divorce, alimony, separate maintenance, property settlement, child support, or child custody.[10]

Most states, such as Michigan, have not revised their laws to provide for Internet disputes for transactions taking place within its state boundaries. However, other states' statutes specifically provide for Internet disputes. For example, Virginia's long arm statute Va. Code Ann. § 8.01–328.1, provides that "using a computer or computer network located in the Commonwealth (with Virginia being a Commonwealth) shall constitute an (appropriate) act" giving a Virginia court personal jurisdiction for Internet disputes.[11]

A court will always be concerned that the out of state party is afforded **due process** of the law. Due process of law means a person must be given notice and the opportunity to be heard by a tribunal before action may be taken by a court.

If a business's connection to a state is unclear in an Internet disputes, courts may look at other criteria called **minimum (minimal) contacts** and **personal availment**.

1.5 Minimum Contacts

What are minimum contacts? Minimum contacts means the party being sued (defendant) must have some type of significant activity that connects the defendant to the state where the lawsuit will be filed. If a court does not have these minimal contacts, jurisdiction over the person or the property may not be established.

How do minimum contacts relate to Internet transactions?[12] The U.S. Supreme Court[13] in *International Shoe v. State of Washington*, 326 U.S. 310 (1945), has held that with the minimum contacts test, that there must be "sufficient contacts or ties to make it reasonable and just" for a court to establish personal jurisdiction over a party[14] and that due process requirements have been met.

Suppose for example, you meet a person through an online dating site. You never meet in person, but you develop a relationship online. You live in Pennsylvania and the other person lives in Florida. Eventually, you agree to meet one another, and you send money to your new friend for airfare to fly to Pennsylvania. However, this acquaintance takes the money for the ticket and you never hear from this person again. To recover the ticket money, you decide you would like to sue. The question is where do you file? If you file a lawsuit in Pennsylvania, the court will ask what is the basis for personal jurisdiction over your former friend. In other words, what contacts does he or she have with the State of Pennsylvania? Unfortunately, the level of contact is very small. In the alternative, the Florida courts would have clearly have jurisdiction over the dispute, as your acquaintance is a resident of that state.

Some state courts have expanded the minimum contacts standard and established an "**effects test**" described in the U.S. Supreme Court case of *Calder v. Jones*, 465 U.S. 783 (1984).[15] In *Calder*, the Court held a state court could establish personal jurisdiction over a defendant in cases in which the defendant targets an action at a particular state or forum. For example, suppose that Wheelz, Inc. sends out an email to 5000 potential customers in Ann Arbor, Michigan that describes their custom car manufacturing services. That type of marketing focus would demonstrate the company is targeting Michigan customers and would establish jurisdiction under the "effects test."

1.6 Purposeful Availment

Federal courts on the other hand, do not universally follow either the minimum contacts test or the effects test, but rather the **Zippo test** based on *Zippo Mfg. Co. v. Zippo Dot Com, Inc.*, 952 F. Supp. 119 (W.D. Pa. 1997).[16] In *Zippo*, the court followed a standard called **purposeful availment.** This means, to determine personal jurisdiction, a court will review a company's website to establish whether the company's website is active or passive. An **active website** would allow a user to order products or services and establish personal jurisdiction. On the other hand, a **passive website** would only present information or advertising. Typically exchanging information with a host computer is insufficient activity to satisfy the purposeful availment standard, and establish personal jurisdiction.

What about international disputes? The law differs across the world, as each country has its own set of regulations and laws, so there is no single established standard.

Four Main Types of Personal Jurisdiction

- The defendant is domiciled or does business within the state.
- The defendant consents to the jurisdiction of the court.
- The defendant is traveling within the geographical boundaries of the state.
- The defendant has minimal contacts with the state.

Figure 1-4

Let's now look at a few fact scenarios. Suppose that several Nevada residents invest in a web company called "BigBuck$Charlie." The company is a scam, and the investors lose all the money they have invested. The Company website is registered to a person incarcerated in a New Hampshire prison, and hosted by an Internet Service Provider in Texas. Can the Nevada residents sue BigBuck$Charlie in Nevada? The answer is probably no. The company did not have offices in Nevada, did not operate in Nevada, and owned no property in the state. If the website was informational (passive), then there is no personal jurisdiction. If the website is mixed (informational with some interactive e-business), jurisdiction will depend on the level of interactivity the parties had with the web company.

The Court Speaks

Impulsaria LLC v. United Distribution Group LLC, File No 1:11-CV-1220, (W.D. Mich. 2012)[17]

Facts:

Plaintiff Impulsaria was the owner of a federal trademark STIFF NIGHTS,[18] a dietary supplement marketed to men. It also owned a distinctive trade dress (see Chapter Three) for STIFF NIGHTS and had copyrighted material in its packaging for the product. Due to concerns by the FDA that the product contained a controlled substance, the Plaintiff stopped manufacturing the product in June 2010, and in August 2010, the Plaintiff recalled any product produced before the June date. However, when the Plaintiff reintroduced the product back into the market, it notified the FDA that a counterfeit product was also being produced, and in fact, only the counterfeit STIFF NIGHTS product that contained the illegal substance. It was during the June to August timeframe, that the Plaintiff discovered its prior distributors were selling a counterfeit version of the product, identical to its packaging and representing it to be its brand. In a Complaint filed with the court, the Plaintiff alleged that "the counterfeit products have 'a package and external image and language identical to that offered by Impulsaria;' that because of the similarity of the marks, consumers 'are likely to be and actually have been deceived, mistaken, and confused as to the source of the STIFF NIGHTS;' and that these acts have damaged Plaintiff's business reputation and have diluted Plaintiff's goodwill it its trademark." (Memorandum Opinion, p. 3)

There were four Defendants in this case: Blake King, E&A Video and Magazine, Inc., Top5supps.com, and SLK Distributors. Defendants filed a motion to dismiss Plaintiff's complaint based on a lack of personal jurisdiction.

Court[19]

Government entity authorized to resolve legal disputes. Judges sometimes use "court" to refer to themselves in the third person, as in "the court has read the briefs."

Figure 1-5

Discussion:

In its opinion, the Court held that the "plaintiff must establish 'with reasonable particularity' sufficient contacts between Defendant and the forum state to support jurisdiction." (p. 3)

"Personal jurisdiction over a defendant exists 'if a defendant is amendable to service of process under the forum state's long-arm statute and if the exercise of personal jurisdiction would not deny the defendant due process'… The due process 'minimum contacts' inquiry is satisfied if the defendant meets the following criteria:

> First, the defendant must purposefully avail himself of the privilege of acting in the focus state or causing consequence in the forum state. Second, the cause of action (legal claim) must arise from the defendant's activities there. Finally, the acts of the defendant or consequences caused by the defendant must have a substantial enough connection with the forum state to make the exercise of the jurisdiction over the defendant reasonable…" (p. 3)

Plaintiff alleged "that the Court has jurisdiction over all four Defendants 'because they are formed under the laws of the State of Michigan, maintain a principal place of business within this judicial district, or conduct business within the judicial district.'" The Plaintiff also alleged that "the Defendants are 'manufacturers, importers, wholesalers, distributors of general merchandise and/or cash and carry stores selling, offering for sale and active Internet sites selling and/or distributing products within the state of Michigan.'" (p. 5)

"Defendant King contends that the Court lacks personal jurisdiction over him. King has presented evidence that he is a resident of the State of Tennessee, that he does not own any property in Michigan, and that he has never been to Michigan, except, possibly, to change planes or during a layover." (p. 5).

However, King admitted "that any contact he has had with the State of Michigan has been solely through business transactions" conducted by BL Supplements, who is the owner of the domain name www.tops5supps.com.

Conclusion:

"The Court has held in the past 'where personal jurisdiction is based on an interactive commercial website, courts require something more than the mere accessibility of the website by residents of the forum state to demonstrate that the defendant directed its activity towards the forum state. King has not denied that Tops5 has done business in the state.' In fact, King noted in his affidavit that any contact he has had with the State of Michigan has been solely through business transactions conducted by BL, the online retailer of dietary supplements that operates and owns the domain name www.top5supps.com. Because King has not come forward with an evidence to challenge Plaintiff's assertion that he is doing business in his district through the Top5 website, the Court is satisfied that Plaintiff has met its burden of making a prima facie showing that the court has personal jurisdiction over Defendant King." (p. 6).

Questions:

1. If King had not admitted he had business contacts through his BL Supplements Company, what would the Plaintiff have to prove for the court to find personal jurisdiction over the Defendant?
2. Defendant SLK was a Georgia company, and it did business in Michigan by selling STIFF NIGHTS in "the normal stream of commerce." SLK was never registered as a Michigan company, never conducted business in Michigan, had no employees in Michigan, or maintained personal or real property in the state. It never shipped products in Michigan, never had any account or paid taxes in the Michigan, and has never been sued in the State. Should the Court take personal jurisdiction over SLK?

1.7 Summary

In this chapter, you learned about the concept of jurisdiction, and the legal criteria to determine which court can hear an Internet dispute.

A court must have both subject matter and personal jurisdiction over the parties. Personal jurisdiction for a state court can be obtained by residency within a state, operating a business or owning property within a state, or by consent. Personal jurisdiction for a federal court is based on the laws of the state where the court is located. Most states have long-arm statutes that allow a state court to establish personal jurisdiction beyond operating or owning property in a state. If a long arm-statute does not provide for personal jurisdiction, a party can argue that minimum contacts exist with the forum state, or that purposeful availment exists in its business operations.

1.8 Key Terms

Active website	Effects test	Personal jurisdiction
Arbitration	Electronic commerce	Plaintiff
Choice of law	Exclusive jurisdiction	Passive website
Concurrent jurisdiction	Forum selection clause	Purposeful availment
Defendant	Jurisdiction	Subject matter jurisdiction
Diversity of citizenship	Long arm statute	Terms of use
Due process	Minimum contacts	Zippo test

1.9 Chapter Discussion Questions

1. The U.S. Federal Court system has exclusive jurisdiction over what types of cases?
2. What is the difference between subject matter jurisdiction and personal jurisdiction?
3. Give an example in interactivity in an active and a passive website.
4. Define purposeful availment.
5. What is a long arm statute?
6. What are the four different types of personal jurisdiction?
7. What is the Zippo test?
8. What are minimum contacts?
9. Based on the case learning story involving K.T. Bird and Wheelz, Inc., can Bird sue Wheelz in Michigan or is she required to file a lawsuit against the company in Indiana?
10. What is a forum selection clause?

1.10 Additional Learning Opportunities

For more information on the U.S. court systems, please see Chapter 2 of *Introduction to American Law* at http://bookboon.com/en/introduction-to-the-american-legal-system-ebook.

1.11 Test Your Learning

1. What court has jurisdiction over a dispute *between two states* (such as Indiana and Ohio)?

A. an Indiana state court
B. an Ohio state court
C. an Indiana or Ohio state court
D. a federal court

2. What is personal jurisdiction?
   A. The authority of a court to subpoena witnesses in a dispute.
   B. The authority of a court to hear a dispute, based on minimum contacts the defendant has with a state.
   C. The ability of a court to hear a real estate dispute.
   D. The ability of an attorney to serve a party with court papers.
   E. The ability of an attorney to appear before a court.

3. A federal court has exclusive jurisdiction over which type of case?
   A. divorce
   B. custody
   C. bankruptcy
   D. contract dispute
   E. product liability

4. A long arm statute allows a state to exercise personal jurisdiction over a nonresident individual or company who has caused damage in that state.
   A. True
   B. False

5. Jurisdiction means a court has the power, right, or authority to interpret and apply the law.
   A. True
   B. False

6. Which of the following factors are evaluated when determining jurisdiction over an e-commerce website?
   A. whether a website is informational
   B. whether a website allows online ordering
   C. whether a website solicits customers from a particular state
   D. A and B
   E. all of the above

7. Long arm statutes can grant personal jurisdiction of a person who lives outside a state's boundaries.
   A. True
   B. False

8. Which of the following would NOT be purposeful availment and subject a company to a state's jurisdiction?
   A. the posting of information about a product
   B. the selling of merchandise to a consumer
   C. an email to a customer
   D. an advertisement targeted to Michigan residents
   E. a company blog that solicits customer feedback on products

9. Paul E. Photographer, a Wyoming resident, uploads a photo of 16-year-old Mary Carrie to his Flickr™ account. He took the photo with her permission while visiting an Orlando, Florida beach during "spring break." Subsequently, an Australian company downloaded and edited her photo and used it in an ad campaign. The 16 year old who lives in Texas sues the Australian company. Does the Texas Court have jurisdiction over the Australian company? Based on your understanding of "minimal contacts," what should be the Court's decision?
   A. The "minimum contacts" between the Australian company and the state of Texas were sufficient for the lawsuit to be successful.

B. The lawsuit will be unsuccessful because the Defendant (Australian company) did not "purposely avail itself to conduct business in Texas."
C. The lawsuit will be unsuccessful because the Defendant (Australian company) did not "purposely avail itself to conduct business in Texas," and the litigation did not arise out of defendant's activities in Texas.
D. The lawsuit will be unsuccessful because the Defendant (Australian company) did not "purposely avail itself to conduct business in Texas," the litigation did not arise out of defendant's activities in Texas, and jurisdiction in Texas was not something foreseeable.

10. The *Zippo* test looks at
    A. effects test
    B. forum selection clause
    C. general jurisdiction
    D. minimum contacts
    E. purposeful availment

Test Your Learning answers are located in the Appendix.

2 Privacy

Objectives

After completing this chapter, the student should be able to:

- Understand how privacy is threatened by technology;
- Describe the key sources of privacy law;
- Understand the elements of the four main privacy torts; and
- Describe the major federal laws in the United States that affect personal privacy.

> "Wherever the real power in a Government lies, there is the danger of oppression. In our Governments, the real power lies in the majority of the Community, and the invasion of private rights is chiefly to be apprehended, not from the acts of Government contrary to the sense of its constituents, but from acts in which the Government is the mere instrument of the major number of the constituents."
>
> *James Madison, Letters and Other Writings of James Madison Volume 3*

2.1 Introduction

Privacy is often defined as the "right to be left alone."[20] From a legal perspective, the right to privacy involves control over one's personal information, such as name, address, birthdate, health data, assets, and certain types of privileged communications.[21]

In *The Right to Privacy*,[22] authors Ellen Alderman and Caroline Kennedy noted "the word 'privacy' does not appear in the United States Constitution. Yet ask anyone and they will tell you they have a fundamental right to privacy. They will also tell you that privacy is under siege."[23]

That siege is most evident with the Internet, as it presents one of the greatest threats to personal information and privacy.

2.2 Threats to Privacy

Threats and challenges to privacy existed before the Internet, even when paper was the standard medium for saving personal and business information. However, as technology and the Internet have developed, personal information is saved on all types of devices including computers, cell phones, tablets, and even activity bands such as Jawbone® and Fitbit®.

Two main areas threaten a person's privacy. The first involves other people. The second threat is from the government (both state and federal). In the United States, governmental privacy issues are concentrated at the federal level.

Figure 2-1 Used with permission

2.3 Sources of Privacy Law

US privacy law is based on five specific areas: 1) the **U.S. Constitution** and **Amendments**, 2) **state constitutions**, 3) **common law torts**, 4) **federal and state statutes**, and 5) **administrative agency rules and actions.**

2.4 U.S. Constitution and Amendments

The right to privacy is not expressly stated in the US Constitution or its Amendments; however, the right to privacy has been recognized by American courts[24] as a **derived** or **implied** right. A derived right is one inferred through Constitutional language.

The U.S. Supreme Court has stated the right of privacy is a derived right through three Amendments: the **Fourth**, **Fifth** and the **Ninth**. These three Amendments protect individuals against an invasion of privacy by the federal *government*. This protection does not extend to personal privacy disputes.

Fourth Amendment	Fifth Amendment	Ninth Amendment
"The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized."	"No person shall be held to answer for a capital, or otherwise infamous crime, unless on a presentment or indictment of a grand jury, except in cases arising in the land or naval forces, or in the militia, when in actual service in time of war or public danger; nor shall any person be subject for the same offense to be twice put in jeopardy of life or limb; nor shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law; nor shall private property be taken for public use, without just compensation."	"The enumeration in the Constitution, of certain rights, shall not be construed to deny or disparage others retained by the people."

Figure 2-2

The *Fourth Amendment* guarantees that individuals will not be subject to unreasonable searches and seizures by the federal government. The key language involving privacy in this Amendment is "the right of the people to be secure in their persons, houses, papers, and effects…"

The U.S. Supreme Court decided its first landmark privacy case interpreting the Fourth Amendment in 1965 in *Griswold v. Connecticut*.[25] In *Griswold*, a married couple sued the State of Connecticut for a violation of their marital privacy. At that time, it was a state crime for a married couple to use any form of birth control. The Court found the law unconstitutional, recognized martial privacy in the bedroom, and established "zones of privacy," or areas or locations that were protected from government intrusion.[26]

As the law evolved, so did the zone of privacy. Later court cases held, if a person has an expectation of privacy and society recognizes the expectation as reasonable, then the privacy zone might expand. For example, it is reasonable to expect that a public restroom will not include cameras or other recording devices.

The *Fifth Amendment* stands for the proposition that no person shall be compelled to be a witness against him or herself. The familiar phrase that "you have a right to remain silent," comes from the Fifth Amendment. Corporations do not have this protection.

The last two Amendments that deal with privacy are the *Ninth* and *Fourteenth*. The Ninth Amendment states "[t]his enumeration shall not be construed to deny other rights retained by the people…" The reading of the Amendment is somewhat fuzzy, but the U.S. Supreme Court has broadly interpreted the Ninth Amendment to infer privacy protection in ways not detailed in the first eight Amendments. This implies there are additional privacy rights not mentioned in the other Amendments.

The Fourteenth Amendment gives individuals privacy protection from ***state*** governments using the federal constitutional standards.

This leads us to several growing questions. For example, is it a violation of privacy for the federal government to monitor a person's computer usage or cell phone conversations? How private are someone's files saved in the cloud? What are the privacy issues with wearable technology (such as Google Glass™) that can record and take photos? Alternatively, how can an individual's privacy be protected as new technologies are created?

2.5 State Constitutions

The second source of privacy law involves state constitutions. It is common for a state to include the language of the federal Fourth Amendment in its constitution, and protect individuals from a **state government's** invasion of privacy. However, many state constitutions *go further* and protect an individual's privacy from the government in other areas, such as medical records, wiretapping, insurance information, school documents, credit data, financial information, and privileged communications (*i.e.*, attorney-client or physician-patient).

2.6 Common Law Torts

The third source of privacy law is **common law**[27] **torts**.

A tort is a wrong of one person against another. Torts are not crimes. Instead, they involve civil disputes that often result in litigation. A tort must have some sort of quantifiable damages for recovery.

There are four main categories of privacy torts:

1. **Intrusion upon seclusion** (often called intrusion);
2. **Public disclosure of private facts** that causing injury to one's reputation;
3. Publicly placing a person in a **false light**; and
4. **Misappropriation** of a person's name or likeness.

Figure 2-3 Used with permission

2.6.1 Intrusion

Intrusion upon seclusion (also called intrusion) is defined as "intentionally intruding, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns."[28]

Three elements must be present for intrusion to take place:

1. There must be an intent to intrude or the knowledge the intrusion was a violation;
2. The person being violated must have had a reasonable expectation of privacy; and
3. The intrusion must be substantial and highly offensive to a reasonable person.

Publication such as posting on the Internet is not a required element.

People in public places have little expectation of privacy. People engaging in public activities must assume they might be photographed or filmed, or that what they say publicly might be recorded.

Photographing or recording another person may constitute an intrusion upon seclusion. Photographing a couple kissing in a public venue would not invade their privacy, but photographing them in a hotel room would. The difference is the expectation of privacy: public versus private.

Defenses to the claim of intrusion include:

- That you did not enter the person's private property;
- That the person gave you consent to enter their property;
- That it is **custom and usage** that privacy is waived. This means, for example, if it is standard practice for a medic to respond to an emergency fire call and the medic enters a person's home, a person could not allege intrusion if the homeowner did not expect the medic to accompany the fire department into the house.

Although property is being used here in the traditional sense (*i.e.*, real estate), courts have expanded this tort to include **electronic property rights**.[29]

2.6.2 Public Disclosure of Private Facts

Public disclosure of private facts causing injury to reputation is defined as publicly disclosing or transmitting highly private or personal information about another that causes damage to their reputation. The private facts made public must be personally embarrassing facts. The information must be "highly offensive to a reasonable person of ordinary sensibilities."[30]

The elements that must be proven for this tort include:

1. An intent to communicate the facts;
2. The disclosure must be highly offensive to a reasonable person;
3. The facts disclosed must be private or personal; and
4. The information must be communicated or publicized to a significant segment of the community.

Examples of Private Facts

- Information on a person's medical condition (such as positive for HIV) posted on Facebook®
- Someone's sexual history posted on a blog
- A viral video showing a person engaging in illegal drug use

Figure 2-4

Defenses to the claim include:

- The information was newsworthy;
- The party consented to the disclosure of the information;
- There existed a *qualified privilege*;[31]
- The information did not outrage the community's notion of decency;
- The event took place in public; or
- The information was a matter of public record.

2.6.3 Publically Placing Another in a False Light

Publically placing another in a false light means "falsely connecting a person to an immoral, illegal, or embarrassing situation causing damage to their reputation."[32]

There are two elements involved with a false light claim. First, it must be shown that "the false light would be highly offensive to a **reasonable person**," and second, that "the person committing the action had knowledge of, or acted in reckless disregard as to the falsity of the publicized matter, and the false light in which the other would be placed."[33]

The *reasonable person standard* is often used in defining a wrong. It simply means the actions of the defendant is distasteful to the average person and to society in general.

False light publicity includes incorrectly attributing an opinion or statement to another person, suing someone and using his or her name without authorization, or using another person's name on a petition without approval. This would include statements posted on the Internet, text messages, tweets, *etc.*

Some defenses to this tort would be:

- The individual was not identified;
- The information came from a privileged source;
- The information was not offensive to a reasonable person; and
- A person consented.

False light and the tort of defamation are often confused. Remember that false light involves hurting a person emotionally by embarrassing them. Defamation is an intentional false communication, either written (libel) or spoken (slander) that harms a person's reputation (see Chapter Five). To prove false light the information must be "highly offensive to a reasonable person." To prove defamation, the information must "adversely harm a person's reputation." Therefore, the threshold of proof is lower for defamation.

Truth is not generally a defense to false light lawsuits, whereas truth is a defense in defamation lawsuits.

2.6.4 Misappropriation of a Person's Name or Likeness

Misappropriation (often called appropriation) is defined as using the name, likeness, or identity of a living person, without their permission or consent, **for commercial gain or advantage**. For example, an advertising company uses a celebrity's likeness or identity to sell a client's product. If the celebrity did not consent to the use of their photo to endorse the merchandise, then a claim of misappropriation might exist.

An example of misappropriation occurred in 2010 involving President Obama and the outerwear company Weatherproof®. The company created a billboard ad using a photo of the President showing President Obama standing in front of the Great Wall in China wearing one of Waterproof's coats. The tagline of the ad said "A Leader in Style." The company was asked by the White House to remove the billboard. The official White House response was "[i]t is misleading and suggests approval by the President or the White House, and the White House has a long-standing policy not allowing a President's name and likeness to be used for commercial purposes."[34]

2.6.4.1 Limitations

A limitation on the tort of misappropriation occurs when there is no actual confusion. Consider voice misappropriation, for example. When a comedian imitates celebrities' voices, everyone recognizes the imitation and no one is confused about the speaker's identity. If there is no confusion, then there is no appropriated interest of the plaintiff.

Figure 2-5 Used with permission

Defenses to the claim of appropriation include:

- Newsworthiness;
- Consent; or
- The individual was not identified.

In most states, there are also different standards for a private person and someone in the public light (such as a celebrity). For example, a superstar could receive damages for the unauthorized use of their likeness, because the associated likeness has monetary value.

2.6.4.2 Examples

Meet Bobby B. and three different fact situations.

Scenario 1. Bobby B. is known as a straight shooter. However, one day Bobby drank excessively at a Pittsburgh Pirates baseball game at a company outing on company time and sponsored by his employer. Bobby was not known for being a heavy drinker, so the news spread quickly at work about his drunken behavior. The drinking took place in a public venue; hence, there was no expectation of privacy.

Scenario 2. Assume that Bobby B. got drunk at a bar in a red light district while vacationing overseas. Bobby B. tells his best friend Raymondo about his escapades. Raymondo makes a post on Ello™ about Bobby's drunken escapades. Bobby's behavior took place in a public venue; hence, there was no expectation of privacy.

Scenario 3. After a hard day at work, Bobby B. has one too many drinks while sitting alone in his backyard. His backyard is fenced in, and he cannot be seen unless someone intentionally peers over the fence. His nosy neighbor Jo peeks over the fence, observes Bobby B. drinking heavily, takes photos of Bobby with the empty beer bottles, and shares the pictures with everyone on the block. Is this a private or public venue? Is there an expectation of privacy in your fenced backyard? Many would say yes.

When you look at these factual situations, you will see that privacy is based on your physical location, whether the situation involved a private activity, and whether others were present. In addition, the privacy limits are clear. What if in scenario 2, a friend took a photo of Bobby B. in the bar and posted the photo on the Internet? Alternatively, what if Bobby B. posted a tweet describing his intoxicated state? What if, in Scenario 3, Bobby B. posted a private message on Facebook about his drinking, and posted a selfie with a drink in his hand? What if a friend posts the photo on a public blog? Yes, all the rules must be rewritten in a 24/7 technological world.

2.7 Federal and State Laws

Both federal and state laws protect an individual's privacy rights. Because each state will have its own set of privacy laws, this section will focus on key federal legislation in the privacy area.

As you learn and read about federal privacy laws, it will be clear that Congress has not stayed current with the changes in technology. This inaction makes it more difficult for current laws to be effective.

Federal laws (also called statutes), are located in a set of books called the **U.S. Code** (also known as the U.S.C.). They are categorized and organized into groupings called **titles** (*e.g.*, Title 47). Each title represents a specific subject. The laws are further broken down into groups called **sections**. Often you will see the section symbol §, used to introduce the section of a federal law. For example, 47 U.S.C. § 551 means the law is located in Section 551 of Title 47 in the United States Code.

The following laws address significant privacy issues. Each will be discussed further in this chapter. They include:

- Cable Communications Policy Act of 1984 – 47 U.S.C. § 521
- CAN-Spam Act of 2003 – 15 U.S.C. § 103
- Children's Online Privacy Protection Act of 1998 – 5 U.S.C. § 6501
- Computer Fraud and Abuse Act of 1986 – 18 U.S.C. § 1030
- Currency and Foreign Transactions Act of 1970 – 31 U.S.C. § 5311
- Electronic Communications Privacy Act of 1986 – 18 U.S.C. § 2510
- Fair Credit Reporting Act of 1970 – 15 U.S.C. § 1681
- Family Educations Rights and Privacy Act – 20 U.S.C. § 1232g
- Freedom of Information Act – 5 U.S.C. § 552
- Gramm-Leach-Bliley Act of 1999 – 15 U.S.C. § 6801
- Health Insurance Portability and Accountability Act of 1996 – 42 U.S.C. § 300gg and 29 U.S.C § 1181 and 42 U.S.C. 1320d
- Privacy Act of 1974 – 5 U.S.C. § 552a
- Privacy Protection Act of 1980 – 42 U.S.C. § 2000aa
- Right to Financial Privacy Act of 1978 – 12 U.S.C. § 3401
- Telephone Consumer Protection Act of 1991 – 47 U.S.C. § 227
- Video Privacy Protection Act of 1988 – 18 U.S.C. § 2710
- USA Patriot Act[35] (various)

2.7.1 Cable Communications Policy Act of 1984[36]

Damages Available for Cable Communications Policy Act Violations[37]
• A monetary amount equal to the amount the subscriber has been damaged; • The amount awarded can be no less than the higher of $1000 or $100 a day for each day the law has been violated; • Punitive damages; • Reasonable attorney fees; and • Court costs.

Figure 2-6

The Cable Communications Policy Act of 1984 is a law that created a "national policy concerning cable communications."[38] A portion of the law included language to protect the privacy rights of cable subscribers.

