Chapter 7

The Environment of Electronic Commerce: Legal, Ethical, and Tax Issues

At a Glance

Instructor’s Manual Table of Contents

- Chapter Overview
- Chapter Objectives
- Instructor Notes
- Quick Quizzes
- Discussion Questions
- Additional Resources
- Key Terms
Chapter Overview

In this section, you will learn about the issues of borders, jurisdiction, and Web site content and how these factors affect a company’s ability to conduct electronic commerce. You will also learn about legal issues that arise when the Web is used in the commission of crimes, terrorist acts, and even the conduct of war.

Chapter Objectives

In this chapter, you will learn about:

- Laws that govern electronic commerce activities
- Laws that govern the use of intellectual property by online businesses
- Online crime, terrorism, and warfare
- Ethics issues that arise for companies conducting electronic commerce
- Conflicts between companies’ desire to collect and use data about their customers and the privacy rights of those customers
- Taxes that are levied on electronic commerce activities

Instructor Notes

The Legal Environment of Electronic Commerce

Businesses that operate on the Web must comply with the same laws and regulations that govern the operations of all businesses. If they do not, they face the same set of penalties—fines, reparation payments, court-imposed dissolution, and even jail time for officers and owners—that any business faces.

Businesses operating on the Web face two additional complicating factors as they try to comply with the law. First, the Web extends a company’s reach beyond traditional boundaries. Thus, a company can become subject to many more laws more quickly than a traditional brick-and-mortar business based in one specific physical location. Second, the Web increases the speed and efficiency of business communications. Further, the Web creates a network of customers who often have significant levels of interaction with each other. Web businesses that violate the law or breach ethical standards can face rapid and intense reactions from many customers and other stakeholders who become aware of the businesses’ activities.
Borders and Jurisdiction

Territorial borders in the physical world serve a useful purpose in traditional commerce: They mark the range of culture and reach of applicable laws very clearly. When people travel across international borders, they are made aware of the transition in many ways.

<table>
<thead>
<tr>
<th>Borders and Jurisdiction:</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ <strong>Power:</strong> A form of control over physical space and the people and objects that reside in that space, and is a defining characteristic of statehood. For laws to be effective, a government must be able to enforce them. The ability of a government to exert control over a person or corporation is called jurisdiction.</td>
</tr>
<tr>
<td>♦ <strong>Effects:</strong> Laws in the physical world are grounded in the relationship between physical proximity and the effects, or impact, of a person’s behavior. Personal or corporate actions have stronger effects on people and things that are nearby than on those that are far away.</td>
</tr>
<tr>
<td>♦ <strong>Legitimacy:</strong> The idea that those subject to laws should have some role in formulating them.</td>
</tr>
<tr>
<td>♦ <strong>Notice:</strong> Physical boundaries are a convenient and effective way to announce the ending of one legal or cultural system and the beginning of another. The physical boundary, when crossed, provides notice that one set of rules has been replaced by a different set of rules. Notice is the expression of such a change in rules.</td>
</tr>
</tbody>
</table>

Jurisdiction on the Internet

Governments that want to enforce laws regarding business conduct on the Internet must establish jurisdiction over that conduct. A contract is a promise or set of promises between two or more legal entities - persons or corporations - that provides for an exchange of value (goods, services, or money) between or among them. A tort is an intentional or negligent action taken by a legal entity that causes harm to another legal entity. People or corporations that wish to enforce their rights based on either contract or tort law must file their claims in courts with jurisdiction to hear their cases. A court has sufficient jurisdiction in a matter if it has both subject matter jurisdiction and personal jurisdiction.

Subject-matter Jurisdiction

Subject-matter jurisdiction is a court’s authority to decide a particular type of dispute. For example, in the United States, federal courts have subject-matter jurisdiction over issues governed by federal law (such as bankruptcy, copyright, patent, and federal tax matters), and state courts have subject-matter jurisdiction over issues governed by state laws (such as professional licensing and state tax matters). If the parties to a contract are both located in the same state, a state court has subject matter jurisdiction over disputes that arise from the terms of that contract. The rules for determining whether a court has subject-matter jurisdiction are clear and easy to apply. Few disputes arise over subject-matter jurisdiction.
Conflict of Laws

In the United States, business is governed by federal laws, state laws, and local laws. Sometimes, these laws address the same issues in different ways. Lawyers call this situation a conflict of laws. Since online businesses usually serve broad markets that span many localities and many states, they generally look to federal laws for guidance. On occasion, this can lead to problems with state and local laws.

