Ethical, Legal, and Social Responsibilities in E-Commerce
Chapter 10

Ethical, Legal, and Social Responsibilities in E-Commerce

Section 10-1 Internet Law and Ethics

Section 10-2 Privacy Issues and the Internet

Section 10-3 Internet Security
Section 10-1
Why It’s Important

Laws are necessary in all segments of society, and e-commerce is no exception.

Those in the online world should recognize that copyright, patent, and trademark laws protect much of the material found on the Internet.

In addition, they should be aware that there are other types of laws they must follow.
Section 10-1
Key Terms

- cyberlaw
- copyright
- trademark
- patent
Legalities of the Internet

While most transactions and behaviors on the Internet are ethical, some individuals and groups attempt to use the Web for disreputable or illegal purposes.

Consumers and sellers who participate in e-commerce transactions have ethical responsibilities.
Just as the real world requires rules and regulations to keep things running smoothly, the Internet has given birth to cyberlaw.

cyberlaw an evolving legal framework that governs Internet activities; covers topics ranging from copyright infringement to e-mail privacy, identity theft, and interstate e-commerce.
Copyright law protects most text, photos, sounds, software, logos, images, and videos on the Web.

For works copyrighted after 1978, copyright protection generally lasts for the life of the author plus 70 years.

copyright a form of protection provided by U.S. law that grants exclusive rights for the original works of an author
Today’s businesses realize that having a domain name that is the same as their company’s or product’s name can be extremely valuable.

As a result, disputes over domain names have become more common.
Domain-name disputes are generally settled in court.

Legal arguments are presented in court about why a domain name registered to one person or company should be canceled or transferred to another.
You have two options if the domain name you want is already taken:

1. Attempt to buy the domain name from its owner.
2. Select another domain name.
The expansion of the World Wide Web has led to increased trademark-infringement claims and lawsuits.

Trademark infringement occurs when someone uses a name or phrase that is already trademarked.

**trademark** the use of a word, phrase, symbol, product shape, or logo by a manufacturer or business to identify its goods and to distinguish them from others on the market.
Cyberlaw

The ® symbol is used to identify a trademark.

The ™ symbol signifies that a trademark has been applied for but the official trademark registration has not happened yet.
A **patent** excludes others from “making, using, offering for sale, or selling” an invention or idea in the United States or “importing” the invention into the United States.
Ethical Considerations on the Internet

Because the Internet is constantly changing, adherence to an ethical framework is more important than ever.

While there may not be written laws governing every e-business situation, an ethical person will do the right thing in these circumstances.
Ethical, Legal, and Social Responsibilities in E-Commerce

Ethical Considerations on the Internet

E-businesses in the United States must charge sales tax on purchases by customers who live in the same state where the selling company is based or has a physical location.

Many state and local government officials wish to see this policy expanded so that all Internet transactions are taxed, thus ensuring a larger sales tax revenue base.
Section 10-1
Review

1. What options do people or companies have if the domain names they want are already taken?

2. How long does a copyright stay in effect?

3. How are domain-name disputes generally settled?

4. What does it mean when a trademark has been infringed?
Section 10-2

Why It’s Important

All Internet users, including minors, need to be assured of their privacy and the safety of their personal information online.

Since 1997 Congress has been working to craft legislation specifically designed for this purpose.
Section 6-2

Key Terms

- privacy policy
- Electronic Communications Privacy Act of 2000
- spam
Online Privacy

When you shop online, you are asked to provide personal data, including your address, phone number, e-mail address, and credit-card information.

Many online companies make no guarantee that they will use your personal information only to process your order.
Online Privacy

Many online companies sell their customers’ personal information to other businesses that will use it to market their own products and services.

Selling personal data has become big business on the Internet.
To earn your trust, a business can voluntarily post a privacy policy on its Web site.

**privacy policy** a written, legally binding statement informing users about how their personal information will be managed and maintained.
Privacy Policy

The federal government has taken various steps to protect consumers’ rights on the Internet.

The Federal Trade Commission has pursued a number of cases to enforce the promises in privacy statements.
The federal government enacted the *Privacy Act of 1974* to protect individuals’ privacy when dealing with the federal government.