Three major privacy requirements are included in the law. First, cable companies cannot reveal individual viewing preferences without the consent of the subscriber. Second, the law required cable companies to provide subscribers with a written notice about the company's privacy practices and its process for collecting and distributing "personally identifiable information." Last, the law required cable operators to provide this notice yearly. Civil monetary damages are available for a breach of privacy as detailed in Figure 2-6.

2.7.2 CAN-SPAM Act of 2003[39]

Spam is the sending of an unsolicited email advertisement. The CAN-SPAM Act of 2003 prohibits deceptive practices in these types of emails. The law "bans false or misleading header information." In addition, subject lines must be truthful, and the email must be identified as an advertisement. The email must also include instructions how to opt out of future emails, and include a "valid physical postal address" in the message.[40]

Example of a CAN-SPAM Act of 2003 Compliant Email

Figure 2-7 Used with permission

CAN-SPAM Act – A Compliance Guide for Business[41]

Despite its name, the CAN-SPAM Act doesn't apply just to bulk email. It covers all commercial messages, which the law defines as "any electronic mail message the primary purpose of which is the commercial advertisement or promotion of a commercial product or service," including email that promotes content on commercial websites. The law makes no exception for business-to-business email. That means all email – for example, a message to former customers announcing a new product line – must comply with the law.

Each separate email in violation of the CAN-SPAM Act is subject to penalties of up to $16,000, so non-compliance can be costly. But following the law isn't complicated. Here's a rundown of CAN-SPAM's main requirements:

1. **Don't use false or misleading header information.** Your "From," "To," "Reply-To," and routing information – including the originating domain name and email address – must be accurate and identify the person or business who initiated the message.
2. **Don't use deceptive subject lines.** The subject line must accurately reflect the content of the message.
3. **Identify the message as an ad.** The law gives you a lot of leeway in how to do this, but you must disclose clearly and conspicuously that your message is an advertisement.
4. **Tell recipients where you're located.** Your message must include your valid physical postal address. This can be your current street address, a post office box you've registered with the U.S. Postal Service, or a private mailbox you've registered with a commercial mail receiving agency established under Postal Service regulations.
5. **Tell recipients how to opt out of receiving future email from you.** Your message must include a clear and conspicuous explanation of how the recipient can opt out of getting email from you in the future. Craft the notice in a way that's easy for an ordinary person to recognize, read, and understand. Creative use of type size, color, and location can improve clarity. Give a return email address or another easy Internet-based way to allow people to communicate their choice to you. You may create a menu to allow a recipient to opt out of certain types of messages, but you must include the option to stop all commercial messages from you. Make sure your spam filter doesn't block these opt-out requests.
6. **Honor opt-out requests promptly.** Any opt-out mechanism you offer must be able to process opt-out requests for at least 30 days after you send your message. You must honor a recipient's opt-out request within 10 business days. You can't charge a fee, require the recipient to give you any personally identifying information beyond an email address, or make the recipient take any step other than sending a reply email or visiting a single page on an Internet website as a condition for honoring an opt-out request. Once people have told you they don't want to receive more messages from you, you can't sell or transfer their email addresses, even in the form of a mailing list. The only exception is that you may transfer the addresses to a company you've hired to help you comply with the CAN-SPAM Act.
7. **Monitor what others are doing on your behalf.** The law makes clear that even if you hire another company to handle your email marketing, you can't contract away your legal responsibility to comply with the law. Both the company whose product is promoted in the message and the company that actually sends the message may be held legally responsible.

Figure: 2-8

2.7.3 Children's Online Privacy Protection Act of 1998[42]

The Children's Online Privacy Protection Act of 1998 (COPPA) prohibits the online collection of personal information about children under age 13 without parental consent.[43]

The law applies to operators of commercial sites targeted to (or those who knowingly collect information from) children under 13. COPPA requires these sites to have a "prominent statement link on their home page" to the website's privacy practices. The law also requires the vendor to obtain verifiable parental consent before collecting personally identifiable information from children. Enforcement of the law is through the Federal Trade Commission (FTC) and Attorney General's office for each state.

An example of protection under COPPA occurred in the 2002 case filed by the FTC against the Ohio Art Company, the makers of the well-known drawing toy Etch-A-Sketch toy. Specifically the FTC alleged that the Ohio Art Company:

> …collected the names, mailing addresses, e-mail addresses, age, and date of birth from children who wanted to qualify to win an Etch-A-Sketch toy on their birthday. The FTC charged that the company merely directed children to "get your parent or guardian's permission first," and then collected the information without first obtaining parental consent as required by the law. In addition, the FTC alleged that the company collected more information from children than was reasonably necessary for children to participate in the "birthday club" activity, and that the site's privacy policy statement did not clearly or completely disclose all of its information collection practices or make certain disclosures required by COPPA. The site also failed to provide parents the opportunity to review the personal information collected from their children and to inform them of their ability to prevent the further collection and use of this information, the FTC alleged.[44]

The lawsuit, filed in the U.S. District Court for the Northern Ohio, resulted in a settlement.[45] The Ohio Art Company agreed to pay the Federal Trade Commission $35,000 for violating COPPA by collecting personal information on children on its website without the proper parental permission.[46]

(NOTE: COPPA is not the same law as COPA. COPA or the Children's Online Privacy Act is an anti-pornography declared unconstitutional and unenforceable by the U.S. District Court in 2007 and affirmed by the Third Circuit Court of Appeals in 2008.)

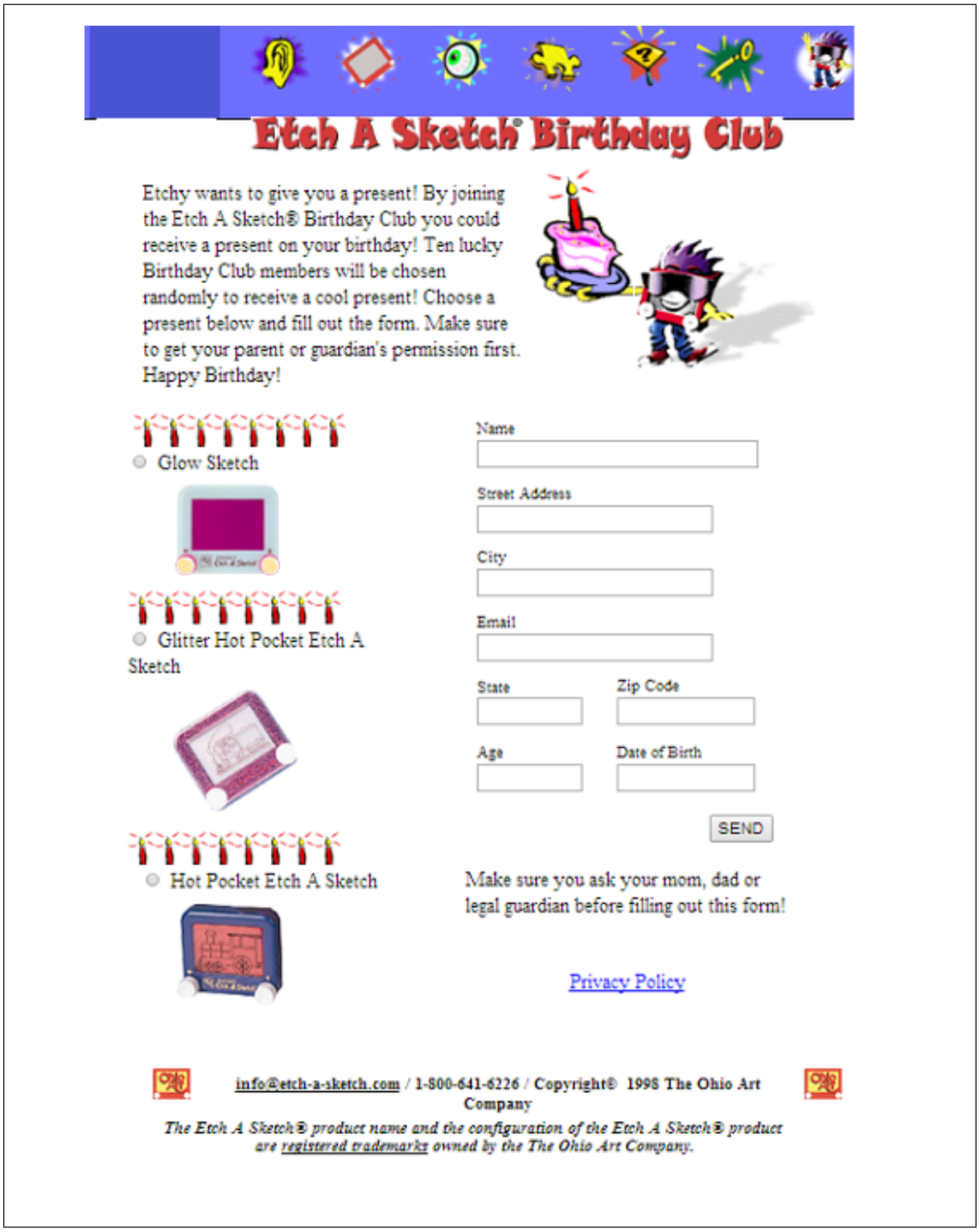


Figure 2-9[47]

2.7.4 Computer Fraud and Abuse Act of 1986[48]

The Computer Fraud and Abuse Act (CFAA) is often referred to as "the federal anti-hacking law." It sanctions criminal penalties for a person accessing a computer without authorization or exceeding their authorization. In 1994, the law was amended to provide also for civil penalties.[49]

A key provision of the CFAA protects data stored in computers owned by or benefiting the U.S. government. The law also prohibits access to consumer information located in the records of a financial institution or of a consumer-reporting agency.

Activities Considered CFAA Violations
• Obtaining national security information; • Compromising confidentiality; • Trespassing in a government computer; • Accessing to defraud and obtain value; • Damaging a computer or information; • Trafficking in passwords; or • Threatening to damage a computer.

Figure 2-10

The law is often criticized as being broadly written without clear definition of what constitutes crimes under the statute. It is an example of a law that has not been revised to reflect changes in technology.[50]

The USA PATRIOT Act[51] increased the scope and penalties of this law and first time offenders are now subject to imprisonment of 10 years.[52]

2.7.5 Currency and Foreign Transactions Reporting Act of 1970[53]

The Currency and Foreign Transactions Reporting Act of 1970 (also known as the "Bank Secrecy Act" or "BSA"), is a key money laundering statute in the United States. This law makes a federal crime to take the proceeds of an illegal activity and legitimize those funds, or to use secret bank accounts for criminal purposes. One of the most well known requirements of the law is the compulsion of businesses and financial institutions to report to the U.S. Treasury any cash transaction over $10,000, or any suspicious financial activity.[54] This information provides law enforcement with evidence to investigate and prosecute currency violations. Under the BSA, companies and banks receiving these large funds are also required to maintain strict business records.[55]

2.7.6 Electronic Communications Privacy Act of 1986[56]

The Electronic Communications Privacy Act of 1986 (ECPA) is a combination of several laws. It includes the federal Wiretap Act[57] (Title I of the ECPA), the Stored Communications Act[58] (Title II of the ECPA), and the Pen-Register Act[59] (Title III of the ECPA).

According to the U.S. Department of Justice, the ECPA "protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically."[60]

Exceptions to those required to comply with the ECPA include:

- Internet service providers (ISPs) other operators needing to access protected information in the "ordinary course of business";
- Prior consent;
- Law enforcement or government officials authorized by law; or
- A probable cause search warrant issued by a federal court.

2.7.7 Fair Credit Reporting Act of 1970[61]

The Fair Credit Reporting Act of 1970 (FCRA) ensures consumer access to credit reports and scores. Additionally, consumers must be notified if they are denied credit because of negative information in their credit report. If incomplete or inaccurate information is included in a credit report (such as caused by identity theft), an individual may dispute that information, and the credit-reporting agency must correct or delete that incomplete information or data that cannot be verified. Consumers can also restrict the sharing of their credit reports to their employers.[62]

The law was amended in 2003 by the Fair and Accurate Credit Transaction Act (FACTA),[63] and also requires the national credit reporting companies upon request, to provide a consumer with a free copy of their credit report every 12 months.

2.7.8 Family Educational Rights and Privacy Act[64]

Congress passed FERPA (known as the Family Educational Rights and Privacy Act) in 1974 to protect the privacy and accuracy of student educational records. Under this law, student educational records are confidential and may not be released without written consent. If a student is under the age of 18 and enrolled in a public school district, the student's parents or legal guardian may enforce the student's privacy rights under FERPA. Once a student turns 18, or is under 18 and enrolled in a higher education institution, all FERPA rights belong to the student.[65]

The law applies to all educational agencies and institutions who receive funding under any program administered by the U.S. Department of Education. This would include public K-12 school districts, community colleges, and four-year institutions. Private institutions rarely receive federal funds, and would not be required to follow FERPA guidelines.[66]

The law grants a parent or student the right to:

1. Review the information that the institution is or have maintained about the student;
2. Seek to amend those records and if appropriate, append a statement to the record;
3. Consent to disclosure of his/her records; and
4. File a complaint with the Family Policy Compliance Office of the U.S. Department of Education.[67]

Any records maintained by an institution directly related to a student are an educational record under FERPA.[68] However, some information, such as directory information, is deemed public and can be released without permission. This is information not regarded harmful or an invasion of privacy if disclosed, and it is often available in online student directories. However, the controlling person has the optional to keep directory information private upon notification to the educational institution.

Exclusions Under FERPA[69]

Generally, schools must have written permission from the parent or eligible student in order to release any information from a student's education record. However, FERPA allows schools to disclose those records, without consent, to the following parties or under the following conditions (34 CFR § 99.31):

- School officials with legitimate educational interest;
- Other schools to which a student is transferring;
- Specified officials for audit or evaluation purposes;
- Appropriate parties in connection with financial aid to a student;
- Organizations conducting certain studies for or on behalf of the school;
- Accrediting organizations;
- To comply with a judicial order or lawfully issued subpoena;
- Appropriate officials in cases of health and safety emergencies; and
- State and local authorities, within a juvenile justice system, pursuant to specific State law.

Figure 2-11

2.7.9 Freedom of Information Act, 1966[70]

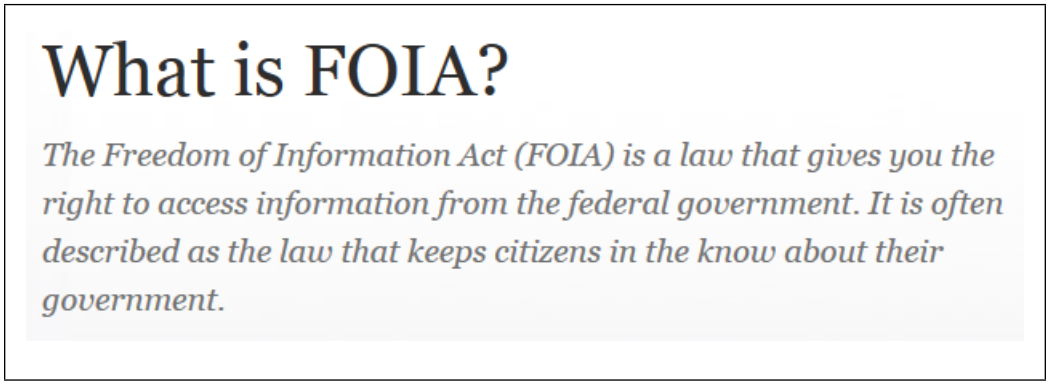


Figure 2-12[71]

The Freedom of Information Act (FOIA) is a 1966 federal law that gives individuals the right to access public information, and in particular federal agency records. Not all records can be requested under FOIA. The law restricts the release of records referred to as exclusions and exemptions. Congress has provided special protection in the FOIA for three narrow categories of law enforcement and national security records. The provisions protecting those records are known as "*exclusions*." Records falling within an exclusion are not subject to the requirements of the FOIA.[72] "Certain categories of information are not required to be released in response to a FOIA request because release would be harmful to governmental or private interests." These categories of information are known as "*exemptions*."[73] (See Figure 2-13)

Federal Records Exempt Under FOIA[74]
• Records kept secret in the interest of national security and classified secret by a Presidential Executive Order; • Records that relate to the internal personnel rules and practices of a federal agency; • Records exempted by federal law; • Information containing trade secrets and commercial or financial information that is privileged or confidential; • Agency documents that would only be available through litigation; • Personnel and medical files that would be a personal privacy violation; and • Records or information compiled for law enforcement purposes.

Figure 2-13

2.7.10 Gramm-Leach-Bliley Act of 1999[75]

This federal law instituted financial services privacy reform in the United States. It protects the privacy of consumers by requiring financial institutions to provide customers with written notice of the company's privacy policies and practices. The Gramm-Leach-Bliley Act (GLBA) also limits the disclosure of nonpublic personal information about customers to third parties and allows consumers the ability to "opt out" of third party disclosure.[76]

The law defines a consumer as an individual who obtains a financial product or service from a financial institution used primarily for personal, family, or household purposes.[77] It describes a financial institution as an organization "significantly engaged in financial activities," including lending, exchanging, transferring, investing, or safeguarding money or securities.[78] It also includes issuing vendor credit cards, such as MasterCard, American Express, and Visa. Banks, credit unions, insurance companies, and savings and loans also qualify as a financial institution.[79]

2.7.11 Health Insurance Portability and Accountability Act of 1996[80]

The Health Insurance Portability and Accountability Act (HIPAA) provides privacy protection for "individually identifiable" information contained in health care related records collected and used by medical care providers.[81] HIPAA requires health care suppliers (such a doctors, hospitals, and pharmacies) who collect medical information about patients to provide the consumer with a "Notice of Privacy Practices" that describes the personal information being collected and how the information is used.[82] Under HIPAA, patients are required to sign a form stating they have received a copy of their privacy practices when they seek medical treatment.[83] The U.S. Office for Civil Rights enforces HIPAA privacy rules.

2.7.12 Privacy Act of 1974[84]

The Privacy Act of 1974 established guidelines for federal agency disclosure of records and documents that contain personal information.[85] Personal information, such as name, photo, fingerprints, *etc*. cannot be released by the federal agency without the consent of the individual. The law, however, applies only to a "system of records."[86] The law defines a system of records as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[87] Exceptions to release include a court order, a valid search warrant, or health and safety exceptions.[88]

Each federal agency is required to publish in the ***Federal Register***[89] the type of records under its control, their physical location, and the procedures for the release of such records.[90]

Under the law, individuals also have the right to request changes to "records that are not accurate, relevant, timely, or complete."[91]

2.7.13 Privacy Protection Act of 1980[92]

This law prohibits law enforcement officers from illegally searching and seizing information from people who disseminate information to the public. The law is primarily intended to protect journalists and news reporters. This Act further requires police seek a search warrant to seize any work product created by journalists and news reporters "reasonably believed to have a purpose of dissemination to the public."[93] Dissemination could be in a newspaper, book, television broadcast, an Internet video, or other similar form of public communication.[94]

2.7.14 Right to Financial Privacy Act of 1978[95]

Under the Right to Financial Privacy Act of 1978, the federal government is required to obtain a search warrant to access bank and financial records of individuals and companies (except in situations falling under the USA Patriot Act[96]). The Patriot Act exception allows the disclosure of financial information to any intelligence or counterintelligence agency actively investigating international terrorism.[97]

This law was a reaction to the case of *United States v. Miller*, 425 U.S. 435 (1976),[98] in which the Court held that customers did not have a right to privacy for their financial records.

2.7.15 Telephone Consumer Protection Act of 1991[99]

The Telephone Consumer Protection Act of 1991, or TOPN, directs the Federal Communications Commission (FCC)[100] to establish regulations concerning telemarketing activities related to telephone solicitations and automatic dialers.[101] The FCC rules require anyone making a telephone solicitation call to provide his or her name, the name of the person or entity on whose behalf the call made, and a telephone number or address at which that person or entity can be contacted.[102]

TOPN provides that solicitors cannot use automatic dial telephone solicitations *if the called person is charged*, or send unsolicited advertisements to fax numbers. Additionally, vendors cannot make unsolicited telemarketing calls to police, fire, or other emergency numbers.[103]

2.7.16 Video Privacy Protection Act of 1988[104]

The Video Privacy Protection Act (VPPA) expanded the Cable Communications Privacy Act to restrict the disclosure of personally identifiable information for video rentals. The VPAA could also apply to the rental of games or movies over the Internet.[105]

The VPPA was passed after the video rentals of a U.S. Supreme Court Justice Nominee, Robert Bork were disclosed to the public.[106]

2.7.17 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept

and Obstruct Terrorism Act of 2001 (USA PATRIOT ACT)[107]

The USA Patriot Act was enacted in response to the terrorist attacks on the United States that took place on September 11, 2001. The law was passed to deter and punish terrorist acts in the United States and abroad.[108] According to the U.S. Department of Treasury, the goals of the law are:

- To strengthen U.S. measures to prevent, detect and prosecute international money laundering and financing of terrorism;
- To subject to special scrutiny foreign jurisdictions, foreign financial institutions, and classes of international transactions or types of accounts that are susceptible to criminal abuse;
- To require all appropriate elements of the financial services industry to report potential money laundering;
- To strengthen measures to prevent use of the U.S. financial system for personal gain by corrupt foreign officials and facilitate repatriation of stolen assets to the citizens of countries to whom such assets belong.[109]

Critics of the law argue that the law is too broad and authorizes unnecessary surveillance of U.S. citizens. In 2011, Congress passed a four-year extension of three expiring Patriot Act provisions, keeping intact the all surveillance provisions.[110]

2.8 Administrative Agency Rules and Regulations

Several federal agencies are involved in investigating violations of federal privacy laws. These include the Federal Trade Commission, the U.S. Department of Education, the U.S. Department of Justice, and the U.S. Department of Treasury. These agencies publish rules and regulations related to the enforcement of privacy laws that found in the *Code of Federal Regulations* (CFR).[111]

2.9 Summary

Privacy law in the United States is developed from five different sources: 1) the U.S. Constitution and Amendments, 2) state constitutions, 3) common law torts, 4) federal and state statutes, and 5) administrative agency rules and actions.

There is no express constitutional right to privacy, but the U.S. Supreme Court has held that privacy is a derived right. In addition, The Fourth, Fifth, Ninth, and Fourteenth Amendments are sources for this implicit right.

Invasion of privacy is a common law tort. This invasion can consist of intrusion, public disclosure of private facts, appropriation of name or likeness, or false light in the public eye.

Intrusion means intruding on a person's privacy, solitude, or seclusion. The intrusion can be physical by entering onto someone's property or by electronic or mechanical means. The tort does not require publications and the intrusion be offensive to a reasonable person.

Public disclosure of private facts involves the publications of private and embarrassing facts unrelated to matters of public concern. The disclosure of the private facts must be widespread. Therefore, information placed on the web can easily meet the disclosure requirement.

Appropriation of name or likeness occurs when someone's name, likeness, or identity is used for advertising or trade without the person's consent.

False light in the public eye exists when someone makes a false or misleading, highly offensive statement and creates a false impression to the public.

Remember that, for compliance, privacy law torts are based on common law and the precise requirements will vary from state to state.

Federal privacy laws were also reviewed in this chapter. These laws cover a variety of types of information including health, financial, and educational records.

2.10 Key Terms

Cable Communications Policy Act of 1984	Family Educations Rights and Privacy Act	Ninth Amendment
CAN-SPAM Act of 2003	Fifth Amendment	Privacy Act of 1974
Children's Online Privacy Protection Act of 1998	Fourth Amendment	Privacy Protection Act of 1980
Computer Fraud and Abuse Act of 1986	Freedom of Information Act	Public disclosure of private facts
Currency and Foreign Transactions Act of 1970	Gramm-Leach-Bliley Act of 1999	Publically placing a person in a false light
Derived right	Health Insurance Portability and Accountability Act of 1996	Right to Financial Privacy Act of 1978
Electronic Communications Privacy Act of 1986	Implied right	Telephone Consumer Protection Act of 1991
Fair Credit Reporting Act of 1970	Intrusion upon seclusion	Video Privacy Protection Act of 1988
	Misappropriation of a person's name or likeness	USA Patriot Act

2.11 Chapter Discussion Questions

1. What are the two major threats to privacy?
2. What are the five main sources of privacy law?
3. What is the difference between an express right and a derived right?
4. What is the significance of the case *Griswold v Connecticut* (1965) to privacy law?
5. What are the four main common law torts that address privacy law?
6. What is the difference between public disclosure of private facts and publically placing another in a false light?
7. Describe the CAN-SPAM Act of 1984.
8. Describe the Computer Fraud and Abuse Act of 1986.
9. How is FERPA important to a college student?
10. What is the difference between the Privacy Act of 1984 and the Privacy Protection Act of 1980?

2.12 Additional Learning Opportunities

The Electronic Privacy Information Center <http://www.epic.org>, describes itself as "is an independent non-profit research center in Washington, DC. EPIC works to protect privacy, freedom of expression, democratic values, and to promote the Public Voice in decisions concerning the future of the Internet."[112] Its website includes information on emerging privacy issues.

2.13 Test Your Learning

1. Which of the following is not a source of privacy law?
   A. The U.S. Constitution
   B. The English Constitution
   C. State constitutions
   D. Federal statutes
   E. State statutes

2. This Amendment to the U.S. Constitution is a safeguard against unreasonable searches and seizures:
   A. 2nd
   B. 4th
   C. 5th
   D. 9th
   E. 14th

3. What is a tort?
   A. A criminal case brought by the U.S. government against another private party for a wrong of one person against another.
   B. A criminal case brought by a state government against another private party for a wrong of one person against another.
   C. A civil case brought by the U.S. government against another private party for a wrong of one person against another.
   D. A civil case brought by a state government against another private party for a wrong of one person against another.
   E. A civil case brought by a private party against another private party for a wrong of one person against another.

4. Betsy accesses Kurt's bank account online without his permission. She simply views the information, and she does not attempt to access any funds from the account. Betsy's actions could constitute which of the following torts?
   A. intrusion
   B. misappropriation causing injury to a person's reputation
   C. negligent use of a computer
   D. public disclosure of public facts
   E. publically placing a person in a false light

5. Will a U.S. Court issue a warrant to search person's Facebook® account without his or her knowledge?
   A. No. The information is private and Facebook cannot be required to provide the information.
   B. Maybe. The information is private and Facebook and can only be retrieved with a court order from the U.S. Attorney General.
   C. Yes. The information is private; however, Facebook must give the information to law enforcement officials if Facebook has been served with a court order,
   D. The information is always public and no warrant is ever needed.

6. Allie Kat keeps getting unsolicited text messages on her iPhone® from the *Astro Modeling News*. She has never done business with the company. This is a potential violation of what law?
   A. Electronic Communications Privacy Act of 1986
   B. Privacy Act of 1974
   C. Privacy Protection Act of 1980
   D. Right to Financial Privacy Act of 1978
   E. Telephone Consumer Protection Act of 1991

7. C.B. is 6 ½ years old. He is very intelligent for his age and some might place his IQ at genius level. He decides to create a LinkedIn® account, but the application does not contain a certification clause that the user is over 13. LinkedIn is
   A. violating COPPA because it failed to include a provision notifying parents of its privacy practices.
   B. violating COPPA because it does not allow parents the ability to verify the personal information from its website.
   C. violating COPPA because it does not have procedures in place to protect the confidentiality of the personal information collected.
   D. not violating COPPA because LinkedIn is not a website directed to children under 13.

8. In reviewing the privacy policy for MEK Investments, Bobby finds a provision that states, "your data will be absolutely safe." This statement
   A. sets the company up for a lawsuit, as it is next to impossible to make that guarantee.
   B. is a perfectly acceptable provision to include in a privacy policy.
   C. violates the Online Personal Privacy Act.
   D. fails to comply with federal law, as it does not state what type of personally identifiable information is being collected.

9. Which of the following is an incorrect statement?
   A. Each state many have its own privacy laws.
   B. Foreign laws may apply in certain circumstances in the U.S.
   C. The greatest threat to privacy may come actually come from an individual person himself or herself.
   D. None of these are correct.
   E. All are correct.

10. The Privacy Protection Act (PPA) allows law enforcement agencies:
    A. to seize books and newspapers that threaten First Amendment rights.
    B. to seize materials from electronic publishers so long as Fourth Amendment requirements are met
    C. both a and b
    D. none of the above

Test Your Learning answers are located in the Appendix.