Contracting and Contract Enforcement in Electronic Commerce

Any contract includes three essential elements: an offer, an acceptance, and consideration. The contract is formed when one party accepts the offer of another party. An offer is a commitment with certain terms made to another party, such as a declaration of willingness to buy or sell a product or service. An offer can be revoked as long as no payment, delivery of service, or other consideration has been accepted. An acceptance is the expression of willingness to take an offer, including all of its stated terms. Consideration is the agreed upon exchange of something valuable, such as money, property, or future services. When a party accepts an offer based on the exchange of valuable goods or services, a contract has been created. An implied contract can also be formed by two or more parties that act as if a contract exists, even if no contract has been written and signed.

- **Written contracts on the Web:** In general, contracts are valid even if they are not in writing or signed. However, certain categories of contracts are not enforceable unless the terms are put into writing and signed by both parties. Most courts will hold that a writing exists when the terms of a contract have been reduced to some tangible form. A signature is any symbol executed or adopted for the purpose of authenticating a writing.
- **Warranties on the Web:** Most firms conducting electronic commerce have little trouble fulfilling the requirements needed to create enforceable, legally binding contracts on the Web. One area that deserves attention, however, is the issue of warranties. Any contract for the sale of goods includes implied warranties. Sellers can avoid some implied warranty liability by making a warranty disclaimer. A warranty disclaimer is a statement declaring that the seller will not honor some or all implied warranties.
- **Authority to form contracts:** Determining whether an individual has the authority to commit a company to an online contract is a greater problem than forged identities in electronic commerce. This issue, called authority to bind, can arise when an employee of a company accepts a contract and the company later asserts that the employee did not have such authority.
- **Terms of service agreement:** Intended to limit the Web site owner’s liability for what you might do with information you obtain from the site. In most cases, a site visitor is held to the terms of service even if that visitor has not read the text or clicked a button to indicate agreement with the terms.

- Ask students to examine a local Web site and then examine the Web sites of an international company, such as Intel or Air Products. Take a look at their forms and posted information. Are there any differences in the information requested or given when someone is from the U.S. as opposed to outside the U.S.?

---

### Quick Quiz

1. ____ is a form of control over physical space and the people and objects that reside in that space, and is a defining characteristic of statehood.
   Answer: Power

2. The ability of a government to exert control over a person or corporation is called ____.
   Answer: jurisdiction

3. A(n) ____ is an intentional or negligent action taken by a legal entity that causes harm to another legal entity.
   Answer: tort

4. True or False: Personal jurisdiction is a court’s authority to decide a particular type of dispute.
   Answer: False

5. A(n) ____ is a commitment with certain terms made to another party, such as a declaration of willingness to buy or sell a product or service.
   Answer: offer
Use and Protection of Intellectual Property in Online Business

Online businesses must be careful in their use of intellectual property. Intellectual property is a general term that includes all products of the human mind. These products can be tangible or intangible. Intellectual property rights include the protections afforded to individuals and companies by governments through governments’ granting of copyrights and patents, and through registration of trademarks and service marks. Online businesses must take care to avoid deceptive trade practices, making false advertising claims, engaging in defamation or product disparagement, and violations of intellectual property rights by using unauthorized content on their Web sites or in their domain names.

<table>
<thead>
<tr>
<th>Web Site Content Issues:</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Copyright infringement: A copyright is a right granted by a government to the author or creator of a literary or artistic work. Note that an entity becomes liable for vicarious copyright infringement if it is capable of supervising the infringing activity and obtains a financial benefit from the infringing activity.</td>
</tr>
<tr>
<td>♦ Patent infringement: A patent is an exclusive right granted by the government to an individual to make, use, and sell an invention. In the United States, patents on inventions protect the inventor’s rights for 20 years. A patent on the design for an invention provides protection for 14 years. To be patentable, an invention must be genuine, novel, useful, and not obvious given the current state of technology.</td>
</tr>
<tr>
<td>♦ Trademark infringement: A trademark is a distinctive mark, device, motto, or implement that a company affixes to the goods it produces for identification purposes. A service mark is similar to a trademark, but it is used to identify services provided. Note that the name that a business uses to identify itself is called a trade name.</td>
</tr>
</tbody>
</table>