The Privacy Act regulates the ways in which the government can obtain personal information.
The federal government enacted the **Electronic Communications Privacy Act of 2000** to give businesses and organizations the right to monitor e-mail and Internet use on their computers.

**Electronic Communications Privacy Act of 2000** legislation that allows companies to monitor an employee’s e-mail if either the sender or the recipient has given consent or the organization can demonstrate a reason why the company and/or its employees could be harmed by the electronic communication.
Privacy Policy

The Federal Trade Commission (FTC) enforces the *Children’s Online Privacy Protection Act of 1998*, also known as COPPA.

This legislation gives parents control over the information that is collected from their children online and how such information is used.
Privacy Policy

Privacy-protection groups have been organized to inform citizens of the need to protect their personal information.
If you ever go on the Internet, you’re probably familiar with spam.

Like junk mail in the postal system, spam makes up more than half of all messages sent on a daily basis.
Privacy Policy

Spam costs organizations billions of dollars in lost productivity and resources used to combat the problem.

Spam can also carry viruses and other dangers that can damage computer systems.
1. When is it permissible for a company to monitor an employee’s e-mail?

2. Why was the Privacy Act of 1974 created?

3. What is the intended goal of the Children’s Online Privacy Protection Act of 1998?

4. What is spam? Why is it considered harmful?
Section 10-3
Why It’s Important

Computer systems are compromised daily by those seeking confidential information for illegal purposes.

Protecting against this type of activity is crucial for all computer users.
Section 10-3
Key Terms

- hacker
- cybersquatter
- firewall
- Internet filter
- encryption
- virus
- worms
- logic bomb
E-businesses are connected to the Internet 24 hours a day, seven days a week. Maintaining the security of corporate data is one of the highest priorities of any e-commerce business.
Though a company may spend millions of dollars to secure sensitive data, a hacker may still be able to break into the company’s computer system.

**hacker** a person who uses technical expertise to break into computer systems for malicious purposes
There is no typical description of a computer hacker.

Some virus attacks have been perpetuated by people who were unhappy about a job loss or who had a personal grudge against a company or organization.
Another problem e-businesses face is **cybersquatters**.

**Cybersquatter** person who registers domain names of well-known companies or individuals with the sole purpose of selling the names back to the rightful owners to make a profit.
Security of Data

The failure of e-businesses to adequately protect consumer data has led to an increase in identity theft.

Identity theft is the practice of running up bills or committing crimes in someone else’s name.
Security of Data

Any computer that is always connected to the Internet needs a **firewall**.

**firewall** a combination of hardware and software used to block potential hackers from gaining access to a computer system.
An **Internet filter** limits or blocks access to certain Web sites and Internet destinations.

**Internet filter** tool used by organizations to secure computer systems; a software program that limits access to Web sites on the Internet.
E-commerce sites use encryption to secure credit-card data transmitted by customers.
How to Know If a Connection Is Encrypted

The “http” portion of the Web page address will read “https.” The “s” indicates that the page is “secure.”

A small gold padlock will appear in the bottom-right-hand corner of your browser window.
Security of Data

Pretty good privacy (PGP) is the most popular program for encrypting and decrypting e-mail messages.

Both sender and recipient must have the software to encrypt and decrypt the message’s information.
Computer **virus** infections harm computer systems, causing a loss of productivity and sales.

Antivirus software is designed to monitor and eliminate viruses.

**virus** a program written to inflict harm on a computer system and to interfere with its normal operation.
Worms usually come through e-mail messages.

Worms programs that replicate themselves exponentially, causing malicious actions against the computer’s resources and files.
A logic bomb can perform actions such as reformatting a hard drive, or deleting, altering, or corrupting data.

**logic bomb** programming code added to a software program that lies dormant until a predetermined period of time passes or an event occurs, triggering the typically malicious code into action; also called slag code.
What are hackers? How can they damage computer systems?

What is encryption? Why is it necessary?

What is PGP?

Why would a hacker want to destroy computer databases and hard drives? What type of people take part in this?