3 Copyright and Trademark Law

Objectives

After completing this chapter, the student should be able to:

- Define the differences between a copyright, trademark, service mark, and trade dress.
- Describe the process for a copyright registration, and works covered by copyright;
- Explain the rights of a copyright owner;
- Describe the process for registering a trademark;
- Explain the requirements for a trademark to be inherently distinctive;
- Explain the benefits of a trademark registration; and
- Define the five categories of marks.

3.1 Introduction

Types of Property
• Property is something you own. There are four types of property: • Real property (*i.e.*, land and any building affixed) • Easements (a right to use real property, such as a utility right of way or a shared driveway) • Personal property (*i.e.*, cars, jewelry, clothing) • **Intellectual (copyrights, trademarks, patents, and trade secrets)**

Figure 3-1

What is property? When most people answer this question, they think about physical possessions, such as a tablet computer, cell phone, car, clothing, *etc*. These types of possessions are referred to as **personal property**. They are movable things you might find in your home.

Property can also be land or real estate, such as a home (**real property**). However, there is a type of property not known to many called **intellectual property**. Intellectual property is a personal property right that involves originality and imagination often referred to as a "creations of the mind." **Copyrights**, **trademarks**, **trade secrets,** and **patents** are classifications of intellectual property.

Chapter Three will discuss copyright and trademark law. Chapter Four will review patents and trade secrets.

3.2 What is a Copyright?

A copyright is a legal protection given to authors for "original works of authorship."[113] An original work is one that has been independently created. A copyright only protects a tangible **form of expression**, and not the subject matter of the work of authorship. For example, a book describing the process of building a home could be copyrighted. However, the copyright would only prevent others from copying parts of the book or the entire book. Copyright would not prevent someone from writing his or her own book on home building or from actually building the home described in the copyrighted book.

What Does A Copyright Protect?[114]

"Copyright, a form of intellectual property law, protects original works of authorship including literary, dramatic, musical, and artistic works, such as poetry, novels, movies, songs, computer software, and architecture. Copyright does not protect facts, ideas, systems, or methods of operation, although it may protect the way these things are expressed."[115]

Figure 3-2

3.2.1 How is a Copyright Obtained?

The U.S. Copyright Act federally regulates copyrights.[116] This law states that a copyright attaches to a document upon creation.[117] It does not require registration for a copyright to be legally binding. However, registration is necessary to enforce the copyright and sue for copyright infringement,[118] when materials are unlawfully used without the author's permission.

Brief History of the Copyright Office

The Constitution gives Congress the power to enact laws establishing a system of copyright in the United States. Congress enacted the first federal copyright law in May 1790, and the first work was registered within two weeks. Originally, claims were recorded by clerks of U.S. district courts. Not until 1870 were copyright functions centralized in the Library of Congress under the direction of then Librarian of Congress Ainsworth Rand Spofford. The Copyright Office became a separate department of the Library of Congress in 1897, and Thorvald Solberg was appointed the first Register of Copyrights.

Today the Copyright Office is an important service unit of the Library of Congress. With public offices located at 101 Independence Avenue, S.E., Washington, D.C., the Office occupies portions of the James Madison Memorial Building and employs approximately 475 people. The Office yearly registers half a million claims to copyright, records more than 11,000 documents containing hundreds of thousands of titles, and collects for later distribution to copyright holders a quarter of a billion dollars in cable television, satellite carrier, and Audio Home Recording Act compulsory license funds. Since 1870, the Copyright Office has registered more than 33,654,000 claims to copyright and mask works and provided many millions of deposits (including books, serials, motion pictures, music, sound recordings, maps, prints, pictures, and computer works) to the collections of the Library of Congress. The Library has been greatly enhanced through the operations of the copyright system, and copyright deposits form the heart of the Library's Americana collections.

Figure 3-3[119]

Both published and unpublished works are eligible for copyright registration.[120] The U.S. Copyright Office located in the Library of Congress registers copyrights.[121]

3.2.2 Who Can Claim a Copyright?

Generally, only the author of a work can claim copyright.[122] Once the work is completed in a fixed form (such as a writing), the copyright becomes the property of the author. Joint authors of a work are co-owners of the copyright unless the authors agree make an agreement otherwise.[123]

If the work is created by an employee, the work is considered a **"work made for hire,"**[124] and the *employer* rather than the employee, is considered the author.

Statutory Definition of a Work Made for Hire[125]

A "work made for hire" is—

(1) a work prepared by an employee within the scope of his or her employment; or

(2) a work specially ordered or commissioned for use as a contribution to a collective work, as a part of a motion picture or other audiovisual work, as a translation, as a supplementary work, as a compilation, as an instructional text, as a test, as answer material for a test, or as an atlas, if the parties expressly agree in a written instrument signed by them that the work shall be considered a work made for hire. For the purpose of the foregoing sentence, a "supplementary work" is a work prepared for publication as a secondary adjunct to a work by another author for the purpose of introducing, concluding, illustrating, explaining, revising, commenting upon, or assisting in the use of the other work, such as forewords, afterwords, pictorial illustrations, maps, charts, tables, editorial notes, musical arrangements, answer material for tests, bibliographies, appendixes, and indexes, and an "instructional text" is a literary, pictorial, or graphic work prepared for publication and with the purpose of use in systematic instructional activities.

Figure 3-4

3.2.3 Rights Conferred By Copyright

Copyright provides **exclusive rights**[126] to the author. These exclusive rights include the right to:

- reproduce the work;
- distribute the work;
- copy the work;
- publicly perform the work;
- publicly display the work; and to
- produce derivative works.[127]

A **derivative work** is a transformation of an expression substantially the same as the first creative endeavor.[128] An example of a derivative work would be an author who writes a book and then contracts with a production company to create a movie based on the book. The original author of the book has the exclusive right to determine how the book's contents can be used.

Authors can also transfer their rights to a copyright. If a person has transferred or assigned their rights to another person or company (called an **agent**), the agent will have all the legal rights as the original author.[129]

Certain information cannot be copyrighted, such as works in the **public domain**.[130] Public domain works are those for which the copyright registration has expired, or which the author intends to share with the general public.[131]

3.2.4 Works Covered by Copyright

Copyright protects "**original works of authorship**." The following categories are examples of copyrightable works:

1. Literary works, such as fictional and non-fictional books, short stories, or poems;
2. Musical works including sheet music, as well as lyrics and the corresponding notes;
3. Dramatic works, such as plays or other dramatic presentations;
4. Pantomimes, choreography, pictorial, sculptural, graphic works, and motion pictures;
5. Scripts for a motion picture, as well as the movie itself;
6. Sound recordings including the recorded performance of a song; and
7. Architectural works.[132]

However, anything that is not in a fixed or tangible form of expression cannot be copyrighted.[133] Choreographic works that have not been recorded or noted could not be copyrightable. Titles, names, short phrases, slogans, symbols, and designs are not copyrightable.[134] But, they may be entitled to trademark protection if used to identify goods or services with a particular source.

Ideas, processes, systems, or discoveries are not entitled to copyright protection, but processes and systems can be protected by patents[135] (see Chapter Four) if they satisfy the other requirements for patentability.

Works that consist entirely of common property, such as standard calendars, rulers, height and weight charts, *etc*. are not copyrightable. However, pictures or other original works of authorship included in calendars are copyrightable.[136]

3.2.5 Copyright Notice

Placing a notice of a copyright on a document is not a legal requirement under U.S. law. This was a requirement prior to copyright law changes in 1989. However, it is still customary to attach a copyright notice on materials, as it is often a deterrent to infringement.[137]

Examples of a Correctly Formatted Copyright Notice[138]

Copyright 2015 Konnie G. Kustron
© 2015 Konnie G. Kustron
Copr 2015 Konnie G. Kustron

Examples of an Incorrectly Formatted Copyright Notice

(C) 2015 Konnie G. Kustron
All Rights Reserved

Figure 3-5

There are three elements required in a copyright notice. These include the copyright symbol © (or the word copyright or Copr), the year the work was published, and the name of the copyright holder.[139] The phrase "all rights reserved," often seen on documents, should not be placed on a notice. See Figure 3-5 for examples of a properly formatted copyright notice.

3.2.6 Duration of Copyright

U.S. Copyright law underwent substantial changes in 1998 with the passing of the **Sonny Bono Copyright Term Extension Act (CETA)**.[140] For copyrights created after January 1, 1978, a copyright extends 70 years past the author's death, and for 95 years for corporate copyrights. Prior to 1978, the length of a copyright was 28 years plus renewal terms of 67 years for a total of 95 years.[141]

3.2.7 What Can An Owner Do With a Copyright?

As noted earlier, a copyright owner can transfer his or her rights. However, the transfer of any of the owner's rights is invalid *unless* the transfer is in writing and signed by the owner whose rights are being conveyed. Transfers should be recorded in the Copyright Office. You can also bequeath copyright ownership upon death in a will.[142]

3.3 Registration

Formal registration of a copyright with the United States Copyright Office in the Library of Congress is *not* a requirement or prerequisite for copyright protection. Since 1978, copyright protection is obtained automatically when the work is created, fixed in tangible medium of expression, and published (*i.e.*, distributed in the public domain).[143]

However, if the author registers a copyright, there are certain benefits to registration. First, a public record is created of the copyright, which is a prerequisite to sue for infringement or unlawful use of a copyright.[144] Registration can be done "after the fact,"[145] or after the works has been published and circulated. However, early registration has a benefit. If the author registers within five years of the publication, such registration constitutes **prima facie evidence**[146] of the validity of the copyright. In other words, there is a legal presumption that the author has a valid copyright. If the registration is completed after the five-year period, validity is not presumed.[147] If no presumption exists, the author must demonstrate that he or she is the creator of the work and that the copyright ownership asserted is valid.

Prompt registration also provides for statutory damages and attorney fees in infringement actions.[148]

3.3.1 How Does An Author Obtain Registration?

Registration is a simple process, and includes sending the required forms and fees to the U.S. Library of Congress Copyright Office. These include:

1. A completed application form;
2. The correct filing fee; and
3. A non-returnable deposit of the work being registered.[149]

Documents can be sent electronically or via regular mail.[150]

Registration is effective on the date the application is received in the Copyright Office. If the application for registration is approved, a registration certificate will be issued to the author. However, a copyright can be rejected; in that case, a letter explaining the rejection will instead be provided to the applicant. Reasons for rejection include a type of work that is ineligible for copyright registration, or previous registration of the work.

Searching Copyright Records[151]

The U.S. Copyright Office provides a search function that allows the public to search copyrights on file with the Library of Congress. Searches can be completed using a keyword search or with a more specific search by title or registration number.

Figure 3-6

3.3.2 Infringement

As mentioned above, copyright **infringement** is using a person's "works protected by copyright law" without their permission. However, in copyright infringement actions, the simple use of copyrighted materials does not prove a violation of copyright law. In certain situations, the person using the copyrighted material can use the materials without the author's permission, and has several defenses to use of the work. The first is **fair use**, which is a provision under copyright law that allows the copying of copyrighted material for a limited and **"transformative" purpose**.[153] Fair use is often used to comment on, criticize, or parody a copyrighted work.

Another defense is the **"first sale" doctrine**,[154] which means a person who buys a legally produced copyrighted work may "sell or otherwise dispose" of the work as he or she sees fit. A third defense is that a work is in the **public domain**,[155] such that that the copyright to a work has expired. For example, works published prior to 1923 are in the public domain, such as the Brothers Grimm Fairy Tales (i.e. *Hansel and Gretel*), and Hans Christian Andersen Fairy Tales (*i.e.*, *The Emperor's New Clothes*.)

3.3.3 Infringement Damages

Copyright law provides for damages in a copyright infringement case.[156] First, a court can order that the works illegally used can be impounded or destroyed. Second, monetary damages can be awarded. Under copyright law, the copyright owner is entitled to recover the actual damages suffered due to the infringement, as well as any of the infringer's profits that are attributable to the infringement. Alternatively, the author can accept statutory damages that range from a "sum of not less than $750 or more than $30,000 as the court considers just."[157] If the court finds **willful infringement**,[158] then there can be an additional award of $150,000. Court costs and attorney fees can also be awarded, as well as injunctive relief.[159]

There are also criminal provisions[160] for violation of copyright law. Penalties include monetary fines and possible imprisonment.

3.4 What Is A Trademark?[161]

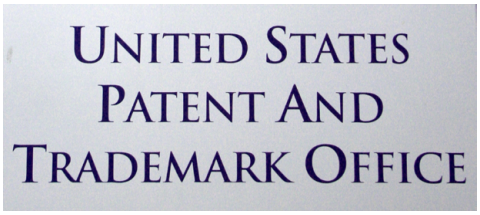


Figure 3-7 Used with permission

According to the U.S. Patent and Trademark Office (USPTO), "a **trademark** is a brand name."[162] A trademark includes "any word, name, symbol, device, or any combination used or intended to be used to identify and distinguish the goods/services of one seller or provider from those of others, and to indicate the source of the goods/services."[163] A trademark is a product identifier showing the *source of goods* used to *distinguish* the marked goods from the goods of others. It is not designed to prevent others from making the same goods or from selling the same goods or services under a different mark.

Trademarks are among the most visible items of intellectual property. A trademark for goods or products generally appears on the product itself or its packaging. Apple®[164] and Tylenol®[165] are examples of registered trademarks. A consumer will typically find the company logo for each of these trademarks both on the product and on its packaging.

What is the Difference Between a Trademark, a Patent, and a Copyright?[156]

A **trademark** is a word, phrase, symbol, and/or design that identifies and distinguishes the source of the goods of one party from those of others. A **service mark** is a word, phrase, symbol, and/or design that identifies and distinguishes the source of a service rather than goods. The term "trademark" is often used to refer to both trademarks and service marks.

Must all marks be registered? No, but federal registration has several advantages, including a notice to the public of the registrant's claim of ownership of the mark, a legal presumption of ownership nationwide, and the exclusive right to use the mark on or in connection with the goods or services set forth in the registration.

A **patent** is a limited duration property right relating to an invention, granted by the United States Patent and Trademark Office in exchange for public disclosure of the invention.

A **copyright** protects works of authorship, such as writings, music, and works of art that have been tangibly expressed.

Figure 3-8

Unlike copyrights that are filed only at the federal level, an owner can file a trademark with an individual state. However, state trademark protection is limited to the boundaries of that state. Therefore, most trademarks are registered on the federal level, providing expanded protection to the owner. The federal law, known as the **Lanham Act**,[167] governs the interstate use of trademarks. A complete listing of the regulations under the Lanham Act is available at the USPTO website.[168]

3.4.1 Service Marks

Trademark law also includes legal protection for **service marks**. A service mark encompasses the same elements as a trademark, but instead identifies services, rather than a product. Restaurants may create and register a service mark for their business, as restaurants provide a service to customers by offering meals for purchase. A restaurant's service mark, often the name of the restaurant, may appear on advertising, such as billboards or on television. The service mark Wendy's® is an example of a restaurant service mark. In the computing sector, an example of a service mark would be Rackspace®, which is known for cloud hosting.

Sample Service Mark Registration[159]

Wendy's

Word Mark	WENDY'S
Goods and Services	IC 043. US 100 101. G & S: Restaurant services, namely, providing of food and beverages for consumption on and off the premises. FIRST USE: 20120601. FIRST USE IN COMMERCE: 20130225
Mark Drawing Code	(3) DESIGN PLUS WORDS, LETTERS, AND/OR NUMBERS
Design Search Code	02.03.01 - Busts of women facing forward; Heads of women facing forward; Portraiture of women facing forward; Women - head, portraiture or busts facing forward 02.03.17 Pigtails; Ponytails; Women with ponytails or pigtails 02.05.04 - Children, girl(s); Girls 09.01.04 - Bows, decorative; Ribbons, giftwrap (gift wrap); Ribbons, hair 26.01.01 - Circles as carriers or as single line borders
Serial Number	85789042
Filing Date	November 28, 2012
Current Basis	1A
Original Filing Basis	1B
Published for Opposition	April 2, 2013
Registration Number	4460006
Registration Date	December 31, 2013
Owner	(REGISTRANT) Oldemark LLC LIMITED LIABILITY COMPANY DELAWARE 4288 West Dublin-Granville Road Dublin OHIO 43017
Attorney of Record	Valerie A. Fabbro
Prior Registrations	0935110;0936803;1269510;AND OTHERS
Description of Mark	Color is not claimed as a feature of the mark. The mark consists of the stylized word "Wendy's" to the left of a circle containing a cartoon of a smiling girl with freckles and dark hair with two pigtails each tied with a bow wearing a striped high neck blouse with a cameo broach.
Type of Mark	SERVICE MARK
Register	PRINCIPAL
Live/Dead Indicator	LIVE

Figure 3-9

3.4.2 Collective Mark and Certification Mark

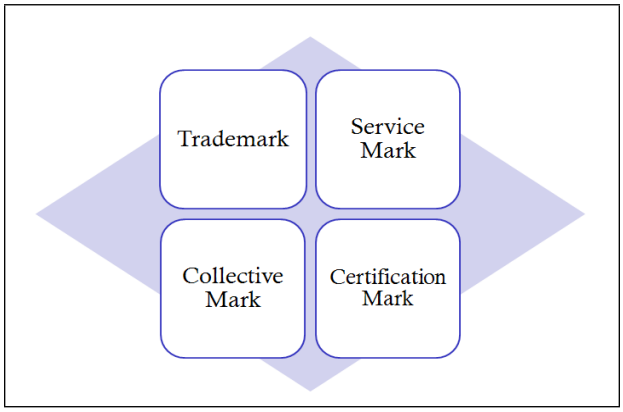


Figure 3-10

The terms "**collective mark**" and "**certification mark**" are also used in trademark law. A collective mark[170] is used by a membership organization, such as a labor union or fraternity. The mark signifies that a person or company is a member of the organization[171] (*i.e.*, Union Label®).

A certification mark[172] is a word, name, symbol, or device (or combination of) used to certify that the goods or services of another have certain features as to quality, material, or some other characteristic[173] (*i.e.*, Real Cheese®). Another example is the computer certification exam CISSP®.

3.4.3 Trade Dress

Trade dress[174] refers to the image or appearance of a non-functional, distinctive product. Trade dress can be trademarked. An example of a distinctive shape is the curved Coca Cola® bottle design.[175]

Sample Trade Dress Registration[176]
Coca Cola® bottle design

Goods and Services	IC 032. US 045. G & S: SOFT DRINKS. FIRST USE: 19160708. FIRST USE IN COMMERCE: 19160901
Mark Drawing Code	(2) DESIGN ONLY
Design Search Code	19.09.02 - Bottles, jars or flasks with bulging, protruding or rounded sides; Flasks with bulging or protruding sides; Jars with bulging or protruding sides
Serial Number	73088384
Filing Date	May 25, 1976
Current Basis	1A
Original Filing Basis	1A
Registration Number	**1057884**
Registration Date	February 1, 1977
Owner	(REGISTRANT) COCA-COLA COMPANY, THE CORPORATION DELAWARE ONE COCA-COLA PLAZA ATLANTA GEORGIA 30313
Attorney of Record	CAROLINE K. PEARLSTEIN
Prior Registrations	0696147
Description of Mark	THE MARK CONSISTS OF THE THREE DIMENSIONAL CONFIGURATION OF THE DISTINCTIVE BOTTLE AS SHOWN.
Type of Mark	TRADEMARK
Register	PRINCIPAL-2(F)
Affidavit Text	SECT 15. SECT 8 (6-YR). SECTION 8(10-YR) 20070314.
Renewal	1ST RENEWAL 20070314
Live/Dead Indicator	LIVE

Figure 3-11

3.5 Federal Registration Benefits

In the United States, trademarks are protected from their first date of public use in commerce. Registration of a mark with the U.S. Patent and Trademark Office[177] (USPTO) is not required to secure protection for a mark, but there are several reasons to obtain federal registration. Federal registration provides nationwide notice of the trademark owner's claim to the mark. This may prevent a potential user of the mark from using the design to identify their own goods or services. Second, federal registration is evidence of actual use and ownership of the mark. This can be valuable in court proceedings to determine who may use the mark. Federal registration allows the owner of the trademark access to federal courts in trademark infringement of a registered trademark.[178] Trademark infringement takes place when someone uses in a trademark in a way that causes confusion in the marketplace. Without federal registration, a trademark owner cannot invoke federal jurisdiction and would have to seek redress in a state court.

Registration is granted for ten years and renewable for additional ten, with a potential for indefinite renewals.[179] In addition, a **Declaration of Use** must be filed with the USPTO during years five and six from the anniversary of the original registration date.[180]

Federal registration can also be the basis for obtaining trademark registration in foreign countries.[171] This may be important for entities who plan to use the mark worldwide. A federally registered trademark may also be submitted to the U.S. Customs Service to prevent the importation of infringing goods.[172]

Sample Federal Trademark Registration[183]

iPhone

Word Mark	**IPHONE**
Goods and Services	IC 009. US 021 023 026 036 038. G & S: Computer gaming machines, videophones, and computer peripherals. FIRST USE: 20070629. FIRST USE IN COMMERCE: 20070629
Mark Drawing Code	(3) DESIGN PLUS WORDS, LETTERS, AND/OR NUMBERS
Design Search Code	05.09.05 - Apples
Serial Number	77353055
Filing Date	December 15, 2007
Current Basis	1A
Original Filing Basis	1B;44D
Published for Opposition	June 15, 2010
Registration Number	4425780
International Registration Number	0975076
Registration Date	October 29, 2013
Owner	(REGISTRANT) Apple Inc. CORPORATION CALIFORNIA MS: 36-4TM 1 Infinite Loop Cupertino CALIFORNIA 95014
Attorney of Record	Thomas R. La Perle
Priority Date	June 22, 2007
Prior Registrations	2715578;2753069;2870477;3669402;AND OTHERS
Description of Mark	Color is not claimed as a feature of the mark. The mark consists of a design of an apple with a bite removed.
Type of Mark	TRADEMARK
Register	PRINCIPAL-2(F)-IN PART
Live/Dead Indicator	LIVE
Distinctiveness Limitation Statement	AS TO "IPHONE"

Figure 3-12

3.5.1 Initial Registration Steps

The first step in the registration process is to determine whether a potential "mark" meets the requirements of trademark protection. This begins with a trademark search. Although this is not a filing requirement, it is recommended to perform a search prior to applying for federal registration. Performing a search can save time and money if a mark is already in use and is registered by another party. Individuals can perform a search through the USPTO's **Trademark Electronic Search System (TESS)**.[184] Additionally, a trademark attorney or a professional search organization can perform searches.

A search will determine whether a proposed mark conflicts with an existing mark. Even though there might be an existing or similar mark, it is possible the mark can still be registered. The key registration determination is whether there is a likelihood of confusion between the marks. In other words, would consumers be likely to confuse the goods or services of one party with those of the other party based on their marks? When searching for conflicting marks, the marks neither have to be identical, nor do they have to be on the same types of goods or services for the marks to cause a likelihood of confusion.

For example, LEXIS® is a computerized legal research service. LEXUS® is an automobile manufacturer. Their names are pronounced the same, but the words are spelled differently. More importantly, the trademarks are in two different industries, and there is very little likelihood of confusion between the two trademarks. Therefore, both names can and have been registered as trademarks.[185]

If no conflicting marks are found, an application for federal registration can proceed.

3.5.2 Mark Format

If the trademark appears to meet the legal requirements, the owner should determine the correct format of the mark. Letters, numbers, or a combination of these can be trademarked.

There are three types of mark format: a **standard character mark**, a **stylized/design mark**, and a **sound mark**.[186]

Standard Character Mark	Stylized/Design Mark	Sound Mark
This format protects words, letters, numbers, or a combination of these. No particular font, size, color, or design is included in the mark.	This format protects words, letters, numbers, or a combination of these using a particular font, size, color or design is included in the mark.	Sounds or a combination of sounds comprise the mark.
[187] FORD	[188] Ford	The roar of the Metro-Goldwyn-Mayer (MGM) lion roar.

Figure 3-13

3.5.3 Categories of Marks

A trademark must be "**inherently distinctive**."[189] A mark that is not distinctive cannot generally be registered. When filing a trademark, the mark cannot be descriptive of the product or service (such as a fast car or a sweet drink). Instead, the mark has to represent and identify the product or service to the public through its distinctiveness.

There are five categories of marks. They are listed in ranked order. Categories one and two are not distinctive, and marks holding these characteristics cannot be registered. Categories three through five meet the inherently distinctive threshold, and can be trademarked.

The five categories include the following:

1. A **generic term** is a common name of a product such as a car, computer, or motherboard. These are not protectable and cannot be registered.
2. A **descriptive mark** describes something about a product or service by depicting some characteristic, quality, ingredient, function, feature, purpose, or use of the product or service. Because a descriptive term describes goods or services rather than identifies the source of the product, they cannot be registered until the mark is associated with a single source. This association is called **secondary meaning of acquired distinctiveness**. This happens after five years of continuous and exclusive use of a mark. This can also be shown by advertising or customer surveys. If a secondary meaning can be shown, the mark can eventually be registered.

3. A **suggestive mark** implies something about the goods or services offered under mark, but it does not immediately describe them. For example, Greyhound Bus®[190] has been held by the courts to be a suggestive mark as a greyhound is a dog known for speed. A suggestive mark does not need to acquire a secondary meaning to be registered. A suggestive word mark requires some mental exercise to make the connection between the mark and the good or service.
4. An **arbitrary mark** is a commonly known word that is applied to an unfamiliar product. Arbitrary marks may be registered without proof of secondary meaning. Apple® is an example of an arbitrary mark, as Apple® Computer has no relationship with the apple fruit.
5. **Fanciful or coined marks** are those that are invented and have no dictionary meaning. Honda®[191] would be an example of a coined mark. Both automobile manufacturers and pharmaceutical companies often create fanciful marks. These are your strongest marks and they are entitled to the greatest level of legal protection.

3.6 Rights of Mark Ownership

There are two types of rights associated with trademarks: the right to use the mark and the right to register the mark. The right to use the mark is generally based on who actually used the mark first. Only a court can ultimately decide who has the right to use the mark. Proceedings to determine this right can be very complicated, especially if neither party has a federal registration. Again, federal registration can provide benefits to a trademark owner in a court proceeding of this type, such as collecting treble damages for trademark infringement.[192]

3.7 Trademark Symbols

There are three possible symbols to use with a mark. They include TM, SM and ®. Such symbols are placed to the right of the mark in a superscript position.[193]

The letters "TM" stand for trademark and "SM" for service mark. They can be used by anyone who claims to have rights in the mark. These designations are useful to alert other parties of the purported rights in the mark. Federal registration is unnecessary to use these symbols with a trademark or service mark. These symbols do not establish conclusive rights to use the mark. Again, only a court can ultimately determine who may use the mark.

On the other hand, the letter R is a trademark registration symbol. It is signified by a capital letter R enclosed by a circle such as a ®. This symbol should not be used until a federal registration is obtained.

3.8 Additional Registration Steps[194]

Once the mark is identified, the goods or services that the mark will identify are determined,[195] a database search is completed, and the basis for filing is determined, an application must be completed and filed with the USPTO. A clear drawing[196] of the mark must be included with the application. An application fee must also be enclosed.

The application can be written and filed by mail, but most are filed electronically though the USPTO Trademark Application System.

Upon receipt by the USPTO, the application is reviewed to ascertain whether the federal filing requirements are met. If the filing requirements *are not* met, then the USPTO returns the entire application including the filing fee to the applicant. If the filing requirements *are* met, the USPTO will send the applicant a receipt about two months after the application is filed. An examiner (who is an attorney), will review the application about four months after filing.

The examiner will search registered marks and pending registrations to determine if there are any conflicting marks. The examiner uses the *likelihood of confusion* standard in this evaluation. If the examiner decides that the mark cannot be registered, the examiner may issue a letter to the applicant stating any grounds for the refusal. Alternatively, the examiner may contact the applicant by telephone, especially if only minor corrections are needed.

The applicant has six months from the mailing date of the examiner's letter for responding to any objections. If the applicant fails to respond, the application is considered abandoned. If the applicant fails to overcome the examiner's objections, then the examiner issues a final refusal. Applicants may appeal a final refusal to the **Trademark Trial and Appeal Board**,[197] which is an administrative panel within the USPTO.