Domain Names, Cybersquatting, and Name Stealing

Considerable controversy has arisen recently about intellectual property rights and Internet domain names. Cybersquatting is the practice of registering a domain name that is the trademark of another person or company in the hopes that the owner will pay huge amounts of money to acquire the URL. In addition, successful cybersquatters can attract many site visitors and, consequently, charge high advertising rates. A related problem, called name changing, occurs when someone registers purposely misspelled variations of well-known domain names. These variants sometimes lure consumers who make typographical errors when entering a URL. Name stealing occurs when someone posing as a site’s administrator changes the ownership of the site’s assigned domain name to another site and owner.
Protecting Intellectual Property Online

Several industry trade groups have proposed solutions to the current problems in digital copyright protection, including host name blocking, packet filtering, and proxy servers. All three approaches illustrate how an Internet service provider might try to block access to an entire offending site. However, none of these approaches are really effective in preventing theft or providing identification of property obtained without the copyright holder’s permission.

Defamation

A defamatory statement is a statement that is false and that injures the reputation of another person or company. If the statement injures the reputation of a product or service instead of a person, it is called product disparagement. In some countries, even a true and honest comparison of products may give rise to product disparagement. Because the difference between justifiable criticism and defamation can be hard to determine, commercial Web sites should avoid making negative, evaluative statements about other persons or products.

Deceptive Trade Practices

In general, trademark protection prevents another firm from using the same or a similar name, logo, or other identifying characteristic in a way that would cause confusion in the minds of potential buyers of the trademark holder’s products or services. For example, the trademarked name “Visa” is used by one company for its credit card services and another company for its type of synthetic fiber. This use is acceptable because the two products are significantly different. However, the use of very well-known trademarks can be protected for all products if there is a danger that the trademark might be diluted. Various state laws define trademark dilution as the reduction of the distinctive quality of a trademark by alternative uses. Trademarked names such as “Hyatt,” “Trivial Pursuit,” and “Tiffany,” and the shape of the Coca-Cola bottle have all been protected from dilution by court rulings. A Web site that sells gift-packaged seafood and claims to be the “Tiffany of the Sea” risks a lawsuit from the famous jeweler claiming trademark dilution.

Advertising Regulation

In the United States, advertising is regulated primarily by the Federal Trade Commission. The FTC publishes regulations and investigates claims of false advertising. Its Web site includes a number of information releases that are useful to businesses and consumers.

<table>
<thead>
<tr>
<th>Information Included in FTC Policy Statements:</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Bait advertising</td>
</tr>
<tr>
<td>♦ Consumer lending and leasing</td>
</tr>
<tr>
<td>♦ Endorsements and testimonials</td>
</tr>
<tr>
<td>♦ Energy consumption statements for home appliances</td>
</tr>
<tr>
<td>♦ Guarantees and warranties</td>
</tr>
<tr>
<td>♦ Prices</td>
</tr>
</tbody>
</table>
Online Crime, Terrorism and Warfare

The Internet has opened up many possibilities for people to communicate and get to know each other better - no matter where in the world they live. The Internet has also opened doors for businesses to reach new markets and create opportunities for economic growth. It is sad that some people in our world have found the Internet to be a useful tool for perpetrating crimes, conducting terrorism, and even waging war.

Online Crime

Crime on the Web includes online versions of crimes that have been undertaken for years in the physical world, including theft, stalking, distribution of pornography, and gambling. Other crimes, such as commandeering one computer to launch attacks on other computers, are new.

Law enforcement agencies have difficulty combating many types of online crime. The first obstacle they face is the issue of jurisdiction. Consider the case of a person living in Canada who uses the Internet to commit a crime against a person in Texas. It is unclear which elements of the crime could establish sufficient contact with Texas to allow police there to proceed against a citizen of a foreign country. It is possible that the actions that are considered criminal under Texas and U.S. law might not be considered so in Canada.

Another problem facing law enforcement officers is the difficulty of applying laws that were written before the Internet became prevalent to criminal actions carried out on the Internet.

Online Warfare and Terrorism

The Internet provides an effective communications network on which many people and businesses have become dependent. Although the Internet was designed from its inception to continue operating while under attack, a sustained effort by a well-financed terrorist group or rogue state could slow down the operation of major transaction-processing centers. As more business communications traffic moves to the Internet, the potential damage that could result from this type of attack increases.