3.9 Reasons for Registration Refusal[198]

There are three main reasons the U.S. Patent and Trademark Office may refuse to register a trademark:

1. Refusal because of a **confusing similarity** with a prior registered or pending registration. The proposed trademark does not have to be for the same type of goods or services for confusion to be found, as long as the marks are related in some manner.
2. Refusal based on **descriptiveness**. This is a serious refusal. In response to this decision, the applicant can argue the mark is not descriptive but suggestive, and it should be registered. The applicant could argue that the cases cited by the examiner in support of the refusal to register are inapplicable. Alternatively, if the mark has been in commerce over five years, there is a presumption of acquired distinctiveness.
3. Refusal based on geographical indication. This mark identifies "a good as originating in the territory of a Member, or a region or locality in that territory, where a given quality, reputation or other characteristic of the good is essentially attributable to its geographic origin."[199] "Under US trademark law, geographic terms or signs are not registrable as trademarks if they are geographically descriptive or geographically misdescriptive of where the goods/services originate."[200]

3.10 Notice of Publication

If the applicant overcomes all of the objections to registration, then the USPTO will send a **Notice of Publication** to the applicant stating the date the mark will be published in the ***Official Gazette*****,** which is a weekly publication of the USPTO. The mark will then be published.[201]

Any other party, who feels they will be injured by the registration of the trademark, may file an opposition within thirty days of the publication in the *Gazette.* An opposition proceeding would then be held before the Trademark Trial and Appeal Board. An example in which a party might oppose a registration would be a party using a similar mark for similar goods or services who possessed no federal registration.[202]

If no opposition is filed or if the opposition fails, the USPTO will issue a registration certificate or a **Notice of Allowance** to the applicant. A registration certificate will be issued if the application was based on actual use of the mark in commerce. If the application was based on an intent to use the mark, then the USPTO will issue a Notice of Allowance. After a Notice of Allowance is issued, the applicant has six months to use the mark and file a statement of use. Once the statement of use is approved, a registration certificate will be issued. Alternatively, the applicant can file for an additional six-month extension in which to use the mark and in certain circumstances, may file for additional extensions.[203]

3.11 Federal Trademark Dilution Act

As mentioned previously, a trademark owner can sue for trademark infringement when someone unlawfully uses another's trademark that causes confusion in the marketplace. The Lanham Act governs infringement actions.[204] However, the unlawful use of a trademark can also cause dilution. Dilution happens when there is a blurring or tarnishment of the mark, and the value of the mark is reduced. Until the Federal Trademark Dilution Act of 1995[205] went into effect, there was no federal law that provided for dilution actions. In 2006, the Trademark Dilution Revision Act (TDRA)[206] amended the Federal Trademark Dilution Act. This revision clarified certain ambiguities in the law and provides for "dilution by tarnishment" as a cause of action. The TDRA defines dilution by tarnishment as an "association arising from the similarity between a mark or trade name and a famous mark that harms the reputation of the famous mark."[207]

3.12 Anti-Cybersquatting Consumer Protection Act

Cybersquatting" is a term defined by the courts as "the bad faith, abusive registration and use of the distinctive trademarks of others as Internet domain names, with the intent to profit from the goodwill associated with those trademarks."[208] In the early growth of the Internet, cybersquatting was a common problem, in which websites using the names of well-known companies would be registered, only to be later sold at a profit.

The Anti-Cybersquatting Consumer Protection Act (ACPA),[209] (15 U.S.C. § 1125(d)) was enacted in 1999 to protect trademark owners from these types of domain abuses. The purpose of the Act is to "protect consumers and American businesses…by prohibiting the bad-faith and abusive registration of distinctive marks as Internet domain names with the intent to profit from the goodwill associated with such marks – a practice commonly referred to as 'cybersquatting.'"[210]

Violators of the law can be ordered to forfeit or cancel the illegal obtained domain name or to transfer the domain to its rightful owner. In addition the mark owner can recover losses sustained by the domain registrant's actions, and the actual damages (*i.e.*, defendant's profits from use of the domain) the plaintiff suffered. The plaintiff can also elect to recover statutory damages instead of actual damages ($1000 to $100,000 per domain).[211]

The Court Speaks

Ford Motor Company v. 2600 Enterprises, 177 F. Supp. 2d 661 (E.D. Mich. 2001)[212]

Facts:

"The essential facts in this case are undisputed. Defendants 2600 Enterprises and Eric Corley, a.k.a Emmanuel Goldstein, are the registrants of the domain name 'f**kgeneralmotors.com.' When an Internet user enters this domain into a web browser, he is automatically linked to the official website of Plaintiff Ford Motor Company ("Ford"), which is located at 'ford.com.' Defendant Corley, a self-proclaimed "artist and social critic," apparently considers this piece of so-called cyberart one of his most humorous. Ford is not amused. Hence, the instant complaint alleging three Lanham Act violations: trademark dilution, 15 U.S.C. § 1125(c); trademark infringement, 15 U.S.C. § 1114(1); and unfair competition, 15 U.S.C. § 1125(a)." (p. 661–662)

Discussion:

A. Dilution

"In relevant part, the Federal Trademark Dilution Act ("FTDA"), codified at 15 U.S.C. § 1125(c), provides that

> [t]he owner of a famous mark shall be entitled…to an injunction against another person's commercial use in commerce of a mark or trade name, if such use begins after the mark has become famous and causes dilution of the distinctive quality of the mark.

At issue in this case is whether Defendants' use of the FORD mark is 'commercial.'" (p. 663)

"…While arguably neither news reporting, competitive advertising, parody, nor criticism is at issue in this case, and although Defendants' use of the term 'art' hardly seems apropos, the court is satisfied that Defendants' use of the word 'ford' in their programming code is, at least, 'noncommercial.' Their use thus is not actionable under the FTDA. If the FTDA's "commercial use" requirement is to have any meaning, it cannot be interpreted so broadly as to include any use that might disparage or otherwise commercially harm the mark owner." (p. 665)

B. Infringement and Unfair Competition

"Plaintiff similarly has failed to allege facts sufficient to show a likelihood of succeeding on the merits of its infringement and unfair competition claims. Pursuant to 15 U.S.C. § 1114(1) (a), to succeed on an infringement claim, a plaintiff must show that the defendant has used the mark 'in connection with the sale, offering for sale, distribution, or advertising of any goods or services.' An essentially identical showing of use 'in connection with any goods or services' is required on an unfair competition claim. 15 U.S.C. § 1125(a).

Plaintiff here has made no allegation that Defendant has used the Ford mark in connection with goods and services in any literal sense." (p. 665)

Conclusion:

For the reasons set forth above, while Plaintiff understandably may be disturbed by Defendants' acts, the Lanham Act provides no remedy… (p. 666)

Questions:

1. What was the Court's reasoning there was no remedy available to the Plaintiff?
2. Why did Ford sue under the Lanham Act and not under the Anti-Cybersquatting Consumer Protection Act?

3.13 Summary

Copyright is a form of legal protection provided to the authors of "original works of authorship" *i*ncluding *literary*, *dramatic*, *musical*, *artistic*, and certain other intellectual works, both published and unpublished. Copyright only protects the expression of ideas, but not the ideas themselves. A copyright gives the author and others who have been authorized the **exclusive rights** to the copyrighted work, such as assignment of the copyright and the creation of derivative works. The Copyright Office of the U.S. Library of Congress handles all registration. Copyright protection, based on Title 17 of the U.S. Code, only lasts for a limited period, and when a copyright expires, the work enters the public domain.

A trademark is a legal protection for a brand. It is a product identifier showing the *source of goods* to *distinguish* from the goods of others. It is not designed to prevent others from making the same goods or from selling the same goods or services under a different mark. A service mark protects a service in the same manner as a trademark.

Trademarks and service marks are used to prevent others from using a confusingly similar mark. Often times the trademark is registered with the U.S. Patent and Trademark Office. Benefits to federal registration include:

- constructive notice to the public of the registrant's claim of ownership of the mark;
- a legal presumption of the registrant's ownership of the mark and the registrant's exclusive right to use the mark nationwide on or in connection with the goods and/or services listed in the registration;
- the ability to bring an action concerning the mark in federal court;
- the use of the U.S. registration as a basis to obtain registration in foreign countries; and
- the ability to file the U.S. registration with the U.S. Customs Service to prevent importation of infringing foreign goods.[213]

Trademark categories include generic, descriptive, suggestive, arbitrary, and fanciful or coined mark. Trademarks must be inherently distinctive to be registered. Generic and descriptive trademarks do not meet this legal threshold. Registration refusal can be based on being confusing similarity, descriptiveness, or geographical indication.

The Federal Trademark Dilution Act is a legal remedy for use of another's mark that causes confusion in the marketplace.

The Anti-Cybersquatting Consumer Protection Act is a law that provides a remedy available to those who register a domain name in bad faith with the intent to profit from its registration.

3.14 Key Terms

Agent	Exclusive rights	Sonny Bono Copyright Term Extension Act (CETA)
Anti-Cybersquatting Consumer Protection Act	Fanciful or coined mark	Sound mark
Arbitrary mark	Generic term	Standard character mark
Certification mark	Geographical indication	Stylized/design mark
Collective mark	Infringement	Suggestive mark
Confusing similarity	Inherently distinctive	Trade dress
Copyright	Intellectual property	Trade secret
Cybersquatting	Lanham Act	Trademark
Declaration of Use	Library of Congress	Trademark Electronic Search System (TESS)
Derivative work	Notice of Allowance	Trademark Trial and Appeal Board
Descriptive mark	Notice of Publication	Trademark symbols
Descriptiveness	*Official Gazette*	Transformative purpose
Easement	Original works of authorship	U.S. Copyright Act
Fair use	Patent	U.S. Copyright Office
Fanciful mark	Personal property	Willful infringement
Federal Trademark Dilution Act	Public domain	Work made for hire
First sale doctrine	Real property	
Form of expression	Secondary meaning of acquired distinctiveness	
Generic term	Service mark	

3.15 Chapter Discussion Questions

1. What type of creative property does a copyright cover?
2. Can website content be copyrighted (such as text, images, or templates)?
3. How is copyright protection obtained?
4. What is an "original work of authorship"?
5. What is the first sale doctrine?
6. What is the difference between a copyright and a trademark?
7. Provide an example of trade dress not discussed in the text.
8. Describe the proper use of a trademark symbol.
9. What is the difference between the five categories of marks?
10. What is the Anti-Cybersquatting Consumer Protection Act?

3.16 Additional Learning Opportunities

The U.S. Copyright Office has several Circulars that provide information on the basics of copyright law. These materials are available at http://copyright.gov/circs/.

Visit the USPTO at http://www.uspto.gov/trademarks/basics/BasicFacts.pdf for a circular on the basics of trademarking.

3.17 Test Your Learning

1. A copyright protects:
   A. a form of expression
   B. ideas
   C. names, titles, or short phrases or expressions
   D. the subject matter of a work
   E. works in the public domain

2. Betty B. researches and writes a paper for her high school English class. The paper can be copyrighted by:
   A. Betty B.
   B. Betty B.'s school
   C. Betty B.'s principal
   D. the school board for Betty B.'s school district
   E. the teacher in the English class

3. Which is the following is a correctly formatted copyright notice?
   A. all Rights Reserved
   B. (c) Patrick Nuckolls
   C. (c) Patrick Nuckolls All Rights Reserved
   D. copyright 2015 Patrick Nuckolls
   E. Notice of Copyright 2015 Patrick Nuckolls

4. Ademar Partida was born in 1951. He copyrighted a book in 2000. Partida died in 2012. The copyright on his book is valid until what date?
   A. 28 years past his death or until 2040.
   B. 67 years past his death or until 2079.
   C. 70 years past his death or until 2082.
   D. 95 years past his death or until 2107.

5. You have developed a blog site for your employer called "Law and Knowledge Management" that focuses on legal issues in the information assurance field. You want to take an **article** from *The Daily Information Security News* and reproduce the article on the blog. Which of the following best represents your next step?
   A. Because the materials are in the public domain, you can simply copy and place them on your web page.
   B. Because the materials are in the public domain, you can simply copy and place them on your web page as long as you acknowledge the source of article.
   C. The materials are not in the public domain, but you can still simply copy and paste them on your web page as long as you acknowledge the source of the copyrighted materials.
   D. You can only place a link on the blog to the *Daily News* without violating U.S. copyright law.
   E. None of the above

6. What type of mark would the company name TranServ (a combination of the words transportation and service) be for a transportation company?
   A. generic
   B. descriptive
   C. suggestive
   D. arbitrary
   E. fanciful

7. George and Jude Jetts own a company called GeJuJet that is a reputation defender service. They want to trademark their company name. Can they trademark GeJuJet when it represents a service and not a "good"?
   A. No, trademarks are only for goods.
   B. No, trademarks are only for services.
   C. They cannot trademark their company name, but they can create a service mark.
   D. This is a copyright issue and not a trademark issue.

8. Assume that the Mid Central-American Conference (MCAC), an athletic conference of Division III colleges, creates a mark that can be used by all the association schools. This mark is known as a
   A. certification mark
   B. collective mark
   C. service mark
   D. trademark
   E. song mark

9. What is the initial term of a trademark?
   A. five years
   B. 10 years
   C. 20 years
   D. 50 years
   E. 75 years

10. A colored design or shape associated with a product is best described as:
   A. collective mark
   B. framing
   C. service mark
   D. trademark
   E. trade dress

Test Your Learning answers are located in the Appendix.

4 Trade Secrets and Patents

Objectives

After completing this chapter, the student should be able to:

- Define what type of business information can receive trade secret protection;
- Describe the main elements of the Uniform Trade Secrets Act;
- Understand the measures a business should take to protect a trade secret;
- Define what type of intellectual property can be patented;
- Describe some elements of the America Invents Act;
- Explain the four categories of patentable subject matter; and
- Describe the U.S. patenting process.

4.1 What is a Trade Secret?

A **trade secret** is commercial information that gives a business a competitive advantage over other companies. Trade secrets can include inventions, ideas, or compilations of data used by a business. As long as the information has economic value to the company, it can be a trade secret.

Trade secrets can include any useful formula, plan, pattern, process, program, tool, technique, mechanism, compound, or device that is not generally known or readily ascertainable by the public.

Figure 4-1

The whole idea behind a trade secret is that the trade secret be kept internal and private, so there is no public registration requirement. If the information is shared with a third party, secrecy protection is lost. Therefore, it is critical that the owner of the information take reasonable steps to maintain the confidentiality of the information. Because there is no government regulation or filing requirement, there is no public disclosure and the trade secret can remain private for unlimited time.

4.2 Protecting the Trade Secret

When protecting trade secrets, a common problem involves theft and misappropriation by employees. For example, a disgruntled employee will often intentionally disclose a secret. On the other hand, well-meaning employees routinely divulge trade secrets to trade show attendees, job candidates, the press, and other third parties. The key to protection is the education of employees to avoid their unintentional release of confidential information.

To acknowledge the importance of confidential information, any organization with a trade secret should have a comprehensive written policy emphasizing the importance of secrecy. This policy should identify what type of information is a trade secret, indicate that the information cannot be shared (internally or externally), and require employees to acknowledge in writing their understanding of this information.

It does not make sense for a company to say everything is secret, because both employees and courts will not take the policy seriously if everything is suddenly important. It is critical that a company share the trade secret only with those employees who need that information to perform their jobs.

Last, a company should have a formal process of periodic review called a trade secret audit. This type of review should determine what information should be kept secret, and who should have access to the material. Those individuals performing the audit would normally be trusted personnel who can identify the trade secrets and act appropriately to secure them.

Besides a written policy, other common education and protection measures include:

1. restricting physical access to the information (such as placing the information in a bank vault);
2. limiting the number of people with knowledge of the trade secret;
3. requiring those having knowledge of the trade secret to agree in writing not to disclose the information (called a confidentiality or non-disclosure agreement[204]); and
4. requiring employees who encounters the trade secret, directly or indirectly, to a sign non-disclosure agreement.

Whenever any information is represented as a trade secret, again a business must use its best efforts to safeguard it from disclosure.

4.3 Length of Protection

Trade secrets can potentially last forever. This is in contrast to other intellectual property, such as a copyright or patent, which have expiration dates.

Did You Know?

One of the most well-known and oldest trade secrets is the Coca-Cola® soft drink formula. Reportedly, pharmacist John Pemberton developed the "secret recipe" in 1886, but it was not until 1919 that the formula was documented in writing.[215] It was rumored for many years only a few executives knew the formula, and that a copy of the recipe was placed in a safe deposit vault with an Atlanta, Georgia bank. However, in 2011 the Company announced that it moved the secret formula to the World of Coca-Cola Exhibit in downtown Atlanta,[216] where it now resides.

Figure 4-2

4.4 Legal History

The unlawful sharing of trade secrets is a tort based on English **common law**. As discussed in Chapter Two, common law is a legal system that originated in England in the Middle Ages when medieval kings handled disputes following a process of "fairness, custom, and common sense."[217]

Common law describes the unlawful taking or use of a trade secret as the **intentional tort of misappropriation**.[218]

4.5 Uniform Trade Secrets Act

In 1939, a professional group of attorneys known as the American Law Institute[219] summarized the common law doctrines that dealt with trade secrets. Their efforts were compiled in a book called the ***Restatement of Torts***. The *Restatement of Torts* (1939) has no binding legal effect on the courts, but influences and brings about uniformity in judicial decision-making. In 1979, the National Conference of Commissioners on Uniform State Laws,[220] a non-profit organization with representatives from all fifty states and territories, took the language in the *Restatement,* and drafted language for proposed **model (uniform) law** called the **Uniform Trade Secrets Act (USTA**). The purpose of a model law is to encourage uniformity of language throughout the U.S. to simplify business operations in multiple states. Having identical or similar language across state jurisdictions makes compliance and enforcement of trade secrets a more efficient process.

The USTA (amended in 1985) incorporated the elements of the common law tort of misappropriation as defined in the 1939 version of the *Restatement of Torts.* The language in the model law was shared with the legislatures in all 50 states and U.S. territories. As of 2014, only a few states such as New York and North Carolina have not adopted the USTA.[211]

The National Conference of Commissioners on Uniform State Laws language in the USTA includes common definitions for terms such as *misappropriation*, *trade secret*, *person,* and *improper means*.[222] Violation of the law is a civil dispute. Remedies under this law include an injunction, monetary damages, and attorney fees.[223] In addition, many states have laws specifically criminalizing the theft of trade secrets. Often this violation falls under larceny, theft, or computer crime laws.

Figure 4-3 includes sample language from Michigan's Uniform Trade Secrets Act. This language is representative of wording in the model law.

Michigan Compiled Laws 445.1902
As used in this act:
(a) "Improper means" includes theft, bribery, misrepresentation, breach, or inducement of a breach of a duty to maintain secrecy or espionage through electronic or any other means.
(b) "Misappropriation" means either of the following:
(i) Acquisition of a trade secret of another by a person who knows or has reason to know that the trade secret was acquired by improper means.
(ii) Disclosure or use of a trade secret of another without express or implied consent by a person who did 1 or more of the following:
(A) Used improper means to acquire knowledge of the trade secret.
(B) At the time of disclosure or use, knew or had reason to know that his or her knowledge of the trade secret was derived from or through a person who had utilized improper means to acquire it, acquired under circumstances giving rise to a duty to maintain its secrecy or limit its use, or derived from or through a person who owed a duty to the person to maintain its secrecy or limit its use.
(C) Before a material change of his or her position, knew or had reason to know that it was a trade secret and that knowledge of it had been acquired by accident or mistake.
(c) "Person" means an individual, corporation, partnership, association, governmental entity, or any other legal entity.
(d) "Trade secret" means information, including a formula, pattern, compilation, program, device, method, technique, or process, that is both of the following:
(i) Derives independent economic value, actual or potential, from not being generally known to, and not being readily ascertainable by proper means by, other persons who can obtain economic value from its disclosure or use.
(ii) Is the subject of efforts that are reasonable under the circumstances to maintain its secrecy.

Figure 4-3

4.6 Disputes

In a trade secret dispute, disagreements can be handled informally or through the courts. If a person or organization has had a trade secret misappropriated and litigation is necessary, the trade secret holder has the option to sue on the state or federal level. Where the litigation is filed depends on the type of breach. For example, a theft based on the UTSA would be a violation of a state law and filed in a state court.

To prevail in a USTA trade secret case, two elements must be proved. The plaintiff will need to demonstrate that a trade secret existed, and that the secret was misappropriated. The misappropriation can be substantiated by establishing the information had financial value, and based on that value plaintiff took certain actions to secure the information (such as it spent large sums of money or expended considerable time developing the secret information). The plaintiff will have to also demonstrate that the defendant had access to the information, and that the information was used in a competitive disadvantage to the plaintiff.

How Can a Defendant Respond to a Trade Secret Lawsuit?
In defense and in response to a trade secret breach, a defendant could argue the following: 1. The information does not meet the requirements for a trade secret, and even if it did, 2. I/we did not have access to the information, and even if I/we did have access, 3. I/we did not know that the information was a trade secret, and even if I/we did know that, 4. I/we did not use information anyway, and even if we did use it, 5. Plaintiff was not damaged.

Figure 4-4

If an unsuspecting **third party** receives a trade secret and uses the trade secret, but does not know the information is secret, then a plaintiff's case for damages is weakened.

4.7 Remedies

Anyone found liable for misappropriating a trade secret can be ordered to pay the owner actual damages for economic losses, unjust enrichment,[224] or for even a royalty fee. A judge may award an injunction (court order) to stop the unlawful dissemination of the information. If the misappropriation is willful or malicious, the court may award attorney fees and double damages.[225]

4.8 Additional Federal Laws

In addition to the Uniform Trade Secrets Act, two other key laws concern trade secrets. These include the **Economic Espionage Act (EEA)**[226]and the **National Stolen Property Act**,[227] both of which are federally based.

The Economic Espionage Act of 1996 prohibits any attempt to steal trade secrets for the benefit of someone other than the owner, including for the benefit of any foreign government. The EEA was enacted in response to the fear that the United States could not maintain its industrial and economic edge or safeguard national security. The National Stolen Property Act criminalizes the transportation of stolen goods valued in excess of $5000.00.

4.9 What is a Patent?

A patent is a **property *right*** (*emphasized*) granted by the U.S. government. A patent is a different type of intellectual property, as it is an **exclusion right**. This means a patent grants the holder the right to exclude others from "making, using, offering for sale, or selling the (their) invention in the United States."[218] The boundaries of the invention are governed by the claims of a patent.

The federal government grants patents.[229] Article I, Section 8, Clause 8 of the U.S. Constitution authorizes the federal government to issue patents. This section reads in part, "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 right to their respective writings and discoveries."

4.10 America Invents Act[230]

In 2013,[231] U.S. patent law underwent major changes to be more consistent with the patent statues of other countries. The Leahy-Smith **America Invents Act** (AIA) took the United States from a **first to invent** country to a **first inventor to file (FITF)** system. In other words, patents are awarded to the inventor who first files their application with the U.S. Patent and Trademark Office.

Figure 4-5[232]

Prior to the America Invents Act, it was presumed that the inventor who first **reduced the invention to practice**[233] was entitled to the patent. This differed greatly from the rest of the world that used a first to file priority system. The old law placed the U.S. in a different posture from other countries, which often caused legal complications for individuals and companies who wanted to secure international patent protection for their product.

Why File a Patent?
The main goal of patent law is to increase the pool of technical knowledge in the United States by encouraging inventors to disclose to the country (and effectively to the world) the details of their inventions. In return, the federal government grants the inventor a limited monopoly to exclude others from using the patent. The government is also interested in having inventors disclose their inventions as early as possible. It has rewards for early disclosure of inventions and penalties for waiting too long.

Figure 4-6

4.11 Patent Rights

A patent is a legal grant awarded to the inventor (**patentee**). A patent does not confer ownership, but a legal right. The U.S Patent and Trademark Office issues a patent for a limited time in exchange for a full disclosure of the invention.[234]

An inventor does not need a patent to make, use, or sell the invention claimed in a patent. However, the owner of the patent may not use, make, or sell an invention if doing so would violate the law. For example, assume an inventor creates a road rage button that blinks bright red lights in his rear car window. If a driver aggravates him, he can flash the lights to get the attention of that driver. Because those lights would interfere with traffic safety, the creator of the patent would not be entitled to use the road rage button on the highway, but he could still be awarded the patent.

4.12 Categories of Patentable Subject Matter

Patent laws specify the subject matter that is appropriate for a patent and the conditions for patentability.[235]

Four key areas can be patented. They include **process**, **machine**, **manufacture**, and **composition of matter**.[236] A patent claim must fit the criteria for one of these categories to be eligible for grant as a patent.

A process is an act or method; these are primarily industrial or technical processes.[237] A machine is "a concrete thing, consisting of parts, or of certain devices and combination of devices."[238] Manufacture includes "an article produced from raw or prepared materials by giving to these materials new forms, qualities, properties, or combinations, whether by handlabor (sic) or by machinery."[239] Composition of matter involves chemical compositions that may include mixtures of ingredients as well as new chemical compounds.[230]

In the area of Internet law, business methods patents are a growing field, though their patentability has been cast into doubt by recent court decisions, including *Alice Corp. Pty. Ltd. v. CLS Bank Int'l*, 134 S. Ct. 2347 (2014). These patents involve a new process or method of data processing. For example, Amazon's 1-Click Shopping is a business method patent. This process allows customers to purchase an item with "one click," and without having to enter payment or delivery information.[241] (See Figure 4-7)

Example of 1-Click Checkout

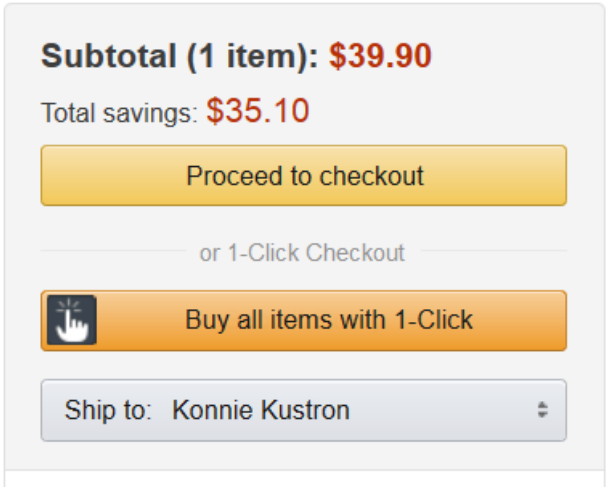


Figure 4-7 Used with permission

Not everything is patentable.

1. An inventor cannot obtain a patent for any law of nature, physical phenomena, or abstract idea. Laws of nature or specific methods or devices employing a law of nature are patentable, though.
2. An abstract idea must be **reduced to practice**[242] as an invention and satisfy the other requirements for patentability before a patent can be obtained.
3. Although literary, dramatic, musical, and artistic works cannot be patented, they may be copyrighted.
4. An invention can also be denied a patent for being offensive to the public morality.

Additionally, the **Atomic Energy Act of 1954**[243] prohibits the patenting of any invention used solely for special nuclear material or atomic energy for atomic weapons.

4.13 USPTO

Federal statutes have established the U.S. Patent and Trademark Office (PTO) as the federal agency to administer the law relating to the granting of patents.[244] The United States Patent and Trademark Office is an agency of the U.S. Department of Commerce.

The USPTO is responsible for examining patent applications and determining whether the applicants are entitled to a patent. The USPTO maintains records of all patents and supports a search room accessible to the public, which contains all documentation for issued patents. Patents can also be searched electronically through the USPTO database.[245]

The USPTO also advises agencies of the government in matters involving intellectual property.

Because the idea of a monopoly is contrary to the free market system, the government makes it easy for an inventor to lose his or her right to a patent if certain rugged criteria are not met. This is to prevent an inventor from effectively extending the period of his or her patent.

How Long Does a Patent Last?[246]
"For applications filed on or after June 8, 1995, utility and plant patents are granted for a term which begins with the date of the grant and usually ends 20 years from the date you first applied for the patent subject to the payment of appropriate maintenance fees for a utility patent. There are no maintenance fees for plant patents. Design patents last 14 years from the date you are granted the patent. No maintenance fees are required for design patents. Note: "Patents in force on June 8, 1995 and patents issued thereafter on applications filed prior to June 8, 1995 automatically have a term that is the greater of the twenty year term discussed above or seventeen years from the patent grant."[247]

Figure 4-8

4.14 Patentability

Four main sections of Title 35 of the U.S. Code govern patentability. These include Title 35 U.S.C. § 101, § 102, § 103, and § 112.[248] Section 101 addresses **usefulness**, 102 reviews **novelty**, 103 discusses **nonobviousness**, and 112 governs the disclosure requirements for patentability. We will look at each one of these individually, but first you should understand the legal concept called **prior art.** Patentability requires that any invention-to-be-patented be "new." Under the American Invents Act, if an invention was in the public use, for sale, or otherwise available to the U.S. public or in a foreign country, it is classified as prior art and not patentable by the person claiming the invention. This does not include disclosures by the inventor within one year of filing.[249]

4.14.1. Usefulness

According to 35 U.S.C. § 101, an invention must be useful. This means the patent must have utility, be useful, and actually work. The inventor may also have a working prototype (reducing the invention to practice) to support application for a patent.[250]

If a machine or other invention does not perform its intended function, then it is not considered useful and cannot be patented.

4.14.2 Novelty

Section 102 states that a patent claim must be new or novel.

An invention, as recited by the patent claim, is not new or novel if the claimed invention was known or used by others in the US or abroad, or patented or described in a printed publication in the U.S. or abroad prior to filing the patent application.[251] So, if the claimed invention has been in public use by another or on sale in the U.S. or in another country, or if the claimed invention was described in a printed publication anywhere in the world prior to the date of filing, then the patent claim cannot be obtained.

4.14.3 Obviousness

Section 103 deals with obviousness.[252] This means that the invention must not be obvious to a person with ordinary skill in the invention's field at the time of filing. Accordingly, even if a patent claim is novel under section 102, the patent claim might still be obvious under section 103, and therefore unpatentable.

This criterion is subjective and is generally the most troublesome for an inventor to overcome. For example, a change in size or material may not make an invention patentable. The general standard is to ask whether the new invention would have been obvious to a person having ordinary skill in the art in view of the previously known subject matter.[243] Rationales supporting a finding of obviousness may include:

(A) Combining prior art elements according to known methods to yield predictable results;

(B) Simple substitution of one known element for another to obtain predictable results;

(C) Use of known technique to improve similar devices (methods, or products) in the same way;

(D) Applying a known technique to a known device (method, or product) ready for improvement to yield predictable results;

(E) "Obvious to try" – choosing from a finite number of identified, predictable solutions, with a reasonable expectation of success;

(F) Known work in one field of endeavor may prompt variations of it for use in either the same field or a different one based on design incentives or other market forces if the variations are predictable to one of ordinary skill in the art;

(G) Some teaching, suggestion, or motivation in the prior art that would have led one of ordinary skill to modify the prior art reference or to combine prior art reference teachings to arrive at the claimed invention.[254]

A common example used to explain obviousness is the creation of a three-legged stool. Assume Company XYZ designs a four-legged stool and receives a patent. In their patent, they claim a stool made of wood having at least four legs underneath a wooden base with equal sides used for the seat. Company ABC invents a three-legged stool with a similar wooden base. Is ABC's three-legged obvious in view of Company XYZ's patent that claims *at least* four legs? The answer is yes, if the artisan having ordinary skill in the art of stool making would find that omission of a leg from the four-legged stood would have been an obvious modification.

What if ABC changes the seat design to a triangle? Alternatively, what about adding a brace to connect the three legs? Alternatively, what if it changes the stool and uses metal instead of wood? Are these obvious changes?

4.14.4 Other Requirements

Various additional formalities must be satisfied in order for a patent claim to be eligible for grant.[255] These include the written description requirement, the enablement requirement, and the best mode requirement.[256] The written description requirement ensures that the specification supporting a patent claim would inform the artisan of ordinary skill that the inventor was in possession of the claimed invention; the enablement requirement ensures that the specification supporting a patent claim would enable the artisan of ordinary skill to make or use the claimed invention; and the best mode requirement ensures that the specification discloses to the artisan of ordinary skill the preferred mode for practicing the claimed invention.

Additional requirements, such as the form of language used in a patent claim, must also be satisfied.[247]

4.15 Types of Patents

In addition to the three conditions of patentability, there are three types of patents an inventor can receive from the USPTO. These type categories include **utility**, **plant**, and **design** patents.[258]

Utility patents are granted to inventions that represent a new and useful process, machine, article of manufacture, or composition of matter, as discussed above. Utility patents may also be granted for *improvements* to a process, machine, article of manufacture, or composition of matter. For example, an inventor may be able to obtain a utility patent on a shoe based on a new and useful shoe structure that supports the arch of the foot correctly. Utility patents may also be obtained on man-made (genetically altered) animals and plants, such genetically altered seeds.

Plant patents can be granted to any person who has invented or discovered and reproduced any asexually reproducing new variety of plant. Asexually reproducing plants are those that reproduce by means other than seeds such as by layering, budding, grafting, and rooting cuttings.

When a patent is granted for an ornamental design of an article of manufacture, the patent rights only extend to the design and appearance of the article. The patent rights do not extend to any structural or functional features. Referring to the shoe example, the inventor might also be able to obtain a design patent based on the appearance of the shoe. This might be desirable if the shoe has a unique and pleasing appearance or if the inventor anticipates commercial success. However, the protection of the design patent would only extend to the appearance of the shoe and it would not protect the functional structure that provides better support.

4.16 Application Process

Patents are awarded through a complex review process that begins with the filing of an application. Prior to filing an application, it is highly recommended that the inventor (or his attorney or agent) complete a full-text and image search of the invention, to verify that the invention has not already been patented. The applicant must also determine whether to file a design, plant, or utility patent application, as there are varying informational requirements depending on the type of patent application.

The application must be sufficiently detailed, as would be understood by the person of *ordinary skill in the art*. Ordinary skill in the art means experience in the area of the patent application being filed. Applications also include a **claims** section. A claim defines "the property rights provided by a patent."[259] If a utility patent application is being filed (which is the most common), the applicant must determine whether to file a provisional or non-provisional application. A provisional application allows an inventor to priority of filing, and is most often employed to delay the formal filing requirements for purposes of cost or to determine whether a patented invention would be commercially viable.[260] However, to receive a full patent, the applicant must file a complete and detailed non-provisional patent application within 12 months from the date of the provisional application filing.[261]

When a non-provisional application is filed, a patent examiner reviews the application. If the application is approved, the inventor will pay an issue fee. The patent will be issued, and published in the *Official Gazette*.

If the examiner does not approve the application, the applicant is notified of the deficiencies. The applicant can then request additional review (reconsideration), or appeal as necessary. Once the examiner's objections are overcome, the USPTO will send the inventor a Notice of Allowance. At this point, the issue fees will become due, and once paid the patent will issue. Figure 4-9 from the USPTO provides a graphic detail of the application process.

Graphical View of the Application Process[262]

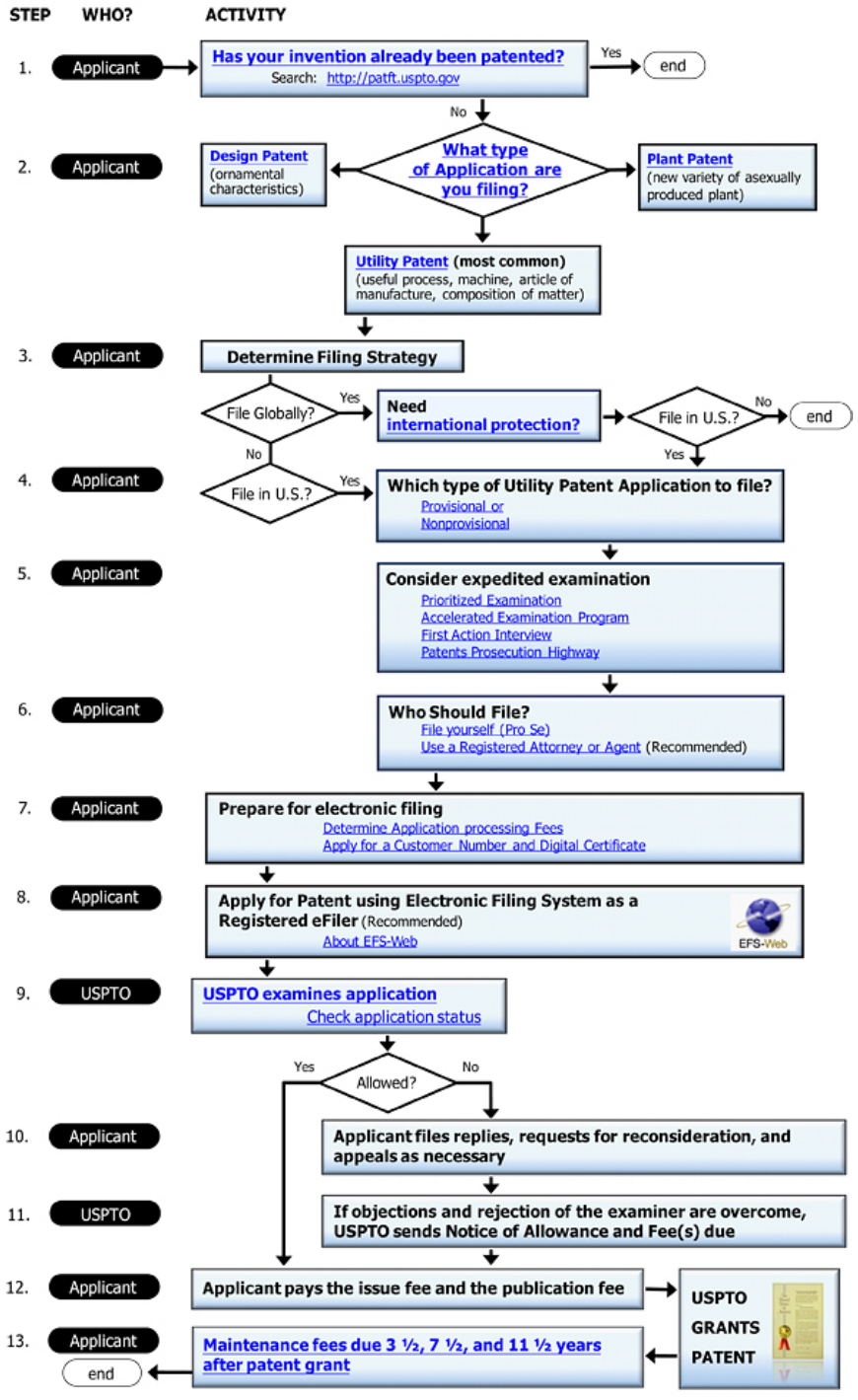


Figure 4-9

4.17 Infringement

The notes below from the USPTO define patent infringement and the legal rules for infringement.

Overview of Patent Infringement[263]

About Patent Infringement?

What is patent infringement?

Patent infringement is the act of making, using, selling, or offering to sell a patented invention, or importing into the United States a product covered by a claim of a patent without the permission of the patent owner. Further, you may be considered to infringe a patent if you import items into the United States that are made by a patented method, unless the item is materially changed by subsequent processes or becomes a trivial and nonessential component of another product. A person "infringes" a patent by practicing each element of a patent claim with respect to one of these acts. Further, actively encouraging others to infringe patents, or supplying or importing components of a patented invention, and related acts can also give rise to liability in certain cases.

What will happen if someone sues me for patent infringement?

A patent owner can sue you in federal court for patent infringement. If the patent owner is able to prove infringement, the court may order you to pay monetary damages and/or stop infringing one or more patent claims. A court can also find that (1) you do not need a license to the patent because you don't practice the invention, (2) one or more of the patent claims are not valid, or (3) there are other reasons why the patent owner is not entitled to prevail against you.

The court may conclude that the patent claim is not valid if it is shown that the claimed invention was disclosed in a prior patent or patents, a book, a magazine, a newspaper, a television show or movie, a webpage or other published work before the date of the claimed invention. Also the court may conclude that the patent claim is not valid if it is shown that the claimed invention was offered for sale in this country or was disclosed to the public more than one year before the application for the patent was filed. In addition, the court could find the patent invalid because it does not meet other statutory requirements, such as a sufficient written description of the invention, or because it does not describe subject matter that is patent eligible.

Further, in "exceptional" cases, the costs of your attorney's fees may be awarded to you if you win the patent case. But if you lose the patent case, you may be held responsible for the attorney's fees of the patent owner. A court may take all of the facts and circumstances of the case into consideration in deciding whether it will find that one party must pay the attorney's fees of the other party. The courts may only award attorney's fees in cases that are out of the ordinary, for example, where the positions of the patent owner are unusually unreasonable.

Figure 4-10

4.18 International Considerations

As mentioned, a patent granted by the U.S. government only protects the invention within the United States and its territories and possessions. For many inventions, it may be financially beneficial to obtain patents in other countries to protect the invention.

To receive protection from other countries, the applicant must file for a patent in **each** country where protections are desired, which may be expensive. However, various international groups facilitate filing around the world. For example, there is a conglomerate in Russia, another in Africa, and one in Asia that assists inventors patent with member countries of their group. There is also a unified office in Europe called the **European Patent Office** (EPO).[264] When an applicant files a patent application with the EPO, the EPO can grant a patent in several European countries. However, the inventor must go through a "validation" process in each of those countries and pay a separate fee to each. The European Patent Office makes it easier, but not necessarily cheaper, to obtain a patent in the countries contracting with the EPO.

In an effort to integrate the patent systems of various countries, the **Patent Cooperation Treaty** (PCT)[265] was formed. The PCT process provides more time for applicants to file in foreign countries. The process involves an International Patent Application, filed with the USPTO, the European Patent Office, or another receiving office. With the application, the applicant states the countries for which protection is being sought, and requests that the receiving office perform a patent search. The applicant then has a certain time in which to file patent applications in the respective countries by entering into the national stage. The World Intellectual Property Organization (WIPO) manages the PCT process.[266]

4.19 Summary

This unit reviewed two types of intellectual property: trade secrets and patents. Trade secrets consist of confidential information that has value to a business. To be classified as a trade secret, the information must truly be secret and have financial value to the company. An organization must use its best efforts to keep the information confidential. To promote the ease of interstate commerce, the Uniform Trade Secrets Act has been adopted by most states.

Patents give the owner the right to exclude others from making, selling, or using the claimed invention. Four types of inventions can be patented: process, machine, manufacture, and composition of matter. Laws of nature, abstract ideas, or physical phenomena cannot be patented. Inventions must be useful, novel, and nonobvious. Three types of patents are awarded by the USPTO: design, plant, and utility.

As of enactment of the AIA, the U.S. is a first inventor to file country.

4.20 Key Terms

America Invents Act	Machine	Prior art search
Atomic Energy Act of 1954	Manufacture	Process
Common law	Model law	Property right
Composition of matter	National Stolen Property Act	Reduced to practice
Design patent	Non-obviousness	Restatement of Torts
Economic Espionage Act of 1966	Novelty	Third party
European Patent Office	Patent	Trade secret
First to file	Patent Cooperation Treaty	Uniform Trade Secrets Act
First to invent	Patentee	Usefulness
Intentional tort of misappropriation	Plant patent	Utility patent

4.21 Chapter Discussion Questions

1. What is a trade secret? How is it different from a copyright, trademark, and a patent?
2. How long does a trade secret last?
3. What is the USTA? What is the purpose of the law?
4. What efforts must a company take to keep their trade secret confidential?
5. What is misappropriation?
6. What is the difference between a first to invent country and a first inventor to file country?
7. Describe the patent application process.
8. What is the difference between a utility, design, and a plant patent? Please provide an example for each.
9. What items cannot be patented?
10. What is the value of securing a patent in countries besides the U.S.?

4.22 Additional Learning Opportunities

Instructional videos on the America Invents Act are available at the USPTO at http://www.uspto.gov/aia_implementation/informational_videos.jsp.

A glossary of terms relating to patents and trademarks is available at the USPTO at http://www.uspto.gov/main/glossary/index.html.

In addition to searching for patents at the USPTO, Google Patents https://www.google.com/?tbm=pts has a search feature for patents and applications that allows searching by country, type of patent, timeframe, *etc*.

Visit http://www.uspto.gov/inventors/index.jsp at the USPTO for inventor resources including a Q & A section.

4.23 Test Your Learning

1. The most common type of patent filed in the U.S. is a(n) _____ patent.
   A. design
   B. foreign
   C. plant
   D. process
   E. utility

2. Under patent law, an inventor with a patent can stop another from _____ a claimed invention.
   A. making
   B. using
   C. making or using
   D. using or selling
   E. making, using or selling

3. James wants to place a clock/timer/alarm on the top of an athletic shoe. This would be an example of what type of patent?
   A. design
   B. foreign
   C. plant
   D. process
   E. utility

4. The right to a patent comes from the
   A. Agreement on Trade Related Aspects of Intellectual Property
   B. American Inventor's Protection Act of 1999
   C. U.S. Constitution
   D. U.S. Patent and Trademark Act

E. Patent Cooperation Treaty

5. Tomas invented a television and received a patent for it two years ago. Tina has now reduced the size of the screen by 1/8 inch. Is this new invention patentable?
   A. Yes, because it is a change to an existing patent.
   B. Yes, because the change is novel.
   C. No, because the change would have been obvious to the artisan of ordinary skill at the time of Tina's reduction.
   D. No, because too much time has passed from the filing of the original application.

6. A trade secret is created by filing
   A. an application with the U.S. Copyright Office.
   B. an application with the U.S. Patent and Trademark Office.
   C. an application with your state's secretary of state office.
   D. an application with your state's corporation office.

E. none of the above.

7. What is the most important element to prove information is a trade secret?
   A. Evidence of the steps taken to keep the information secret.
   B. The number of people who have access to the information.
   C. That the information has value to the owner.
   D. How long the information has been considered a trade secret.
   E. A and B
   F. A, B, and C
   G. All of the above

8. Misappropriation of a trade secret is defined as
   A. Acquisition of a secret of another.
   B. Acquisition of a secret of another by someone who knows it was acquired by improper means.
   C. Disclosure of the trade secret without the express consent of the owner.
   D. Disclosure of the trade secret without the express or implied consent of the owner.
   E. A or C
   F. B or D
   G. A or D
   H. B or C

9. Information that is properly protected as a trade secret
   A. may maintain that status forever
   B. must have a definite duration
   C. must be protected through a trade secret agreement
   D. must be complex
   E. must be recorded with the corporations bureau of your state

10. Einok Inc. invented a software function where text in a document can be highlighted, copied, and pasted into another document. Is this a trade secret?
    A. Yes, since it is a process that is not public.
    B. Yes, because the process can be "undone" by reverse engineering.
    C. No, because the process is already public.
    D. No, because the process can be discovered by reverse engineering.

Test Your Learning answers are located in the Appendix.

5 Free Speech, Defamation & Obscenity

Objectives

After completing this chapter, the student should be able to:

- Understand the limitations of free speech on the Internet;
- Describe the definitions of obscenity as defined by the *Roth* and *Miller* cases;
- Define and apply the elements of defamation; and
- Distinguish between the torts of slander, libel, and libel per se.

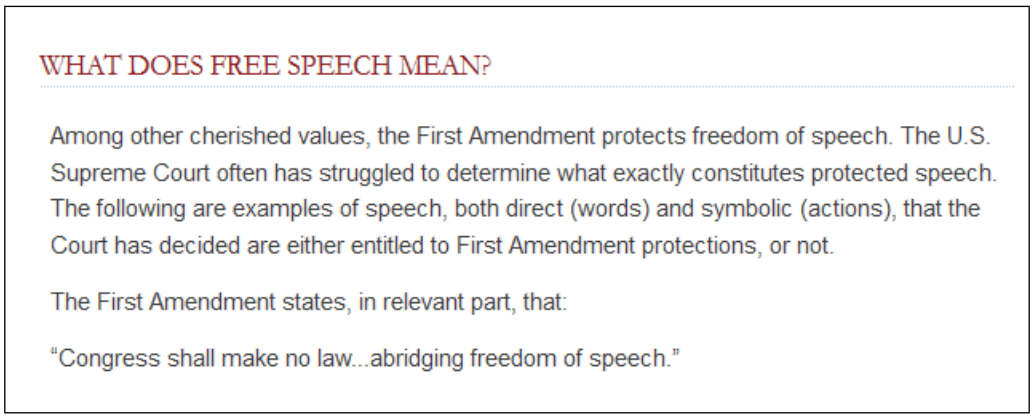
5.1 Introduction

This chapter discusses "**free speech**" on the Internet. Because the Internet is used so often as a communication tool, free speech is a common theme in legal challenges involving the Internet.

The ability for U.S. citizens to share information on the Internet is based on the First Amendment of the U.S. Constitution, which states:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

This right is not absolute. People cannot always speak or write what they think and there are many situations in which free speech does not apply. For example, Justice Holmes, writing for the U.S. Supreme Court in *Schenck v. United States,* 249 U.S. 47 (1919)[267] stated that free speech did not apply to someone falsely shouting fire in a crowded theater. He indicated that this type of speech had no value, other than causing confusion and panic. Later cases have supported this proposition and stated that speech is not protected when such speech may "incite imminent lawless action."[268]


WHAT DOES FREE SPEECH MEAN?

Among other cherished values, the First Amendment protects freedom of speech. The U.S. Supreme Court often has struggled to determine what exactly constitutes protected speech. The following are examples of speech, both direct (words) and symbolic (actions), that the Court has decided are either entitled to First Amendment protections, or not.

The First Amendment states, in relevant part, that:

"Congress shall make no law...abridging freedom of speech."

Figure 5-1[269]

Similarly, obscene speech does enjoy unfettered protection under the law. For example, the emailing of obscene material is not protected under the First Amendment.[270] Along similar lines and as will be discussed later, speech that is **defamatory** *is also unprotected.*[271]

5.2 Obscenity

Obscenity is a type of unprotected speech. Obscenity includes not only words, but also photographs and pictures. There is a long history of federal cases that have reviewed the question of speech in relation to obscenity. The results of such decisions have molded the criteria for determining whether material is classified as obscene or protected as free speech under the U.S. Constitution.

5.3 *Roth v. United States*[272]

The first key case that looked at the obscenity question was decided in 1957 by the U.S. Supreme Court in *Roth v. United States*. The case consisted of two criminal defendants by the name of Roth and Alberts.

Roth conducted a business in New York in the publication and sale of books, photographs, and magazines. He used circulars and advertising matter to solicit sales."[273] He was convicted violating a federal obscenity law that prohibited the mailing of "obscene, lewd, or lascivious book, pamphlet, picture, or other publication of an indecent character…"[274]

Roth's case was combined with the *Alberts v. California* case. Defendant Alberts also conducted a mail-order business, but he was based in Los Angeles, California. Alberts was charged with a misdemeanor complaint "with lewdly keeping for sale obscene and indecent books, and with writing, composing, and publishing an obscene advertisement of them, in violation of the California Penal Code."[275]

The *Court* in Roth reviewed two questions: 1) if the federal and California state laws that prohibited the sale or transfer of obscene materials through the mail were constitutional, and 2) whether the restrictions of these laws violated the federal constitutional right to free speech.

In its decision, the Court held that obscenity was not "within the area of constitutionally protected speech or press."[276] The Court also used *Roth* to establish the criteria to determine obscenity. The test is to ask the question "whether to the average person, applying contemporary community standards, the dominant theme of the material taken as a whole appeals to prurient interest."[277]

In other words, the rule in Roth was that the First Amendment does not protect obscenity because it is utterly without social value and it is not within the area of constitutionally protected speech or press. However, this rule creates other questions: some materials may have social value to one person, but may be offensive to another.

5.4 *Miller v. California*[278]

In 1973, the U.S. Supreme Court again reviewed the questions of free speech and obscenity, and revised the law through the *Miller v. California* case.

In Miller, the defendant mailed unsolicited and unrequested obscene materials to a restaurant owner and his mother, resulting in the defendant's conviction under a state law. The U.S. Supreme Court reversed Miller's conviction and sent the case back to the trial court for retrial. The Court suggested the trial court use a *refined* three-prong test to determine whether the materials were obscene and without First Amendment protection. The new standard included asking two additional questions:

1. whether "the average person, applying contemporary community standards" would find that the work, taken as a whole, appeals to the prurient interest,"[279]
2. whether the work depicts or describes, in a patently offensive way, sexual conduct specifically defined by the applicable state law, and
3. whether the work, taken as a whole, lacks serious literary, artistic, political, or scientific value. If a state obscenity law is thus limited, First Amendment values are adequately protected by ultimate independent appellate review of constitutional claims when necessary.[280]

Note the first two questions are based on the community. In contrast, the third question "whether a work has serious literary, artistic, political, or scientific value," is to be judged by a national standard. A national standard is difficult to apply to the Internet, as the community standard crosses borders.

Below is the case of *FCC v. Pacifica Foundation* decided five years after *Miller* and involving the late comic George Carlin's use of the "seven filthy words."[281] To this day, these seven words cannot be spoken on television or on the radio. As you read this case, think of its application to the Internet, and whether it would be realistic to apply the *Pacific Foundation* rules to online speech.

The Court Speaks

FCC v. Pacifica Foundation, 438 U.S. 726 (1978)[282]

(ADVISORY: The *Pacifica* case contains Carlin's entire monologue, *uncensored*. The text of the case may be offensive to certain readers.)[283]

Facts:

A radio station belonging to Pacifica Foundation made an afternoon broadcast of a satiric monologue, entitled "Filthy Words," which listed and repeated a variety of colloquial uses of "words you couldn't say on the public airwaves." A father who heard the broadcast while driving with his young son complained to the Federal Communications Commission (FCC). While not imposing formal sanctions, the FCC issued an order "associated with the station's license file, and in the event subsequent complaints are received, the Commission will then decide whether it should utilize any of the available sanctions it has been granted by Congress." The FCC characterized the language of the monologue as "patently offensive," though not necessarily obscene, and expressed the opinion that it should be regulated by principles analogous to the law of nuisance where the "law generally speaks to channeling behavior rather than actually prohibiting it." The FCC found that certain words in the monologue depicted sexual and excretory activities in a particularly offensive manner, noted that they were broadcast in the early afternoon "when children are undoubtedly in the audience," and concluded that the language as broadcast was indecent and prohibited. The U.S. Supreme Court agreed with the FTC. (p. 726–727)

Pacifica argued that the broadcast was not indecent within the meaning of the statute because of the absence of prurient appeal and the judgment was reversed.

Discussion:

The only other statutory question presented by this case is whether the afternoon broadcast of the "Filthy Words" monologue was indecent within the meaning of § 1464. Even that question is narrowly confined by the arguments of the parties. (p. 738–739)

The Commission identified several words that referred to excretory or sexual activities or organs, stated that the repetitive, deliberate use of those words in an afternoon broadcast when children are in the audience was patently offensive, and held that the broadcast was indecent. Pacifica takes issue with the Commission's definition of indecency, but does not dispute the Commission's preliminary determination that each of the components of its definition was present. Specifically, Pacifica does not quarrel with the conclusion that this afternoon broadcast was patently offensive. Pacifica's claim that the broadcast was not indecent within the meaning of the statute rests entirely on the absence of prurient appeal. (p. 739)

The plain language of the statute does not support Pacifica's argument. The words "obscene, indecent, or profane" are written in the disjunctive, implying that each has a separate meaning. Prurient appeal is an element of the obscene, but the normal definition of "indecent" merely refers to nonconformance with accepted standards of morality… (p. 740)

…It is true that the Commission's order may lead some broadcasters to censor themselves. At most, however, the Commission's definition of indecency will deter only the broadcasting of patently offensive references to excretory and sexual organs and activities. While some of these references may be protected, they surely lie at the periphery of First Amendment concern. (p. 744)

Questions:

1. Does this case apply to the Internet? Why or why not? If not, should it apply?
2. If this case were decided today, would the court's ruling be the same?
3. How do television and radio differ as entertainment and communication tools from the Internet?

5.5 Communications Decency Act of 1996[284]

As access to the Internet expanded in the mid 1990's, Congress determined it was necessary to pass legislation to deal with the growing availability of pornography and obscenity to children. The **Communication Decency Act** (CDA) of 1996, 47 U.S.C. §§ 223 and 230, was the first law designed to protect minors from pornography on the Internet. Section 223 of the law made it a crime to transmit materials over the Internet to those known to be under the age of 18 that were "obscene or indecent."[285] After passage, the law was immediately challenged as censorship (see *Reno v. ACLU 1* below). The key challenge to the law was its definition of the word "indecent."

Another noteworthy element of the law was Section 230[286] that distinguished an "access provider" from a "content provider." This was significant because the law stated that Internet operators were not publishers and therefore, not liable for posts made by third parties. What exactly does this mean? Assume two parties A and B are involved in a sexual relationship and break off the relationship. Person A in the relationship is angry with the other, and posts embarrassing sexual photographs of Party B online. Under Section 230 of the CDA, the Internet service provider (ISP) would not be responsible for financial damages caused by Party A's posting of the pornographic images.