Ethical Issues

Companies using Web sites to conduct electronic commerce should adhere to the same ethical standards that other businesses follow. If they do not, they will suffer the same consequences that all companies suffer: the damaged reputation and long-term loss of trust that can result in loss of business. In general, advertising on the Web should include only true statements and should not omit any information that could mislead potential purchasers or wrongly influence their impressions of a product or service. Even true statements have been held to be misleading when the ad omits important related facts. Any comparisons to other products should be supported by verifiable information.
Ethics and Web Business Policies

An important ethical issue that organizations face when they collect e-mail addresses from site visitors is how the organization limits the use of the e-mail addresses and related information. In the early days of the Web, few organizations made any promises to visitors who provided such information. Today, most organizations state their policy on the protection of visitor information, but many do not. In the United States, organizations are not legally bound to limit their use of information collected through their Web sites. They may use the information for any purpose, including the sale of that information to other organizations. This lack of government regulation that might protect site visitor information is a source of concern for many individuals and privacy rights advocates. These concerns are discussed in the next section.

Privacy Rights and Obligations

The issue of online privacy is continuing to evolve as the Internet and the Web grow in importance as tools of communication and commerce. Many legal and privacy issues remain unsettled and are hotly debated in various forums. The Electronic Communications Privacy Act of 1986 is the main law governing privacy on the Internet today. Of course, this law was enacted before the general public began its wide use of the Internet.

Ethics issues are significant in the area of online privacy because laws have not kept pace with the growth of the Internet and the Web. The nature and degree of personal information that Web sites can record when collecting information about visitors’ page-viewing habits, product selections, and demographic information can threaten the privacy rights of those visitors.

<table>
<thead>
<tr>
<th>Principles for Handling Customer Data:</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ Use the data collected to provide improved customer service.</td>
</tr>
<tr>
<td>♦ Do not share customer data with others outside your company without the customer’s permission.</td>
</tr>
<tr>
<td>♦ Tell customers what data you are collecting and what you are doing with it.</td>
</tr>
<tr>
<td>♦ Give customers the right to have you delete any of the data you have collected about them.</td>
</tr>
</tbody>
</table>

Communications with Children

In the United States, Congress enacted the Children’s Online Protection Act (COPA) in 1998 to protect children from “material harmful to minors.” This law was held to be unconstitutional because it unnecessarily restricted access to a substantial amount of material that is lawful, thus violating the First Amendment. Congress was more successful with the Children’s Online Privacy Protection Act of 1998 (COPPA), which provides restrictions on data collection that must be followed by electronic commerce sites aimed at children. This law does not regulate content, as COPA attempted to do, so it has not been successfully challenged on First Amendment grounds. In 2001, Congress enacted the Children’s Internet Protection Act (CIPA).
The CIPA requires schools that receive federal funds to install filtering software on computers in their classrooms and libraries. Filtering software is used to block access to adult content websites. The Supreme Court held that the CIPA was constitutional in 2003.

**Issues Box: MasterCard reveals plan**

MasterCard is launching a two-pronged initiative to help e-tailers crack down on online crime. The Site Data Protection scheme involves e-commerce vendors filling out a MasterCard questionnaire, which is then graded to produce a security rating. The company will also scan e-tailers' websites to check for improper configuration or other security weaknesses.

The second part of the plan involves physical security measures such as chip and pin and the use of a pass code on credit card transactions, as well as a signature. It will be rolled out before January 2005.

Online fraud is a serious problem in the channel because IT equipment is a prime target. According to recent figures released by the Association of Payment Clearing Services, 'card not present' transactions over the internet increased by 68 per cent from £28m in 2002 to £45m last year.

Brian Morris, head of e-business solutions at MasterCard Europe, said: "We are very concerned about fraud. We have a duty to protect cardholders, merchants and banks, and we want to increase trust in shopping securely on the internet."

In addition, MasterCard is teaming up with security specialist Ubizen to offer security services. The credit card company is also working with insurance firm Marsh to provide e-commerce insurance services.

However, David Atherton, managing director of online reseller Dabs.com, said that despite anti-fraud measures by firms such as MasterCard and Visa, there is still some way to go.

"Fraud was a huge problem when payments were made offline because we didn't have the tools to check customer details.

"But now credit card companies are coming round to the right way of thinking and giving us the means to check details online," Atherton said.

"However, some major card issuers have not yet implemented any anti-fraud measures, which means there are still some loopholes for fraudsters."