5.6 *Reno v. ACLU 1*[287]

As noted above, the American Civil Liberties Association (ACLU) filed suit against the U.S. Attorney General, Janet Reno, challenging the constitutionality and enforcement of Section 223.

In 1997, the Supreme Court in a 9-0 decision determined that the "CDA restrictions violated the First Amendment" because the terms "indecent and" patently offensive" were too broad.[288] In other words the Court held "the CDA's "indecent transmission" and "patently offensive display" provisions abridge "the freedom of speech" protected by the First Amendment."[289] It stated that it agreed with the District Court that the "CDA places an unacceptably heavy burden on protected speech… (and that it) cast(s) a far darker shadow over free speech, (and) threatens to torch a large segment of the Internet community."[290]

Free Speech Includes the Following Free Speech Rights[291]

Freedom of speech includes the right:

- **Not to speak (specifically, the right not to salute the flag).**
  West Virginia Board of Education v. Barnette, 319 U.S. 624 (1943).
- **Of students to wear black armbands to school to protest a war ("Students do not shed their constitutional rights at the schoolhouse gate.").**
  Tinker v. Des Moines, 393 U.S. 503 (1969).
- **To use certain offensive words and phrases to convey political messages.**
  Cohen v. California, 403 U.S. 15 (1971).
- **To contribute money (under certain circumstances) to political campaigns.**
  Buckley v. Valeo, 424 U.S. 1 (1976).
- **To advertise commercial products and professional services (with some restrictions).**
  Virginia Board of Pharmacy v. Virginia Consumer Council, 425 U.S. 748 (1976); *Bates v. State Bar of Arizona*, 433 U.S. 350 (1977).
- **To engage in symbolic speech, (e.g., burning the flag in protest).**
  Texas v. Johnson, 491 U.S. 397 (1989); *United States v. Eichman*, 496 U.S. 310 (1990).

Freedom of speech does not include the right:

- **To incite actions that would harm others (e.g., "[S]hout[ing] 'fire' in a crowded theater.").**
  Schenck v. United States, 249 U.S. 47 (1919).
- **To make or distribute obscene materials.**
  Roth v. United States, 354 U.S. 476 (1957).
- **To burn draft cards as an anti-war protest.**
  United States v. O'Brien, 391 U.S. 367 (1968).
- **To permit students to print articles in a school newspaper over the objections of the school administration.**
  Hazelwood School District v. Kuhlmeier, 484 U.S. 260 (1988).
- **Of students to make an obscene speech at a school-sponsored event.**
  Bethel School District #43 v. Fraser, 478 U.S. 675 (1986).
- **Of students to advocate illegal drug use at a school-sponsored event.**
  Morse v. Frederick, __ U.S. __ (2007).

Figure 5-2

5.7 Child Pornography Prevention Act of 1996[292]

Passed the same year as the CDA, the **Child Pornography Prevention Act of 1996** (CPPA) prohibited and criminalized the use of computers to knowingly produce child pornography. Two sections of the law characterized child pornography as illegal speech.[293] The first section prohibited "any visual depiction, including any photograph, film, video, picture, or computer or computer generated image or picture" that "is, or appears to be, or a minor engaging in sexually explicit conduct."[294] Another key section prohibited "any sexually explicit image that was advertised, promoted, presented, described, or distributed in such a manner than conveys the impression it depicts a minor engaging in sexually explicit conduct."[295]

Litigation was also filed challenging the constitutionality of this law. In *Ashcroft v. Free Speech Coalition,* 535 U.S. 234 (2002),[296] the U.S. Supreme Court struck down the aforementioned two provisions of the law because they were overbroad and they abridged "the freedom to engage in a substantial amount of lawful speech."[297] The Court viewed the CPPA definition of child pornography as too vague and too broad under the First Amendment, because the CPPA applied to both depictions of real and fictitious children.[298]

5.8 Child Online Protection Act of 1998[299]

The Child Online Protection Act (COPA) was passed in reaction to the striking down of Section 223 of the Communications Decency Act by the U.S. Supreme Court. COPA made it a crime to publish "any communication for commercial purposes that included sexual material that was harmful to minors, without restricting access to such material by minors." "Harmful to minors" in the Act was defined as lacking "any scientific, literary, artistic, or political value" and offensive to "community standards."[300]

Why Was COPA Held Unconstitutional?
1. The case challenged Congress's power to regulate interstate commerce while limiting the First Amendment free speech rights of adults. In addition, the statute was vague (for example, what are materials harmful to children) and overbroad, because adults were denied access to these materials. 2. Children could access pornographic materials on foreign and non-commercial websites since COPA only applied to commercial U.S. websites, and there were other resources besides the web to access these materials.

Figure 5-3

The Act never took effect and after several court appeals, the law was ruled unconstitutional.[291]

5.9 The Children's Internet Protection Act of 2000[302]

The Children's Internet Protection Act of 2000 (CIPA) was a Congressional attempt to regulate computer access to adult-oriented Web sites in public schools and libraries. This law denied federal funds to libraries who refused to place filters on the Internet accessible computers.[303] It also required libraries to block visual depictions of obscenity, child pornography, or "materials harmful to minors." (Note: this law defined minors as children under age 17, and not 18).[304] The law also required libraries to disable filtering software on the request of an adult. In early 2001, the Federal Trade Commission (FTC) issued rules implementing CIPA, and updated the rules most recently in 2011.[305]

Additionally, the FCC requires schools and libraries subject to CIPA to adopt and implement an Internet safety policy addressing these factors:

a) access by minors to inappropriate matter on the Internet;
b) the safety and security of minors when using electronic mail, chat rooms and other forms of direct electronic communications;
c) unauthorized access, including so-called "hacking," and other unlawful activities by minors online;
d) unauthorized disclosure, use, and dissemination of personal information regarding minors; and
e) measures restricting minors' access to materials harmful to them.[306]

5.10 Child Protection and Obscenity Enforcement Act of 1988[307]

This 1988 law (18 U.S.C. § 2251), required producers of actual, sexually explicit materials (magazines and videos) to maintain onsite records to verify that all models, or actors are of legal age.[308] The main purpose of the law was to prevent minors from being involved in producing pornography. Late in 2005, the law was extended to websites, but NOT ISP's.[309] In 2007, the Sixth Circuit Court of Appeals in Cincinnati ruled that the federal anti-child pornography law, the Child Protection and Obscenity Enforcement Act, violated the First Amendment.[310]

The Court felt that the record keeping requirements of the law were invalid because they "imposed an overbroad burden on legitimate, constitutionally protected speech."[311] However, the U.S. Department of Justice requested a review of the case by the entire Sixth Circuit (called an **en banc hearing**), which issued an opinion in 2009 upholding the constitutionality of the record-keeping requirements. The United States Supreme Court refused review of the case.[312]

5.11 Defamation

Another aspect of free speech involves the tort of **defamation.** Defamation involves the publication (sharing) of false statements that harm another's reputation. These statements can be written or spoken. Written defamation is **libel**. Spoken defamation is **slander**. Lawsuits on the Internet are based on libel.

Defamation is a state action. Most states have defamation statutes used as the basis for a defamation lawsuit.

Sample Libel and Slander State Statute[313]
Ohio Revised Code Chapter 2739: SLANDER; LIBEL **2739.01 Libel and slander.** In an action for a libel or slander, it is sufficient to state, generally, that the defamatory matter was published or spoken of the plaintiff. If the allegation is denied, the plaintiff must prove the facts, showing that the defamatory matter was published or spoken of him. In such action it is not necessary to set out an obscene word, but it is sufficient to state its import. Effective Date: 10-01-1953 **2739.02 Defenses in actions for libel or slander.** In an action for libel or a slander, the defendant may allege and prove the truth of the matter charged as defamatory. Proof of the truth thereof shall be a complete defense. In all such actions any mitigating circumstances may be proved to reduce damages. Effective Date: 10-01-1953

Figure 5-4

5.12 Elements

There are four elements involved in common law defamation. First, the statement must harm a person or a business's reputation. The assertion can be made through direct evidence, innuendo, insinuation, or by reference to the person. It must be understood that the statement refers to the person.

Second, the statement must be false, and not simply represent someone's opinion. Third, it must be communicated (called published) to a third party. With Internet libel, the threshold to prove injury is very low due to ease of sharing and the permanent nature of online communications.

Fourth, the person must be injured or damaged by the statement (such as a person being terminated from a job, or a business losing profits). To prove defamation, it must also be shown that there was some degree of fault or negligence on the part of the defendant. If the libel involves a public figure, the plaintiff must demonstrate the defendant acted with actual malice (reckless disregard of the truth).

5.13 Libel Per Se

Libel per se is written statement that society has determined is so outrageous *that a plaintiff does not have to prove injury*. There are four kinds of libel per se: accusing a person of committing a serious crime, saying someone has a sexually transmitted disease, alleging incompetence in a person's profession, or claiming a woman is unchaste. Again, as long as the statement is proven false, a person does not have to prove damages. There are similar rules for slander per se.

5.14 Defenses

An opinion is generally a valid defense in a defamation lawsuit. Opinion is covered by the First Amendment of the U.S. Constitution.[314] It must be clear to a third party that the comment is an opinion.

Other defenses to a libel claim include truth, absolute privilege, and qualified privilege.

1. Truth is an **absolute defense**. This means if Party A sues Party B for libel and the statement made by the Party B is true, Party A will lose the case.
2. **Absolute privilege** applies to statements made by individuals in government positions. Absolute privilege makes a person immune from a lawsuit. Members of the three branches of government enjoy protection from liability for whatever they say so long as the statement relates to their function as a government official.
3. **Qualified privilege** attaches to individuals who possess a common interest in sharing information about another, such as a prospective employer asking a prior employer about a job applicant's past job performance.

Remember under Section 230 of the CDA, an Internet service provider is not responsible as a publisher of any defamatory material published on their Web site unless they exercised a sufficient degree of editorial control over the contents of what was published.

5.14 Free Speech and Social Media

Facebook, Instagram®, YouTube®, Twitter®, and Google+® are just a few of the most popular social networking sites on the Internet. If someone makes a derogatory post about another person on one of these sites, defamation law applies. If the information is false and harms another's reputation, there is potential for a libel lawsuit.

For example, assume that Sam is angry with her partner Charlie and Tweets that Charlie stole $250 from petty cash at work, and that he gave her a sexually transmitted disease. The post is a lie, but Charlie loses his job based on Sam's allegations. Charlie has the option to sue Sam for libel. Anonymous posts or posts using an alias are also subject to defamation laws, which may include the ordering of a monetary award by a court.

5.15 Free Speech and Work

Speech at work is governed by company policy. This means that the employer regulates any electronic or verbal communications. In other words, there is no First Amendment right to free speech in the private workforce. Employees should closely read their company policies as they relate to social media.

Employees not on company time, in general, may legally engage in personal communications on the Internet without intervention from an employer. However, it simply may be imprudent to criticize publically an employer on social media.

Free Speech Standards for Public Employees
Pickering v. Board of Education, 391 U.S. 563 (1968) "used a balancing test to determine whether the First Amendment protects a public employee's speech. These three questions need to be asked: 1. Did the individual demonstrate that his or her speech address a matter or matters of public interest and concern? 2. Did the individual demonstrate that his or her speech was a significant or motivating factor in the employer's decision? 3. Did the court balance the interests of the individual commenting on matters of public concern as a citizen and the public employer's interest in "promoting the efficiency of public service?"

Figure 5-5

What about the standards for public employees? In 2014, the U.S. Supreme Court case of *Lane v. Franks*,[316] reiterated the standards of *Pickering v. Board of Education* requiring balancing "the interests of the [employee], as a citizen, in commenting upon matters of public concern and the interest of the State, as an employer, in promoting the efficiency of the public services it performs through its employees." (p. 2)

5.16 Summary

Free speech is an area of the law that will continue to change with technology. The conflict between obscenity and First Amendment free speech will be ongoing. As changes in the U.S. Supreme Court's view of free speech change, you will see continued expansion and restriction of free speech.

Remember, the Constitution does not protect obscene speech, and pornography is entitled to First Amendment protection unless it is obscene or contains child pornography. Courts have attempted to define obscenity using the three-prong *Miller* test, which uses community standards. Because the Internet does not have borders, however, applying a community standard is very difficult.

Defamation via e-mail, chat rooms, blogs, Facebook posts *etc.*, is likely to be termed libel, because of its permanent nature. Defamation must cause harm, be false, be communicated, and cause injury. Defenses include truth, absolute privilege, and qualified privilege.

The liability issues of service providers for online defamation are covered by Section 230 of the Communications Decency Act of 1996, which protects service providers from liability in defamation.

5.17 Key Terms

Absolute defense	Communications Decency Act of 1966	Libel per se
Absolute privilege	Defamation	*Miller v California*
Child Protection and Obscenity Enforcement Act of 1988	Children's Internet Protection Act of 2000	Obscenity
Child Online Protection Act of 1998	Communications Decency Act of 1996	Prurience
Child Pornography Prevention Act of 1996	Defamation	Qualified privilege
Children's Internet Protection Act of 2000	Free speech	*Reno v ACLU 1*
	Libel	*Roth v United States*
		Serious literary, artistic, political, or scientific value
		Slander

5.18 Chapter Discussion Questions

1. What speech protections does the First Amendment provide?
2. What is the difference between libel and slander?
3. What are the obscenity standards as described by *Miller*?
4. What are the obscenity standards as described by *Roth*?
5. What is the difference between absolute defense, absolute privilege, and qualified privilege?
6. What are the requirements of the Children's Internet Protection Act?
7. What does Section 320 of the Communications Decency Act provide?
8. What did the Court determine in *Reno v. ACLU 1*?
9. Define "serious literary, artistic, political, or scientific value."
10. Give an example of libel per se.

5.19 Additional Learning Opportunities

The Electronic Frontier Foundation https://www.eff.org/issues/free-speech has an excellent website that discusses emerging free speech issues.

5.20 Test Your Knowledge

1. "Publication" in a defamation case means
   A. The defamatory statement must be false.
   B. The defamatory statement must be made known to a third party.
   C. Electronic statements cannot be defamatory.
   D. The defamatory statement must be made in writing.

2. Under the Communications Decency Act of 1996, an online service provider
   A. can be held liable for material posted by another on its service if it takes no action to screen the material.
   B. can be held liable for material posted by another on its service if it acts as a "common carrier."
   C. can be held liable for material posted by another on its service if it voluntarily agrees to monitor that material for truthfulness.
   D. cannot be held liable for material posted by another.

3. Which of the following is the best definition of defamation?
   A. Defamation is a written or oral statement that harms another's reputation.
   B. Defamation is a written false statement that wrongfully harms another's reputation.
   C. Defamation is a written or oral statement wrongfully made directly to the individual defamed.

D. Defamation is a written or oral false statement that wrongfully harms another's reputation.

4. Defenses to defamation include
   A. absolute privilege
   B. incapacity of the speaker
   C. qualified privilege
   D. A and C
   E. A and B
   F. B and C

5. The difference between libel and libel per se is that
   A. In a libel case, the plaintiff must prove damages, whereas in a "libel per se" case damages are assumed.
   B. Libel contains written words, and libel per se consists of spoken words.
   C. Libel must be published, while libel per se need not be published.
   D. In a libel per se case, plaintiff must prove actual malice, whereas in a slander case, proof of actual malice is unnecessary.

6. As a defense to defamation, truth is
   A. always a defense
   B. sometimes a defense depending on the intent of the speaker
   C. a defense only if it can be proved beyond a reasonable doubt
   D. none of the above

7. Obscenity is more than pornography as it must pass the legal test of
   A. prurient interests
   B. sexual arousal
   C. lewd conduct
   D. lustful desires

8. Jamie makes a post on LinkedIn that Taylor is a crooked and unethical attorney. The statement is not true. Taylor's actions are an example of
   A. free speech
   B. slander

C. libel
D. libel per se
E. slander per se

9. Congressman Smith criticizes the President of the United States and refers to him by a vulgar term. The President can sue the Congressman for
   A. libel
   B. libel per se
   C. slander
   D. slander per se
   E. He cannot sue as the Congressman has an absolute privilege.

10. Which of the following is NOT an example of libel per se?
    A. accusing a person of committing a serious crime
    B. saying someone has a sexually transmitted disease
    C. alleging incompetence in a person's profession
    D. alleging a woman is unchaste
    E. none of the above

Test Your Learning answers are located in the Appendix.

6 Cybercrime

Objectives

After completing this chapter, the student should be able to:

- Describe the three types of computer crime;
- Describe and define the types of Internet crime that target individuals and businesses; and
- Explain the key federal laws that target Internet crime against property.

6.1 Overview

This chapter will review privacy and security breaches on the Internet that are of a criminal nature, or called cybercrime. Broadly speaking, cybercrime is defined as any illegal action that *uses* or *targets* computer networks to violate the law.

The U.S. Department of Justice (DOJ)[317] categorizes computer crime in three ways:

1. As a target: a computer is the subject of the crime (such causing computer damage). For example, a computer attacks the computer(s) of others in a malicious way (such as spreading a virus).
2. As a weapon or a tool: a computer is used to help commit the crime. This means that the computer is used to commit "traditional crime" normally occurring in the physical world (such as fraud or illegal gambling).
3. As an accessory or incidental to the crime: a computer is used peripherally (such as for recordkeeping purposes). The DOJ suggests this would be using a computer as a "fancy filing cabinet" to store illegal or stolen information.[318]

6.2 Types of Crimes

Many types of crimes are committed in today's networked environment. They can involve either people, businesses, or property. Perhaps you have been a victim of Internet crime, or chances are you know someone who has been a victim. Crimes against a person or business include auction fraud, credit card fraud, debt elimination, parcel courier email scheme, employment/business opportunities, escrow service fraud, identity theft, Internet extortion, investment fraud, lotteries, Nigerian letter or "419," phishing/spoofing, Ponzi/pyramid, reshipping, spam, third party receiver of funds.[319] Property crimes involve cracking and hacking, drive by download, a logic bomb, malware, password sniffers, piggybacking, pod slurping, and wardriving.

6.3 Crimes Against a Person/Business

Auction fraud involves an online auction in which the goods described are not what the customer receives. Or, auction fraud could involve a buyer who transfers funds to a seller and the seller never receives the product. Online auction sites, such as eBay®, are very sensitive to this type of issue, and eBay has instituted a "money back guarantee" for customers who purchase an item from a fraudulent seller.[320]

Auction fraud from Romania is in its own category because it is often a part of fraudulent selling issues. In Romanian fraud, the seller appears to be from the United States, and creates a scenario that asks the buyer to send the money to a business associate or family member in Europe. The money is sent through Western Union® or a Moneygram®, which can be picked up anywhere in the world.

Credit card fraud is simply the unauthorized and fraudulent use of someone's credit card over the Internet.

Debt elimination involves a situation in which a website advertises elimination of a person's debt. The borrower fills out an application providing all their personal information and is asked by the debt elimination company to send a large deposit such as $3000 or $4000 with the borrower's application. In return, the debtor receives a "loan" document to present to their bank or mortgage company. Unfortunately, the document will be a fake, so the consumer will not only owe their original debt, but they will also have been cheated out of their deposit.

Counterfeit cashier's checks involve a situation in which an individual posts an item for sale on the Internet, and a prospective purchaser outside the U.S. contacts the seller expressing an interest in acquiring the item. The purchaser tells the seller he would like to buy the seller's item. However, the buyer tells the seller that someone owes him money that is more than the purchase price. The seller has his "phantom" borrower send a check to the seller to pay for the product. The amount of the check is more than the cost of the product, so the seller is asked to send the overpayment to the purchaser. Unfortunately, the check the seller receives in counterfeit. Figure 6-1 presents an example of this type of fraud.

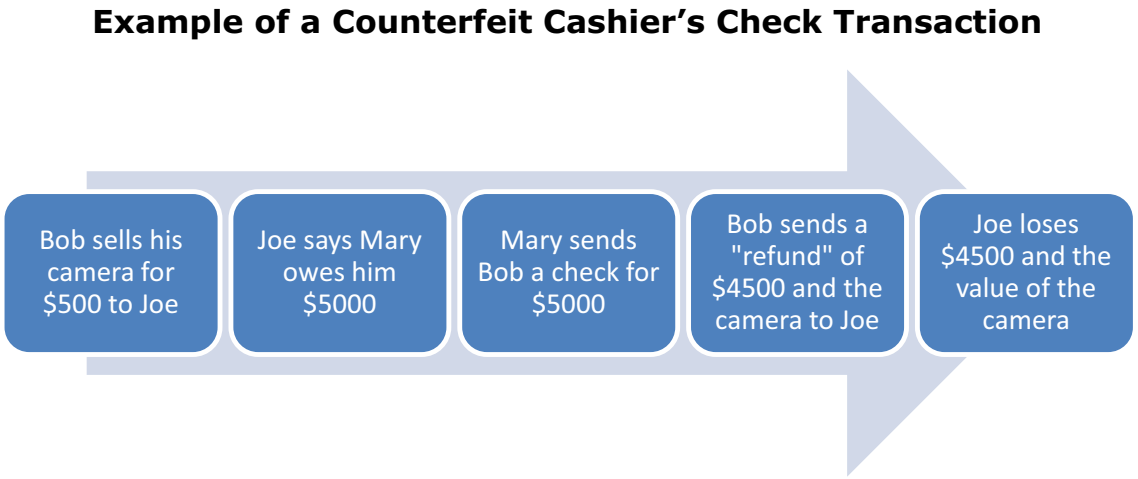


Figure 6-1

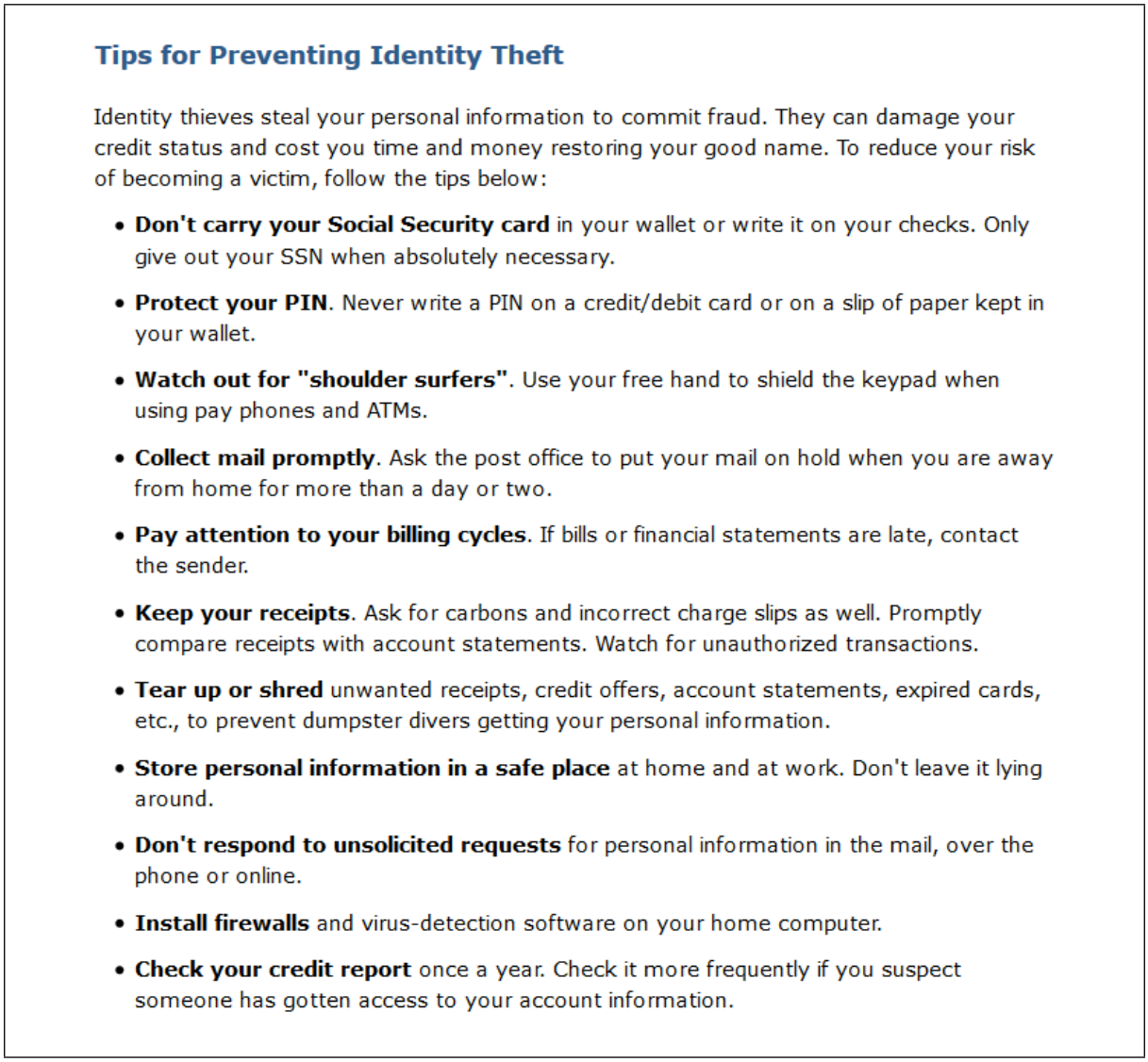
Another way that the counterfeit cashier's check has been used is with the "secret shopper" scam. A person receives a "cashier check" in the mail for roughly $3,000. Enclosed with the check is an official looking letter that says that "you have been selected to be a secret shopper to test the quality of service for Western Union." Also enclosed will be a survey form. The cashier's check will look very legitimate. The letter would include instructions to cash the check at a local bank, take $2800.00 of the $3,000.00 to Western Union, and send the $2800 to an address in California. Those caught by this fraud would be out $2800, instead of receiving the promised $200.

Email spoofing is the forgery of an email header so that a message appears to come from someone other than the true sender (who would be called the **spammer**). The recipient thinks that the email is legitimate and from the true sender. Spoofing is illegal under the CAN-AM SPAM Act[321]. Often times, the email will include a virus or link to a pornographic site when opened.

In **employment/business opportunities fraud,** typically there is an international company supposedly soliciting people for work at home opportunities. Similar to auction fraud, the potential employee is told that the company has U.S. based creditors and one of those will be paying the employee. However, when the person receives their paycheck, it is higher than what was owed and the employee is told to cash the check and then wire the difference back to the international company. The check is fraudulent, and the "employee" is out the entire amount of the check.

Escrow services fraud also involves Internet auctions. In this type of scam, the seller creates a payment look alike service such as PayPal®, which is actually a fake site. The victim sends money to the site to pay for their purchase, bus instead loses their funds.

Identity theft is the fastest growing Internet crime in the United States.[322] This is an instance in which the criminal takes someone's personal information, such as a Social Security number or a person's mother's maiden name, and impersonates that person to make purchases using the stolen credentials. Many times credit card purchases are also charged to the person whose credentials were stolen.



Tips for Preventing Identity Theft

Identity thieves steal your personal information to commit fraud. They can damage your credit status and cost you time and money restoring your good name. To reduce your risk of becoming a victim, follow the tips below:

- **Don't carry your Social Security card** in your wallet or write it on your checks. Only give out your SSN when absolutely necessary.
- **Protect your PIN**. Never write a PIN on a credit/debit card or on a slip of paper kept in your wallet.
- **Watch out for "shoulder surfers"**. Use your free hand to shield the keypad when using pay phones and ATMs.
- **Collect mail promptly**. Ask the post office to put your mail on hold when you are away from home for more than a day or two.
- **Pay attention to your billing cycles**. If bills or financial statements are late, contact the sender.
- **Keep your receipts**. Ask for carbons and incorrect charge slips as well. Promptly compare receipts with account statements. Watch for unauthorized transactions.
- **Tear up or shred** unwanted receipts, credit offers, account statements, expired cards, etc., to prevent dumpster divers getting your personal information.
- **Store personal information in a safe place** at home and at work. Don't leave it lying around.
- **Don't respond to unsolicited requests** for personal information in the mail, over the phone or online.
- **Install firewalls** and virus-detection software on your home computer.
- **Check your credit report** once a year. Check it more frequently if you suspect someone has gotten access to your account information.

Figure 6-2[313]

International lottery type frauds usually begin with an unsolicited email with a message a person has won or has been selected to receive money from an international lottery. The consumer is often asked to provide a variety of personal information to collect the promised funds.

Example of an International Lottery Scam[324]

"Congratulations! You may receive a certified check for up to $400,000,000 U.S. CASH!
One Lump sum! Tax free! Your odds to WIN are 1-6."

"Hundreds of U.S. citizens win every week using our secret system!
You can win as much as you want!"

Figure 6-3

Internet extortion has many twists and turns. The most common is a case in which someone hacks into a company's website or mainframe, and then refuses to give control back to the company unless a payment is made.

Investment fraud is defined as "an offer using false or fraudulent claims to solicit investments or loans, or providing for the purchase, use, or trade of forged or counterfeit securities."[325] The well-known billions of fraud[326] committed by Bernie Madoff[327] would fit in this category.

The **Nigerian letter** is a take-off from the lottery fraud, often called 419's, which is a section of the Nigerian civil code these schemes violate. With this scam, the perpetrator will send an email asking for the reader's help to transfer money to the United States. This is one of the oldest frauds on the net. The FTC provides more details in Figure 6-4 below.

The "Nigerian" Email Scam[328]
The Bait: These messages are the butt of late night jokes, but people still respond to them. The people behind these messages claim to be officials, businesspeople, or the surviving spouses of former government honchos in Nigeria or another country whose money is tied up temporarily. They offer to transfer lots of money into your bank account if you will pay the fees or "taxes" they need to get their money. If you respond to the initial offer, you may receive documents that look "official." They may even encourage you to travel to the country in question, or a neighboring country to complete the transaction. Some fraudsters have produced trunks of dyed or stamped money to try to verify their claims. **The Catch:** The emails are from crooks trying to steal your money or your identity. Inevitably, emergencies come up, requiring more of your money and delaying the "transfer" of funds to your account. In the end, there aren't any profits for you, and your money is gone along with the thief who stole it. According to State Department reports, people who have responded to their emails have been beaten, subjected to threats and extortions, and in some cases, murdered.

Figure 6-4

Online **phishing** (pronounced like the word fishing) is a way to trick computer users into revealing personal or financial information through a fraudulent email message or website. A common online phishing scam starts with an email message that looks like an official notice from a trusted source, such as a bank, credit card company, or reputable online merchant. In the email message, recipients are directed to a fraudulent website at which they are asked to provide personal information, such as an account number or password. This information is then used to steal a person's identity. As an aside, text messaging can also be used for phishing.

In a **Ponzi scheme,** an investment person promises what to most people appears to be an unreasonable rate of return on an investment. This is actually a fraudulent investment and the operator usually pockets the money. Similar to a Ponzi, is a **pyramid scheme**. This is an operation in which the operator takes money from one investor and uses a part of the proceeds to pay dividends to other investors, and keeps the remainder for his or her own use. Pyramid schemes also are perpetrated through email. Figure 6-5 below explains the process behind a pyramid scam.

How Pyramid Schemes Operate[329]

Let's look at how a pyramid scheme operates from three points of view: the potential investor, the promoter or con artist, and the victim Many pyramid schemes will present a payout formula or matrix much like this one:

	# Payment of $500		
Level 1 $150 x 3 = $450	#	#	#
Level 2 $30 x 9 = $270	###	###	###
Level 3 $30 x 27 = $810	#########	#########	#########
Level 4 $30 x 81 = $2430	etc. #########	#########	########etc.
-------- $3960			

This example illustrates what is known as a three by four matrix. Each investor pays $500 to the promoter and is told to build a "downline" by recruiting three new members, who then each should recruit three more members. The investor is told that he will be paid $150 for each of the three members whom he enlists at the first level. The investor is also promised a $30 commission for each recruit at the next three levels. Thus, the investor should receive commission for four levels of recruits below him, each of whom must recruit three more members, hence the name – a three by four matrix.

Figure 6-5

Skimmers are devices that attach to point of sale (POS) devices. They are used to capture credit card and bankcard information. In addition to devices at the point of sale, skimmers can be placed on ATM machines. These devices are essentially elaborate, genuine looking face plates placed over real ATMs. When a customer inserts his or her card, the skimmer reads the card just before the card enters the ATM machine. Typically, a small hidden camera has also been placed in close proximity to capture the customer's PIN number. Less frequently, a fake ATM will be in place, which receives a card, asks for the PIN, and then simply gives an "out of service" or other error message. The customer's card is then returned after recording the card information and PIN number. In addition, certain credit cards using RFID tags (radio frequency identification) can be electronically scanned with a skimmer from a few feet away. Note that enhanced drivers licenses and passports now have RFID tags embedded within them as well, and users of these cards should exercise caution particularly when traveling overseas.

Reshipping is similar to employment and business fraud, and occurs when a person is offered employment and their job is to package and ship products to the "employer" overseas. Unknown to the supposed employee, the goods he or she is packaging and shipping were purchased with fraudulent credit cards, so they are participating in shipping "stolen" merchandise.

Spam is the sending of unsolicited email to bulk email. However, spam can also be used to provoke attacks on company and government computers with viruses or botnets.

Third party receiver of funds has common elements with reshipping. The scammer posts availability of work at home job opportunities and the person's job is to post payments for the company. The business has its supposed client send the employee payment for his or her work. The checks are made out to the employee who is directed to deposit the checks in his or her personal bank account less commission (such as 10%) and then send the remainder (90%) via Western Union to the scammer located overseas. It is common that the person picking up the funds from Western Union will have fake ID, making tracking much more difficult.

6.4 Crimes Against Property

A **cracker** is someone who hacks, and uses his or her skills for illegal and personal gain. Crackers have an illegal intent in mind.

Drive by download occurs when an Internet user visits a website, or views an html email message, and a program is automatically downloaded to the user's computer. Most of the time, the user does not know the program is being installed.

Hacking is the unauthorized use and entry into a network by either a person or some sort of equipment.

A **logic bomb** is like a **Trojan horse** (see malware), but the program is activated upon some event or date.

Malware involves programming developed for doing harm. This could include computer **viruses** and **worms**, or Trojan horses. A virus is a computer program that, when downloaded, causes harm to a computer. A worm it is a self-replicating virus that resides in the computer and duplicates itself but it does not alter files. A Trojan horse is a program with harmful or malicious code that is found inside what the user believes is harmless data or a program. The Trojan horse's goal is to gain control of the user's computer or to harm its programs and data.

A **password sniffer** is a computer program that goes through a network to capture user passwords. It can be used for both legal and illegal means.

Pod slurping involves a person setting up a portable media player, such as an iPod®, to a business network to steal data and information. A keyboard is not needed to pod slurp, and to the casual observer, the person is simply listening to music.

Piggybacking is using an unsecured wireless connections to surf the Internet. This is actually theft of Internet bandwidth and it is communications theft.

Wardriving is driving around with a WIFI laptop and then mapping the houses, apartments and businesses that have unsecured, wireless access points. The driving part is not illegal.

There are many, many more types of crimes against property, but these are just a few.

6.5 Case Study One

This is a Nigerian 419 example.

Ann Marie Poet had worked for Michigan attorney Jules Olsman for nine years. One fall day in 2002, Olsman came back to the office from a business trip to find that paychecks he had just signed were being bounced by his bank. Upon investigation, he quickly learned that Poet, described as a meticulous and religious woman, had written checks over $2.2 million from the firm's account and were sent to Africa in a Nigerian scam. The woman only had $200 signature authority that the firm's financial institution, Bank One, had ignored.[330] The Bank One manager approved these transfers knowing she had limited signature authority. [331]

Since the embezzlement also involved client funds, Olsman eventually had to pump in one-half million in personal funds to cover the loss. He was particularly concerned because he could have been subject to discipline because of the loss of client funds.

Poet made 13 wire transfers between February and August of 2001 that encompassed the $2.2 million loss.[322] She was eventually indicted by a federal grand jury in Detroit, Michigan on 13 counts of wire fraud. Each count carried a maximum penalty of five years in prison and a $250,000 fine.[333]

6.6 Case Study Two

This is a Ponzi example.

P. Scott Scherrer was a smart and dashing attorney formerly from Michigan who later settled in New Hampshire. According to the federal court documents, "Scherrer induced or attempted to induce over 40 individuals or couples – some of them his friends – to "invest" over $3 million, primarily through sales of stock in a software company. False statements concerning the value of the stock and other particulars facilitated the sales and attempted sales. Scherrer did not buy the stock, but used the money to maintain a luxurious lifestyle, including membership in a country club, expensive cars, gambling, frequent vacations, and lavish entertaining,"[334] similar to the fraud perpetrated by Bernie Madoff.

It is interesting to note that Scherrer moved from Michigan to North Carolina to New Hampshire, while committing Ponzi and Pyramid schemes in each state. He was imprisoned in Michigan for a short period of time. It was not until the federal government charged Scherrer with a federal crime that he ended up in prison with a nine-year sentence.[335]

6.7 Case Study Three

Figure 6-6 below represents an example of an Internet employment fraud with ScottsMoneyBlog.com.[336] Frauds of this type should be reported to the Federal Trade Commission.[337]

Employment Fraud from ScottsMoneyBlog.com

Figure 6-6 Used with permission

6.8 Case Study Four

This case study is an example of hacking.

In December 2013, Target Corporation announced to its customers that its computing systems had been hacked between November 2013 to December 2013. Hackers were able to access customer debit and credit card information including names, addresses, email addresses, and phone numbers. At the time of the attack, this was described as the largest computer breach of customer information in US history.[328] Below is a customer letter received by your author, as one of Target's customers.

Target Guest Breach Notification Letter

Dear Target Guest,

As you may have heard or read, Target learned in mid-December that criminals forced their way into our systems and took guest information, including debit and credit card data. Late last week, as part of our ongoing investigation, we learned that additional information, including name, mailing address, phone number or email address, was also taken. I am writing to make you aware that your name, mailing address, phone number or email address may have been taken during the intrusion.

I am truly sorry this incident occurred and sincerely regret any inconvenience it may cause you. Because we value you as a guest and your trust is important to us, Target is offering one year of free credit monitoring to all Target guests who shopped in U.S. stores, through Experian's® ProtectMyID® product which includes identity theft insurance where available. To receive your unique activation code for this service, please go to creditmonitoring.target.com and register before April 23, 2014. Activation codes must be redeemed by April 30, 2014.

In addition, to guard against possible scams, always be cautious about sharing personal information, such as Social Security numbers, passwords, user IDs and financial account information. Here are some tips that will help protect you:

- Never share information with anyone over the phone, email or text, even if they claim to be someone you know or do business with. Instead, ask for a call-back number.
- Delete texts immediately from numbers or names you don't recognize.
- Be wary of emails that ask for money or send you to suspicious websites. Don't click links within emails you don't recognize.

Target's email communication regarding this incident will never ask you to provide personal or sensitive information.

Thank you for your patience and loyalty to Target. You can find additional information and FAQs about this incident at our Target.com/databreach website. If you have further questions, you may call us at 866-852-8680.

Gregg Steinhafel

Chairman, President and CEO

Figure 6-7 Used with permission

6.9 Federal Legislation

This last section will review major federal legislation that controls many of the cybercrimes previously discussed. Laws to be covered include:

1. Computer Fraud and Abuse Act (18 U.S.C. § 1030)
2. Electronic Communications Privacy Act (18 U.S.C. § 2510)
3. Electronic Funds Transfer Act (15 U.S.C. § 1601)
4. Fair Housing Act (42 U.S.C. § 3601)
5. Identify Theft Penalty Enhancement Act (18 U.S.C. § 1001)
6. Mail and Wire Fraud Act (18 U.S.C. § 1343)
7. National Stolen Property Act (18 U.S.C. § 2314)
8. Racketeer Influenced and Corrupt Organizations Act (18 U.S.C. § 1961)
9. Securities Act of 1933 (15 U.S.C. § 77a) and the Securities and Exchange Act of 1934 (15 U.S.C. 78a–78kk)
10. USA Patriot Act (various)
11. Wire Wager Act (18 U.S.C. § 1084)

6.9.1 Computer Fraud and Abuse Act[339]

This law was enacted in 1984 and revised in 1994. It makes illegal the intentional and unauthorized access of a "federal interest computer." A federal interest computer may be:

- used by a financial institution,
- government computers,
- financial systems,
- medical systems,
- interstate commerce, and
- any computer on the Internet.[340]

The concept "federal interest" is interpreted broadly, and covers any area over which the federal government has jurisdiction (such as financial, medical, and government computers and computers relating to national security).

An interesting case based on a violation of the statute was decided by the United States District Court, Western District of Washington State in Seattle, in which a Michigan plaintiff, Justin Gawronski and California plaintiff, A. Bruguier, sued Amazon.com, after a copy of George Orwell's *1984* was deleted from their Kindle electronic reading devices. Amazon had remotely deleted the content from the devices without asking or telling the users, although Amazon did refund the payment amounts. The book was deleted because Amazon developed concerns over possession of the proper copyright permissions to have made the initial sale. Plaintiff's alleged Amazon committed a violation of the Computer Fraud and Abuse Act of 1986. Ultimately the case was settled in September, 2009, for $150,000. Additionally Amazon agreed not to delete or remove content in the future from Kindle devices, absent a few exceptions.[341]

6.9.2 Electronic Communications Act[342]

The Electronic Communications Act (ECPA) was signed into law in 1986. This key law provides rules for the access, use, disclosure, interception, and privacy protections of electronic communications. According to the law, electronic communications are defined as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photo electronic or photo optical system that affects interstate or foreign commerce."[343]

This law protects computer networks and communication systems from tampering and eavesdropping. This law often also forms the basis for the prosecution of crackers.

6.9.3 Electronic Funds Transfer Act[344]

This law "establishes the basic rights, liabilities, and responsibilities of consumers who use electronic fund transfer services and of financial institutions that offer these services. The primary objective of the act and this part is the protection of individual consumers engaging in electronic fund transfers."[345] It outlines the legal rights of a consumer when confronted with a bank mistake or error on an ATM or banking statement, as well as the rights a consumer in case an ATM card is lost or stolen. This law also covers any Internet fraud involving a patron's bank account.

6.9.4 Fair Housing Act[346]

This law is the combination of traditional law with an Internet twist. The Fair Housing Act prohibits discrimination in the sale and rental of housing. The "twist" is that in 2004 the U.S. Department of Justice filed the first federal lawsuit against a website for violation of the law. Specifically, Spyder Web Enterprises was sued over an allegation of publishing notices and online ads on the Internet in violation of the Fair Housing Act,[347] and that Spyder Web discriminated based on race, gender, family status, religion, and national origin.

The law also applies to mortgage or home improvement loans discrimination on the web.

6.9.5 The Identify Theft Penalty Enhancement Act[348]

The Identity Theft Penalty Enhancement Act (ITPEA) is a 2004 law that provides penalties for aggravated identity theft, which is identify theft in conjunction with a felony, such as the use of a stolen identity to commit a crime. A person convicted of aggravated identity theft must serve an additional mandatory two-year prison term beyond the punishment for identity theft.[349]

More recently, Congress passed the Identity Theft Enforcement and Restitution Act of 2008.[350] The Act allows restitution to identity theft victims for time spent recovering from the harm caused by the actual or intended identity theft.

6.9.6 Mail and Wire Fraud Act[351]

This law goes back to the nineteenth century to 1872. Under the Mail and Wire Fraud Act, a person commits mail or wire fraud if he or she has "a) perpetuated a scheme to defraud that includes a material deception; b) with the intent to defraud; c) while using the mails in furtherance of the scheme."[352]

Fraudulent actions on the Internet, fall under this statute. Keep in mind that intent is a key element of this crime and intent must be evident from the facts the perpetrator intended to commit the crime. Punishment for a conviction under the mail fraud statute is a fine or imprisonment for not more than five years, or both. If the violation affects a financial institution, the punishment is increased and "the person shall be fined not more than $1,000,000 or imprisoned not more than 30 years, or both."[353]

6.9.7 The National Stolen Property Act[354]

The National Stolen Property Act (NSPA) criminalizes the "*interstate* transportation, transmittal, transfer, receipt, possession, concealment, storage, barter, sale, or disposal of any goods, wares, merchandise, securities, money or articles used in counterfeiting valued at $5,000 or more."[355] It requires evidence of actual knowledge that the goods were stolen or that the perpetrator should have known they were stolen.[356] Presenting proof that the person receiving goods was unaware the goods were stolen can be admitted as a defense.

6.9.8 Racketeer Influenced and Corrupt Organizations Act[357]

The Racketeer Influenced and Corrupt Organizations Act, known as RICO, is a law originally passed to curb organized crime. However, courts have broadly interpreted the law to also cover criminal enterprises[358] that take place over the Internet. RICO has been used to combat rogue Internet pharmacies and some Internet gambling, along with many other more traditional crimes that are not web based.

Under RICO, certain acts are prohibited, including:

- Investment of income derived from racketeering activities in an enterprise engaged in interstate commerce;
- Acquisition or maintenance of interest in an enterprise that effects commerce *through racketeering activities*;
- Conduct or participation in an *enterprise's affairs* **through** *a pattern of racketeering activities*; or
- Engaging in a conspiracy to do any of the above.[359]

The maximum penalties for racketeering include a fine of up to $25,000 and up to 20 years in prison plus forfeiture of monetary gains and profits.[360]

6.9.9 Securities Act of 1933[361] and the Securities and Exchange Act of 1934[362]

Securities fraud is a crime that has matured from a friend-to-friend interaction to online interaction. In securities fraud, a criminal will use blogs, message boards, and chat rooms that focus on the stock market to make posts that are intended to manipulate stock prices. In other words, the criminal posts lies about the value of a company's stock. This is called "pumping up" the price of the stock, or a pump and dump scheme.[363]

"Pump-and-Dumps" and Market Manipulations[364]

"Pump-and-dump" schemes involve the touting of a company's stock (typically small, so-called "microcap" companies) through false and misleading statements to the marketplace. These false claims could be made on social media such as Facebook and Twitter, as well as on bulletin boards and chat rooms. Pump-and-dump schemes often occur on the Internet where it is common to see messages posted that urge readers to buy a stock quickly or to sell before the price goes down, or a telemarketer will call using the same sort of pitch. Often the promoters will claim to have "inside" information about an impending development or to use an "infallible" combination of economic and stock market data to pick stocks. In reality, they may be company insiders or paid promoters who stand to gain by selling their shares after the stock price is "pumped" up by the buying frenzy they create. ***Once these fraudsters "dump" their shares and stop hyping the stock, the price typically falls, and investors lose their money.***

Figure 6-8

Often times, the criminal in a pump and dump might have a false online identity, which is referred to as a "sock puppet." One example of pumping up involved the former CEO of Whole Foods Market. The CEO, John Mackey used a "sock puppet" and posted messages on Yahoo stock message boards for about seven years to push his company's stock and to criticize the business efforts of his competitors.[365]

6.9.10 USA Patriot Act[366]

The Patriot Act's full name is the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001. It has been controversial from its inception, primarily because many of the traditional constitutional safeguards were changed by its inaction. The law was passed in response to the terrorist attacks of 9/11.

The Patriot Act amended many federal statutes. One key provision is that the federal government may intercept electronic messages that are "relevant to an ongoing criminal investigation".[367] In the past, the law required that a crime first had to have been committed before messages could be intercepted. This law applies to all types of surveillance cases and it is not limited to those that appear to be related to suspected terrorists.

One criticism of the law is the lowering of the bar that the government can use to intercept Internet routing information. The law also allows ISP's to disclose voluntarily to the government customer records and content of electronic transmissions.[368]

Another controversial area of the law is that it allows, "sneak and peek warrants".[369] Such warrants allow federal law enforcement agencies, such as the FBI, to search a home or business without immediately notifying the person or company that they are the target of an investigation. In other words, this section allows for "delayed notice" of search warrants. This is a contentious provision because law enforcement can use these warrants for minor crimes and not only terror and espionage cases.

6.9.11 Wire Wager Act[370]

The U.S. Wire Wager Act makes illegal the use of an electronic wire method (i.e. the Internet) to transmit bets to places where gambling is not allowed. Therefore, a casino set up in the Bahamas is breaking U.S. law if a player in the U.S. plays their games. However, the U.S. does not really have the legal authority to prosecute someone in another country. The federal government relies primarily on the Wire Wager Act (WWA) to prosecute online casino operators.

This law states:

> Whoever being engaged in the business of betting or wagering knowingly uses a wire communication facility for the transmission in interstate or foreign commerce of bets or wagers or information assisting in the placing of bets or wagers on any sporting event or contest, or for the transmission of a wire communication which entitles the recipient to receive money or credit as a result of bets or wagers, or for information assisting in the placing of bets or wagers, shall be fined under this title or imprisoned not more than two years, or both.[371]

There is some controversy application of the law to the Internet; yet attempts to amend the law or enact a specific law on Internet gaming have not been successful. If this law is challenged in court, changes may take effect. Note that many credit card companies decline credit card transactions from online casinos based on pressure from the U.S. DOJ.

6.10 Summary

In this chapter, you learned that the U.S. DOJ classifies computer crimes as a target, as a weapon or tool, and as an accessory or incidental to a crime. Computer crimes can be against a person or business, or against property. Several key federal laws were discussed; however, the list was not intended to be exhaustive. Instead, it was meant to provide an overview of the key crimes that take place on the Internet. It should be noted that most of these laws were not written to address Internet crimes, and courts have been forced to take existing laws and *make them work*.

6.11 Key Terms

Auction fraud	Escrow services fraud	Password sniffer
Auction fraud from Romania	Fair Housing Act	Pod slurping
Computer Fraud and Abuse Act	Hacking	Piggybacking
Conspiracy/RICO	Identity theft	Ponzi/Pyramid
Cracking	Identity Theft Penalty	Racketeer Influenced and Corrupt
Credit card fraud	Enforcement Act	Organizations Act
Counterfeit cashier's checks	Internet extortion	Reshipping
Debt elimination	Investment fraud	Securities Act of 1933
Drive by download	Logic bomb	Securities and Exchange Act of 1934
Email spoofing	Lottery type frauds	Spam
Electronic Communications Privacy Act	Mail and Wire Fraud Act	Third party receiver of funds
Electronic Funds Transfer Act	Malware	USA Patriot Act
Employment/business opportunities fraud	National Stolen Property Act	Wardriving
	Nigerian letter	Wire Wager Act
	Online phishing	

6.12 Chapter Discussion Questions

1. How does the U.S. DOJ describe computer crime?
2. What is a Nigerian letter or "419"?
3. Provide an example of identity theft.
4. What is the difference between hacking and cracking?
5. Who is a third party receiver of funds?
6. What is wardriving?
7. The Mail and Wire Fraud Act goes back to 1872. How can such an old law be relevant to the Internet?
8. Under RICO, what is a criminal enterprise?
9. What is the NSPA?
10. List three key elements of the USA Patriot Act.

6.13 Additional Learning Opportunities

For more information on cybercrime look at the following sources for more ideas:

Department of Justice Computer Crime & Intellectual Property Section's website at http://www.cybercrime.gov;

The Computer Emergency Response Team (CERT) at http://www.cert.org;

The National Infrastructure Protection Center at the FBI at http://www.infragard.net provides regularly updated information and descriptions of cybercrimes;

The Federal Trade Commission at http://www.ftc.gov; and

The Internet Crime Complaint Center at http://www.ic3.gov.

The primary federal law enforcement agencies that investigate domestic crime on the Internet include the Federal Bureau of Investigation (FBI), the United States Secret Service, the United States Immigration and Customs Enforcement (ICE), the United States Postal Inspection Service, and the Bureau of Alcohol, Tobacco and Firearms (ATF).

For more information on identity theft, you can visit the Federal Trade Commission website http://www.ftc.gov in which they have an entire section on this crime and what to do if you become a victim.

6.14 Test Your Learning

1. Drive by download is an example of using a computer
   A. as a target
   B. as a weapon or tool
   C. as an accessory
   D. incidental to a crime

2. Auction fraud is an example of a
   A. crime against a person/business
   B. crime against property
   C. crime against the government
   D. crime against a person/business and property
   E. crime against property and the government

3. Charlie Criminal uses a skimmer to take a person's credit card information from a credit card reader at a gas station. This is an example of
   A. debt elimination
   B. counterfeit cashier's checks
   C. escrow services fraud
   D. identity theft
   E. Ponzi/pyramid

4. A computer program is set to be activated on September 11, 2016, and act as a virus to shut down the system. This is an example of
   A. cracking
   B. logic bomb
   C. pod slurping
   D. piggybacking
   E. wardriving

5. This law provides privacy protection for electronic communications.
   A. Electronic Communications Act
   B. Electronic Funds Transfer Act
   C. Mail and Wire Fraud Act
   D. National Stolen Property Act
   E. RICO

6. This law is used to combat rogue Internet pharmacies.
   A. Electronic Communications Act
   B. Electronic Funds Transfer Act
   C. Mail and Wire Fraud Act
   D. National Stolen Property Act
   E. RICO

7. Pump and dump violates which of the following laws?
   A. Electronic Communications Act
   B. Electronic Funds Transfer Act
   C. National Stolen Property Act
   D. RICO
   E. Securities Act of 1933/Exchange Act of 1934

8. This law allows for sneak and peak warrants.
   A. National Stolen Property Act
   B. RICO
   C. USA Patriot Act
   D. Wire Wager Act
   E. None of the above

9. This law was enacted as a response to the 9/11 attacks in the United States.
   A. National Stolen Property Act
   B. RICO
   C. USA Patriot Act
   D. Wire Wager Act
   E. None of the above

10. In debt elimination fraud
    A. a website advertises it will eliminate a person's debt
    B. the consumer is asked to send a large money deposit with their application
    C. documents from the "loan" company are fake
    D. all of the above
    E. none of the above

Test Your Learning answers are located in the Appendix.

Appendix

Chapter 1: Jurisdiction

1. D	2. B	3. C	4. A	5. A
6. E	7. A	8. A	9. D	10. E

Chapter 2: Privacy Law

1. B	2. B	3. E	4. A	5. C
6. E	7. D	8. A	9. E	10. B

Chapter 3: Trademark and Copyright Law

1. A	2. A	3. D	4. C	5. D
6. C	7. C	8. B	9. B	10. E

Chapter 4: Patent Law and Trade Secrets

1. E	2. E	3. E	4. C	5. C
6. C	7. A	8. F	9. A	10. C

Chapter 5: Free Speech, Defamation, and Obscenity

1. B	2. D	3. D	4. D	5. A
6. A	7. A	8. D	9. E	10. E

Chapter 6: Cybercrime

1. B	2. A	3. D	4. B	5. B
6. B	7. E	8. C	9. C	10. D

Endnotes

1. Merriam-Webster's dictionary defines the Internet as "an electronic communications network that connects computer networks and organizational computer facilities around the world."
2. See http://www.internetlivestats.com/internet-users/.
3. These statistics were reported by Forrester Research at https://www.forrester.com/US+CrossChannel+Retail+Sales+Forecast+2014+To+2018/fulltext/-/E-RES115515 in its "US Cross-Channel Retail Sales Forecast: 2014 To 2018."
4. See http://www.uscourts.gov/Common/Glossary.aspx.
5. In addition to the federal court system and the 50 individual states, there are nine territories under US control. These include American Samoa, the Federal States of Micronesia, Guam, Midway Islands, Northern Mariana Islands, Puerto Rico, the Republic of Palau, the Republic of the Marshall Islands, and the US Virgin Islands. See http://www.usa.gov/Agencies/State-and-Territories.shtml for more information.
6. There is a third type of jurisdiction called in rem jurisdiction, which typically involves real estate or personal property such as large pieces of machinery.
7. See http://www.uscourts.gov/FederalCourts/UnderstandingtheFederalCourts/Jurisdiction.aspx.
8. See http://www.uscourts.gov/EducationalResources/FederalCourtBasics/CourtStructure.
9. See http://www.uscourts.gov/uscourts/rules/civil-procedure.pdf.
10. See http://www.legislature.mi.gov/%28S%28x4issf3c44g4i4u12oyxm445%29%29/mileg.aspx?page=getObject&objectName=mcl-600-705.