*Source: http://www.vnunet.com/News/1154483*
Questions

- What are the implications of not implementing anti-fraud measures?

Taxation an Electronic Commerce

An online business can become subject to several types of taxes, including income taxes, transaction taxes, and property taxes. Income taxes are levied by national, state, and local governments on the net income generated by business activities. Transaction taxes, which include sales taxes, use taxes, excise taxes, and customs duties, are levied on the products or services that the company sells or uses. Customs duties are taxes levied by the United States and other countries on certain commodities when they are imported into the country. Property taxes are levied by states and local governments on the personal property and real estate used in the business. In general, the taxes that cause the greatest concern for Web businesses are income taxes and sales taxes.

<table>
<thead>
<tr>
<th>Taxation and Electronic Commerce:</th>
</tr>
</thead>
<tbody>
<tr>
<td>♦ <strong>Nexus:</strong> A government acquires the power to tax a business when that business establishes a connection with the area controlled by the government. This connection between a taxpaying entity and a government is called nexus.</td>
</tr>
<tr>
<td>♦ <strong>U.S. Income Taxes:</strong> The Internal Revenue Service (IRS) is the U.S. government agency charged with administering the country’s tax laws. A basic principle of the U.S. tax system is that any verifiable increase in a company’s wealth is subject to federal taxation. Thus, any company whose U.S.-based Web site generates income is subject to U.S. federal income tax.</td>
</tr>
<tr>
<td>♦ <strong>U.S. State Sales Taxes:</strong> Most states levy a transaction tax on goods sold to consumers. This tax is usually called a sales tax. Businesses that establish nexus with a state must file sales tax returns and remit the sales tax they collect from their customers. If a business ships goods to customers in other states, it is not required to collect sales tax from those customers unless the business has established nexus with the customer’s state. However, the customer in this situation is liable for payment of a use tax in the amount that the business would have collected as sales tax if it had been a local business. Note that a use tax is a tax levied by a state on property used in that state that was not purchased in that state.</td>
</tr>
<tr>
<td>♦ <strong>European Union Value Added Taxes:</strong> The Value Added Tax (VAT) is the most common transfer tax used in the European Union. A VAT is assessed on the amount of value added at each stage of production and is collected by the seller at each stage of the transaction.</td>
</tr>
</tbody>
</table>
Teaching Tip:

♦ Examine different Web sites (K-mart, Best Buy, and Amazon.com) and observe how they handle taxes. Some places charge taxes if the buyer is in the same state as the company. Should this matter? Ask students to research Congressional proposals to charge tax on anything bought on the Internet.

Quick Quiz

1. A(n) _____ is a right granted by a government to the author or creator of a literary or artistic work.
   Answer: copyright

2. An entity becomes liable for _____ if it is capable of supervising the infringing activity and obtains a financial benefit from the infringing activity.
   Answer: vicarious copyright infringement

3. A(n) _____ is an exclusive right granted by the government to an individual to make, use, and sell an invention.
   Answer: patent

4. A(n) _____ is a distinctive mark, device, motto, or implement that a company affixes to the goods it produces for identification purposes.
   Answer: trademark

5. A(n) _____ statement is a statement that is false and that injures the reputation of another person or company.
   Answer: defamatory

Discussion Questions

- What measures can be taken to protect children on the Web?
- Discuss the role of ethics when formulating Web business policies.

Additional Resources

- Copyright infringement: [http://en.wikipedia.org/wiki/Copyright_infringement](http://en.wikipedia.org/wiki/Copyright_infringement)
- Trademark infringement: [http://cyber.law.harvard.edu/metaschool/fisher/domain/tm.htm#7](http://cyber.law.harvard.edu/metaschool/fisher/domain/tm.htm#7)
**Key Terms**

- **Acceptance**: The expression of willingness to take an offer, including all of its stated terms.
- **Contract**: A promise or set of promises between two or more legal entities that provides for an exchange of value (goods, services, or money) between or among them.
- **Cybersquatting**: The practice of registering a domain name that is the trademark of another person or company in the hopes that the owner will pay huge amounts of money to acquire the URL.
- **Income taxes**: Levied by national, state, and local governments on the net income generated by business activities.
- **Nexus**: Connection between a taxpaying entity and a government
- **Property tax**: Levied by states and local governments on the personal property and real estate used in the business.