11. See http://leg1.state.va.us/cgi-bin/legp504.exe?000+cod+8.01-328.1.
12. Internet disputes often complicate matters when it comes to personal jurisdiction. To understand these hurdles, it will be useful to take a brief look at the case of *International Shoe Co. v. Washington*, 326 U.S. 310 (1945). This United States Supreme Court case held for a court to have personal jurisdiction over an out-of-state resident, the parties must have certain **"minimal" contacts** (emphasis added) within the boundaries where the court sits to establish "presence."
13. For the full text of the *International Shoe* case see https://supreme.justia.com/cases/federal/us/326/310/case.html.
14. *Id.*
15. For the full text of *Calder*, see http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=465&invol=783.
16. For the full text of *Zippo Manufacturing Inc.* see http://cyber.law.harvard.edu/metaschool/fisher/domain/dncases/zippo.htm.
17. See the Memorandum Opinion authored by the Honorable Robert Holmes Bell located at http://law.justia.com/cases/federal/district-courts/michigan/miwdce/1:2011cv01220/68607/265/.
18. The trademark STIFF NIGHTS, No. 3621660 is available at http://tmsearch.uspto.gov/bin/gate.exe?f=doc&state=4801:pnog88.2.1.
19. See http://www.uscourts.gov/Common/Glossary.aspx.

Chapter Two

20 This quote is from an opinion written by Supreme Court Justice Louis Brandeis in *Olmstead v.* U.S., 277 U.S. 438 (1928). This case is located at http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=277&invol=438.

21 A privileged communication is a confidential communication between two parties that is protected by law. For example, communications between a physician and a patient are privileged and protected by law from being shared unless the patient waives the privilege. For more information on privileged communications visit http://ovc.ncjrs.gov/sartkit/develop/comm-confidentiality-a.html.

22 More information on the book is available at http://www.amazon.com/The-Right-Privacy-Caroline-Kennedy/dp/0679744347.

23 *Id. at p. i.*

24 See *Griswold v. Connecticut*, 381 U.S. 479 (1965) located at http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=381&invol=479.

25 *Id.*

26 *Id.*

27 Common law is a term that describes countries with a legal system having a historical basis in English law.

28 See Restatement (Second) of Torts § 652B (1977) located at http://cyber.law.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm.

29 See for example, Kyllo v. *United States*, 533 U.S. 27 (2001), located at http://www.oyez.org/cases/2000-2009/2000/2000_99_8508.

30 This is a common standard used by most states. See https://www.eff.org/issues/bloggers/legal/liability/privacy.

31 A qualified privilege is a relationship that allows the holder of the privilege to make certain statements without liability based on a legal or moral duty. See http://thelawdictionary.org/qualified-privilege/.

32 See Restatement (Second) of Torts § 652D (1977) located at http://cyber.law.harvard.edu/privacy/Privacy_R2d_Torts_Sections.htm.

33 See Restatement (Second) of Torts § 652E (1977) located at http://www.tomwbell.com/NetLaw/Ch05/R2ndTorts.html.

34 See http://www.today.com/id/34733504/site/todayshow/ns/today-today_news/t/obama-image-used-huge-times-square-ad/#.UTzp2VfuxQI.

35 This law creates and amends several sections of the U.S. Code. See http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/content-detail.html.

36 The full text of the Cable Communications Policy Act of 1984 can be located at http://www.law.cornell.edu/uscode/text/47/chapter-5/subchapter-V%E2%80%93A.

37 *Id.*

38 *Id.*

39 The full text of the CAN-SPAM Act of 2003 can be located at http://www.law.cornell.edu/wex/inbox/can-spam_act_core_requirements.

40 *Id.*

41 See http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business.

42 The full text of the Children's Online Privacy Protection Act of 1998 can be located at http://www.law.cornell.edu/uscode/text/15/chapter-91.

43 See http://www.cybertelecom.org/privacy/coppa.htm.

44 See http://www.ftc.gov/news-events/press-releases/2002/04/ftc-protecting-childrens-privacy-online.

45 See http://www.ftc.gov/enforcement/cases-proceedings/022-3028/ohio-art-company.

46 *Id.*

47 This image is Exhibit "B" from the Complaint filed in the case of United States v. The Ohio Art Co., No 3:02CV720 (N.D., Ohio).

48 The full text of the Computer Fraud and Abuse Act of 1986 can be located at http://www.law.cornell.edu/uscode/text/18/1030.

49 See https://ilt.eff.org/index.php/Computer_Fraud_and_Abuse_Act_%28CFAA%29.

50 See http://business.time.com/2013/03/19/u-s-hacker-crackdown-sparks-debate-over-computer-fraud-law/.

51 See http://www.justice.gov/archive/ll/highlights.htm.

52 See http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.

53 The Currency and Foreign Transactions Reporting Act of 1970 can be located at http://www.law.cornell.edu/uscode/text/31/subtitle-IV/chapter-53/subchapter-II.

54 See the Financial Crimes Enforcement Network, U.S. Department of Treasury's *Quick Reference Guide for Money Services Businesses* located at http://www.fincen.gov/financial_institutions/msb/materials/en/bank_reference.html.

55 *Id.*

56 The Electronic Communications Privacy Act of 1986 can be located at http://www.law.cornell.edu/uscode/text/18/2510.

57 See http://www.law.cornell.edu/uscode/text/18/part-I/chapter-119.
58 See http://www.law.cornell.edu/uscode/text/18/part-I/chapter-121.
59 See http://www.law.cornell.edu/uscode/text/18/part-II/chapter-206.
60 See https://it.ojp.gov/default.aspx?area=privacy&page=1285.
61 The Fair Credit Reporting Act of 1970 can be located at http://www.law.cornell.edu/uscode/text/15/1681.
62 See https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf.
63 See http://www.gpo.gov/fdsys/pkg/PLAW-108publ159/pdf/PLAW-108publ159.pdf.
64 The Family Educational Rights and Privacy Act can be located at http://www.law.cornell.edu/uscode/text/20/1232g.
65 *Id.*
66 *Id.*
67 *Id.*
68 *Id.*
69 See http://www2.ed.gov/policy/gen/guid/fpco/ferpa/index.html.
70 The Freedom of Information Act can be located at http://www.law.cornell.edu/uscode/text/5/552.
71 See http://www.foia.gov.
72 See http://www.foia.gov/faq.html#exclusions.
73 See http://www.foia.gov/faq.html#exemptions.
74 Exemptions are listed in 5 U.S.C. § 552(b)(1)–(9).
75 The Gramm-Leach-Bliley Act of 1999 can be located at http://www.business.ftc.gov/privacy-and-security/gramm-leach-bliley-act.

76 See http://www.business.ftc.gov/documents/bus53-brief-financial-privacy-requirements-gramm-leach-bliley-act.

77 *Id.*

78 *Id.*

79 *Id.*

80 The Health Insurance Portability and Accountability Act of 1996 can be located at http://www.hhs.gov/ocr/privacy/.

81 *Id.*

82 *Id.*

83 *Id.*

84 The Privacy Act of 1974 can be located at http://www.law.cornell.edu/uscode/text/5/552.

85 *Id.*

86 See http://www.gsa.gov/portal/content/104253.

87 See http://www.law.cornell.edu/uscode/text/5/552a.

88 *Id.*

89 See https://www.federalregister.gov/.

90 See http://www.law.cornell.edu/uscode/text/5/552.

91 The Privacy Protections Act of 1980 can be located at http://www.law.cornell.edu/uscode/text/5/552a.

92 See http://www.law.cornell.edu/uscode/text/42/2000aa.

93 *Id.*

94 *Id.*

95 The Right to Financial Privacy Act of 1978 can be located at http://www.law.cornell.edu/uscode/text/12/chapter-35.

96 See http://www.justice.gov/archive/ll/highlights.htm.

97 See https://www.epic.org/privacy/rfpa/.

98 *United States v. Miller* involved a case where the defendant failed to pay a liquor tax. The Bureau of Alcohol, Tobacco, and Firearms (ATF) issued a subpoena and requested his banking records. See http://www.oyez.org/cases/1970-1979/1975/1975_74_1179/.

99 The Telephone Consumer Protection Act of 199s can be located at http://www.law.cornell.edu/topn/telephone_consumer_protection_act_of_1991.

100 See http://www.fcc.gov/encyclopedia/telemarketing.

101 *Id.*

102 *Id.*

103 *Id.*

104 The Video Privacy Protection Act of 1988 can be located at http://www.law.cornell.edu/topn/video_privacy_protection_act_of_1988.

105 See http://epic.org/privacy/vppa/.

106 See http://epic.org/privacy/vppa/.

107 See http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/pdf/PLAW-107publ56.pdf and http://www.fincen.gov/statutes_regs/patriot/.

108 See http://www.justice.gov/archive/ll/highlights.htm.

109 See http://www.fincen.gov/statutes_regs/patriot/

110 See http://www.foxnews.com/politics/2011/05/27/senate-clearing-way-extend-patriot-act/|date.

111 See http://www.ecfr.gov/cgi-bin/ECFR?page=browse

112 See http://epic.org/epic/about.html.

Chapter Three

113. See http://www.copyright.gov/circs/circ01.pdf.

114. See http://copyright.gov/help/faq/faq-general.html#protect.

115. See Circular 1, Copyright Basics located at http://copyright.gov/circs/circ01.pdf.

116. See 17 U.S.C. §§ 101–810 located at http://copyright.gov/title17/

117. *Id.*

118. Infringement is unlawful use of copyrighted information. See http://www.copyright.gov/title17/92chap5.html.

119. See Circular 1, *Copyright Basics* located at http://copyright.gov/circs/circ01.pdf.

120. *Id.*

121. See http://copyright.gov/about/.

122. See http://copyright.gov/circs/circ01.pdf.

123. *Id.*

124. Section 101 of the Copyright Act of 1976 defines a work made for hire.

125. *Id.*

126. See http://www.copyright.gov/title17/92chap1.html.

127. See http://www.copyright.gov/title17/92chap1.html#106.

128. See http://copyright.gov/circs/circ14.pdf.

129. See http://copyright.gov/title17/92chap2.html.

130. See http://www.copyright.gov/pr/pdomain.html.

131. *Id.*

132. See http://www.copyright.gov/circs/circ01.pdf.

133. *Id.*

134. *Id.*

135. See http://www.uspto.gov/.

136. See http://www.copyright.gov/circs/circ01.pdf.

137. See http://www.copyright.gov/circs/circ03.pdf

138. *Id.*

139. *Id.*

140. See http://www.copyright.gov/legislation/s505.pdf.

141. See http://www.copyright.gov/circs/circ15a.pdf.

142. See http://copyright.gov/circs/circ12.pdf.

143. See http://www.copyright.gov/circs/circ01.pdf.

144. See 17 U.S.C. § 411.

145. See http://www.law.cornell.edu/uscode/text/17/412.

146. See http://www.copyright.gov/title17/92chap4.html#410.

147. See http://www.law.cornell.edu/uscode/text/17/410.

148. See http://www.law.cornell.edu/uscode/text/17/412.
149. See http://copyright.gov/eco/.
150. *Id.*
151. See http://cocatalog.loc.gov/cgi-bin/Pwebrecon.cgi?DB=local&PAGE=First.
152. See http://www.copyright.gov/fls/fl102.html.
153. See http://fairuse.stanford.edu/overview/fair-use/four-factors/.
154. See http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm01854.htm.
155. See http://fairuse.stanford.edu/overview/public-domain/.
156. See http://www.uspto.gov/trademarks/basics/definitions.jsp.
157. *Id.*
158. The Copyright statute does not define willful. Some courts define it as "the intentional disregard of a known legal duty." Others describe it at "as acting with knowledge or with reckless disregard."
159. Injunctive relief is "a court-orderedact or prohibitionagainst an act or condition which has been requested…" See http://legal-dictionary.thefreedictionary.com/injunctive+relief.
160. See http://www.copyright.gov/title17/92chap5.html#506.
161. See http://www.uspto.gov/trademarks/basics/index.jsp.
162. *Id.*
163. *Id.*
164. See http://www.apple.com/legal/intellectual-property/guidelinesfor3rdparties.html.
165. See http://www.trademarkencyclopedia.com/tylenol/ and http://www.tylenol.com/legal-notice
166. See http://www.uspto.gov/trademarks/basics/definitions.jsp.

167. See http://www.uspto.gov/trademarks/law/Trademark_Statutes.pdf.
168. *Id.*
169. See http://tmsearch.uspto.gov/bin/showfield?f=doc&state=4805:nxnn9j.2.12.
170. Per the USPTO "[a] collective mark is any word, phrase, symbol or design, or a combination thereof owned by a cooperative, an association, or other collective group or organization and used by its members to indicate the source of the goods or services." See http://www.uspto.gov/faq/trademarks.jsp#_Toc275426676.
171. See http://tmep.uspto.gov/RDMS/detail/manual/TMEP/Oct2012/TMEP-1200d1e718.xml#/manual/TMEP/Oct2012/TMEP-1300d1e319.xml.
172. Per the USPTO "[a] certification mark is any word, phrase, symbol or design, or a combination thereof owned by one party who certifies the goods and services of others when they meet certain standards. The owner of the mark exercises control over the use of the mark; however, because the sole purpose of a certification mark is to indicate that certain standards have been met, use of the mark is by others." See http://www.uspto.gov/faq/trademarks.jsp#_Toc275426676.
173. See http://tmep.uspto.gov/RDMS/mashup/html/page/manual/TMEP/Oct2012/TMEP-1300d1e585.xml.
174. See http://www.law.cornell.edu/wex/trade_dress.
175. See Reg. Nos. 696,147 and 1,057,884.
176. See http://tmsearch.uspto.gov/bin/showfield?f=doc&state=4804:mplxlp.4.19.
177. See http://www.uspto.gov/trademarks/index.jsp.
178. See http://www.uspto.gov/faq/trademarks.jsp#_Toc275426681.
179. See http://www.uspto.gov/faq/trademarks.jsp#_Toc275426707.
180. *Id.*
181. See http://www.uspto.gov/faq/trademarks.jsp#_Toc275426708.
182. See http://www.uspto.gov/trademarks/notices/tmrecorduscustoms.jsp.
183. See http://tmsearch.uspto.gov/bin/showfield?f=doc&state=4809:onoy0z.2.20.
184. See http://tmsearch.uspto.gov/bin/gate.exe?f=tess&state=4804:he8miz.1.1.
185. See http://www.law.cornell.edu/wex/trademark_infringement.
186. See http://www.uspto.gov/trademarks/basics/mark.jsp.
187. See http://tmsearch.uspto.gov/bin/showfield?f=doc&state=4807:t4pg3j.5.46.
188. See http://tmsearch.uspto.gov/bin/showfield?f=doc&state=4807:t4pg3j.5.6.6.
189. See http://www.tmcenter.com/information_trademark_faq.htm.
190. See https://www.greyhound.com/default.aspx.
191. See http://world.honda.com/legal/.
192. See 15 U.S.C. §1117.
193. See http://www.uspto.gov/faq/trademarks.jsp#_Toc275426682.
194. See http://www.uspto.gov/trademarks/teas/initial_app.jsp.
195. See http://www.uspto.gov/trademarks/notices/international.jsp.
196. See http://www.uspto.gov/faq/trademarks.jsp#_Toc275426697.
197. See http://www.uspto.gov/trademarks/process/appeal/index.jsp.
198. See http://www.uspto.gov/trademarks/process/search/refusal_grounds.jsp.
199. See http://www.uspto.gov/ip/global/geographical/faq/.
200. *Id.*
201. See http://www.uspto.gov/trademarks/process/.

202. *Id.*
203. *Id.*
204. See http://www.law.cornell.edu/wex/trademark_infringement.
205. See http://www.law.cornell.edu/wex/dilution_trademark.
206. See http://www.gpo.gov/fdsys/pkg/PLAW-109publ312/pdf/PLAW-109publ312.pdf.
207. *Id.*
208. See *Shields v. Zuccarini*, 254 F.3d 476 (3d Cir. 2001)
209. See http://www.internetlibrary.com/publications/anticybsquattSamson9-05_art.cfm.
210. See http://www.law.cornell.edu/uscode/text/15/1125.
211. *Id.*
212. See https://www.courtlistener.com/opinion/2571197/ford-motor-co-v-2600-enterprises/.
213. See http://www.uspto.gov/trademarks/basics/register.jsp.

Chapter Four

214. This type of written agreement restricts dissemination of confidential information during and after employment.
215. See http://www.coca-colacompany.com/stories/the-chronicle-of-coca-cola-birth-of-a-refreshing-idea.
216. See http://www.coca-colacompany.com/press-center/press-releases/coca-cola-moves-its-secret-formula-to-the-world-of-coca-cola#TCCC%20to%20the%20World%20of%20Coca-Cola%20Exhibit%20in%20Atlanta,%20GA.
217. See Kustron, Konnie. Introduction to the American Legal System. London, England: Bookboon, 2013. p. 12.
218. As indicated in Chapter Two, "[a] tort is a wrong of one person against another. Torts are not crimes, but they involve civil disputes, that often result in litigation. A tort by the way is a wrong of one person against another. It is a civil wrong and there needs to some sort of quantifiable damages for recovery."
219. See http://www.law.cornell.edu/wex/trade_secret.
220. See http://www.uniformlaws.org/.
221. See http://www.uniformlaws.org/Act.aspx?title=Trade%20Secrets%20Act.
222. See http://www.legislature.mi.gov/%28S%28ryts5e45ffig0seehsqm2qqu%29%29/mileg.aspx?page=getobject&objectname=mcl-445-1905/.
223. See http://www.law.cornell.edu/wex/trade_secret.
224. "A general equitable principle that no person should be allowed to profit at another's expense without making restitution for the reasonable value of any property, services, or other benefits that have been unfairly received and retained." See http://legal-dictionary.thefreedictionary.com/unjust+enrichment.
225. See http://www.ncga.state.nc.us/EnactedLegislation/Statutes/HTML/ByArticle/Chapter_66/Article_24.html.
226. See http://www.fbi.gov/about-us/investigate/counterintelligence/economic-espionage.
227. See http://www.justice.gov/usao/eousa/foia_reading_room/usam/title9/crm01312.htm.
228. See 35 U.S.C. § 154 located at http://www.law.cornell.edu/uscode/text/35/154.
229. See http://www.uspto.gov.
230. See http://www.aipla.org/advocacy/congress/aia/Pages/summary.aspx.

231. Section 3 of the America Invents Act (AIA), 35 U.S.C. § 146, has an effective date of March 16, 2013.
232. Reduction to practice means making a copy of the invention for the purpose(s) intended.
233. See http://www.uspto.gov/inventors/patents.jsp#heading-1.
234. What can you patent? This is a very good question. According to 35 U.S.C. § 101:
235. "Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefore, subject to the conditions and requirements of this title."
236. *Id.*
237. See *Gottschalk v. Benson*, 409 U.S. 63, 70 (1972).
238. See http://www.uspto.gov/web/offices/pac/mpep/s2106.html and *Burr v. Duryee,* 68 U.S. (1 Wall.) 531, 570 (1863).
239. See *Diamond v. Chakrabarty*, 447 U.S. 303, 308 (1980) (emphasis added) (quoting *Am. Fruit Growers, Inc. v. Brogdex Co.*, 283 U.S. 1 (1931) (Dec. Comm'r Pat. 711 (1931). See also http://www.uspto.gov/web/offices/pac/mpep/s2106.html.
240. See http://thelawdictionary.org/composition-of-matter/.
241. See http://www.uspto.gov/patents/resources/methods/index.jsp.
242. See http://www.uspto.gov/inventors/patents.jsp.
243. See http://www.nrc.gov/about-nrc/governing-laws.html.
244. See http://www.uspto.gov/web/offices/pac/mpep/consolidated_laws.pdf.
245. See http://www.uspto.gov/patents/process/search/index.jsp.
246. See http://www.uspto.gov/inventors/patents.jsp.

247. See http://www.uspto.gov/inventors/patents.jsp#heading-5.
248. See http://www.uspto.gov/web/offices/pac/mpep/consolidated_laws.pdf.
249. See 35 U.S.C. § 102(b).
250. See http://www.law.cornell.edu/uscode/text/35/101.
251. See http://www.law.cornell.edu/uscode/text/35/102.
252. See http://www.law.cornell.edu/uscode/text/35/103.
253. See *KSR International Co. v. Teleflex Inc.*, 550 U.S. 398 (2007) located at http://www.oyez.org/cases/2000-2009/2006/2006_04_1350.
254. *Id. at 1396.*
255. See 35 U.S.C. § 112.
256. See 35 U.S.C. § 112(a).
257. See 35 U.S.C. § 112(b)–(f).
258. See http://www.uspto.gov/patents/index.jsp.
259. See the definition of a claim at http://www.uspto.gov/main/glossary/#c.
260. See http://www.uspto.gov/patents/resources/types/provapp.jsp.
261. *Id.*
262. Available at http://www.uspto.gov/patents/process/index.jsp.
263. Available at http://www.uspto.gov/patents/litigation/What_is_Patent_Infringement.jsp.
264. See http://www.epo.org/.
265. The full text of the Patent Cooperation Treaty is available at the World Intellectual Property Organization (WIPO) website at http://www.wipo.int/pct/en/texts/articles/atoc.htm.
266. See http://www.wipo.int/portal/en/index.html.

Chapter Five

267. The full text of the case is available at http://www.oyez.org/cases/1901-1939/1918/1918_43.
268. This is known as the *Brandenberg* test from the US Supreme Court case of *Brandenburg v. Ohio*, 395 U.S. 444 (1969). See http://www.law.cornell.edu/wex/brandenburg_test.
269. See http://www.uscourts.gov/educational-resources/get-involved/constitution-activities/first-amendment/free-speech.aspx.
270. See http://www.law.cornell.edu/wex/obscenity.
271. See http://legal-dictionary.thefreedictionary.com/defamation for a definition of defamation.
272. *Roth v. United States*, 354 U.S. 476 (1957) is available at http://www.oyez.org/cases/1950-1959/1956/1956_582.
273. *Id. at 480.*
274. *Id. at 480.*
275. *Id. at 481.*
276. *Id. at 485.*
277. *Id. at 488–489.*
278. The full text of the *Miller v. California* case 413 U.S. 15 (1973) is located http://www.law.cornell.edu/supremecourt/text/413/15.
279. This standard is previously described in the *Roth* case.
280. See *Miller v. California*, 413 U.S. 15, 24–25 (1973).

281. Also known as the seven "dirty" words. For details on Carlin's speech, see http://www.theatlantic.com/entertainment/archive/2012/05/the-7-dirty-words-turn-40-but-theyre-still-dirty/257374/.
282. The full text of the *FCC v. Pacifica* case is located at http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=us&vol=438&invol=726.
283. See http://www.oyez.org/cases/1970-1979/1977/1977_77_528.
284. The full text is available at http://transition.fcc.gov/Reports/tcom1996.txt.
285. *Id.*
286. "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." (47 U.S.C. § 230)
287. See https://www.aclu.org/technology-and-liberty/supreme-court-decision-reno-v-aclu-et-al.
288. *Id.*
289. *Id.*
290. *Id.*
291. See http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=000&invol=00-795.
292. See http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=000&invol=00-795.
293. *Id.*
294. *Id.*
295. *Id.*
296. The case can be located at http://www.oyez.org/cases/2000-2009/2001/2001_00_795.
297. *Id at 256.*
298. *Id.*
299. The American Library Association provides a history of the COPA at http://www.ala.org/offices/oif/ifissues/issuesrelatedlinks/cppacopacipa.
300. The text of the law is available at http://www.law.cornell.edu/uscode/text/47/231.
301. See http://www.law.cornell.edu/supct/html/03-218.ZS.html.
302. See http://www.fcc.gov/guides/childrens-internet-protection-act.
303. *Id.*
304. *Id.*
305. Both the FCC and the FTC are involved in the regulation of CIPA. http://www.nap.edu/netsafekids/pp_li_ra.html. For applicable rules, see http://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule.
306. See http://www.fcc.gov/guides/childrens-internet-protection-act.
307. See http://www.law.cornell.edu/uscode/text/18/2251.
308. *Id.*
309. *Id.*
310. See http://www.ca6.uscourts.gov/opinions.pdf/09a0063p-06.pdf.
311. *Id.*
312. See http://www.supremecourt.gov/orders/courtorders/100509zor.pdf.
313. See http://codes.ohio.gov/orc/2739.
314. See http://www.ushistory.org/gov/10b.asp.
315. The full text of the case is available at http://caselaw.lp.findlaw.com/scripts/getcase.pl?court=US&vol=391&invol=563.
316. See http://www.supremecourt.gov/opinions/13pdf/13-483_9o6b.pdf.

Chapter Six

317. See http://www.justice.gov/.
318. See the *U.S. Department of Justice Prosecuting Computer Crimes Manual* located at http://www.justice.gov/criminal/cybercrime/docs/ccmanual.pdf.
319. The Internet Crime Complaint Center (IC3) partnership with the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center (NW3C) categorizes common Internet crimes. Chapter Six reviews crimes that IC3 often investigates.
320. More information on the eBay "money back guarantee" is available at http://pages.ebay.com/ebay-money-back-guarantee/.
321. See http://www.business.ftc.gov/documents/bus61-can-spam-act-compliance-guide-business.
322. See https://postalinspectors.uspis.gov/investigations/mailfraud/fraudschemes/mailtheft/identitytheft.aspx.
323. See http://www.usa.gov/topics/money/identity-theft/prevention.shtml.
324. See http://www.consumer.ftc.gov/articles/0086-international-lottery-scams.
325. See http://www.ic3.gov/crimeschemes.aspx#item-11.
326. See http://www.sec.gov/spotlight/secpostmadoffreforms/oig-509-exec-summary.pdf.
327. See http://www.businessinsider.com/how-bernie-madoffs-ponzi-scheme-worked-2014-7.
328. See http://www.consumer.ftc.gov/articles/0002l-nigerian-email-scam.
329. See http://www.ftc.gov/public-statements/1998/05/pyramid-schemes.
330. See http://www.cbsnews.com/news/an-updated-scam-black-money/.
331. See http://www.dmnews.com/feds-woman-embezzles-21m-in-e-mail-scam/article/78743/.
332. Published sources vary in the amounts, which have been reported from $2.1 to $2.3 million.

333. See http://archive.wired.com/techbiz/media/news/2002/09/55329.
334. See http://www.cbsnews.com/news/an-updated-scam-black-money/.
335. See http://caselaw.findlaw.com/us-1st-circuit/1061656.html.
336. See http://fraudpreventionunit.org/tag/scotts-money-blog/.
337. See http://workbench.cadenhead.org/news/3501/scottsmoneyblogcoms-get-rich-click-scheme.
338. See http://www.bloomberg.com/infographics/2014-05-14/target-data-breach.html.
339. See http://www.law.cornell.edu/uscode/text/18/1030.
340. *Id.*
341. The complaint filed with the court is available at http://www.prnewschannel.com/pdf/Amazon_Complaint.pdf.
342. See https://it.ojp.gov/default.aspx?area=privacy&page=1285.
343. *Id.*
344. See https://www.fdic.gov/regulations/laws/rules/6500-1350.html.
345. *Id.*
346. See http://www.justice.gov/crt/about/hce/title8.php.
347. The URL for the company is http://www.spyderwebenterprises.com/. If you search the Internet archives (http://www.archive.org) and look at the website before 2004, some of the discriminatory language may be available for viewing.
348. See http://www.ssa.gov/legislation/legis_bulletin_062904.html.
349. *Id.*
350. See https://www.govtrack.us/congress/bills/110/hr6060.
351. See http://www.law.cornell.edu/uscode/text/18/1343.
352. See *Neder v.U.S.*, 527 U.S. 1 (1999).
353. See http://www.law.cornell.edu/uscode/text/18/1343.
354. See http://www.law.cornell.edu/uscode/text/18/2314.
355. *Id.*
356. *Id.*
357. See http://www.law.cornell.edu/uscode/text/18/part-I/chapter-96.
358. A RICO enterprise is defined by statute to mean an individual, partnership, corporation, association, or other legal entity, and any union or group of individuals associated together in some type of operation.
359. See http://www.law.cornell.edu/uscode/text/18/part-I/chapter-96.
360. *Id.*
361. See https://www.sec.gov/about/laws/sa33.pdf.
362. See https://www.sec.gov/about/laws/sea34.pdf.
363. See http://www.sec.gov/answers/pumpdump.htm.
364. *Id.*
365. See http://consumerist.com/2007/07/12/whole-foods-ceo-caught-bashing-wild-oats-stock-on-yahoo-forums/.

366. See http://www.justice.gov/archive/ll/highlights.htm.
367. *Id.*
368. *Id.*
369. See http://definitions.uslegal.com/s/sneak-and-peek-search-warrant/.
370. See http://www.law.cornell.edu/uscode/text/18/1084.
371. *Id.*