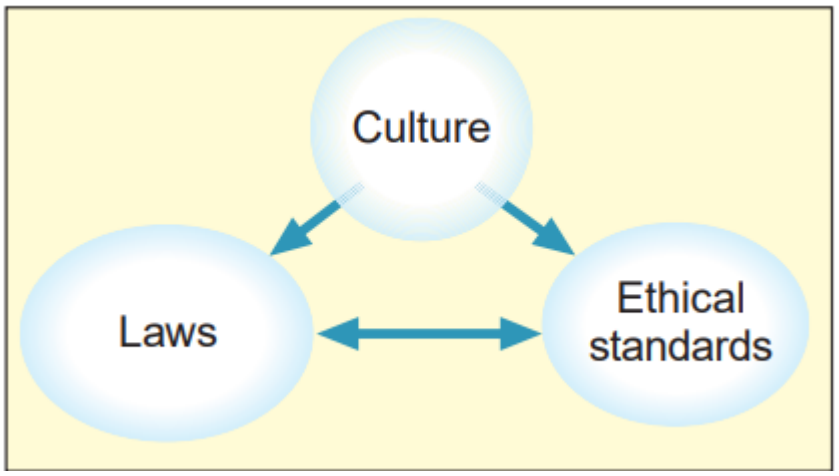
FOE Chapter-2

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. For example, exiting one country and entering another usually requires a formal examination of documents, such as passports and visas. In addition, both the language and the currency usually change upon entry into a new country. Each of these experiences, and countless others, are manifestations of the differences in legal rules and cultural customs in the two countries. In the physical world, geographic boundaries almost always coincide with legal and cultural boundaries. The limits of acceptable ethical behavior and the laws that are adopted in a geographic area are the result of the influences of the area's dominant culture. The relationships among a society's culture, laws, and ethical standards appear in Figure 7-1, which shows that culture affects laws directly and indirectly through its effect on ethical standards. The figure also shows that laws and ethical standards affect each other.



The geographic boundaries on culture are logical; for most of our history, slow methods of transportation and conflicts among various nations have prevented people from travelling great distances to learn about other cultures. Both restrictions have changed in recent years, however, and now people can travel easily from one country to another within many geographic regions. One example is the European Union (EU), which allows free movement within the EU for citizens of member countries. Most of the EU countries (Great Britain being a notable exception) now use a common currency (the euro) instead of their former individual currencies (for example, French francs, German marks, and Italian lire). Legal scholars define the relationship between geographic boundaries and legal boundaries in terms of four elements: power, effects, legitimacy, and notice.

Power

Power 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. For laws to be effective, a government must be able to enforce them. Effective enforcement requires the power both to exercise physical control over residents, if necessary, and to impose sanctions on those who violate the law. The ability of a government to exert control over a person or corporation is called

jurisdiction.

Laws in the physical world do not apply to people who are not located in or do not own assets in the geographic area that created those particular laws. For example, the United States cannot enforce its copyright laws on a citizen of Japan who is doing business in Japan and owns no assets in the United States. Any assertion of power by the United States over such a Japanese citizen would conflict with the Japanese government's recognized authority over its citizens. Japanese citizens who bring goods into the United States to sell, however, are subject to applicable U.S. copyright laws. A Japanese Web site that offers delivery of goods into the United States is, similarly, subject to applicable U.S. laws.

The level of power asserted by a government is limited to that which is accepted by the culture that exists within its geographic boundaries. Ideally, geographic boundaries, cultural groupings, and legal structures all coincide. When they do not, internal strife and civil wars can erupt

Jurisdiction on the Internet

The tasks of defining, establishing, and asserting jurisdiction are much more difficult on the Internet than they are in the physical world, mainly because traditional geographic boundaries do not exist. For example, a Swedish company that engages in electronic commerce could have a Web site that is entirely in English and a URL that ends in ".com," thus not indicating to customers that it is a Swedish firm. The server that hosts this company's Web page could be in Canada, and the people who maintain the Web site might work from their homes in Australia. If a Mexican citizen buys a product from the Swedish firm and is unhappy with the goods received, that person might want to file a lawsuit against the seller firm. However, the world's physical border-based systems of law and jurisdiction do not help this Mexican citizen determine where to file the lawsuit. The Internet does not provide anything like the obvious international boundary lines in the physical world. Thus, the four considerations that work so well in the physical world—power, effects, legitimacy, and notice—do not translate very well to the virtual world of electronic commerce.

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—people or corporations—that provides for an exchange of value (goods, services, or money) between or among them. If either party to a contract does not comply with the terms of the contract, the other party can sue for failure to comply, which is called breach of contract. Persons and corporations that engage in business are also expected to exercise due care and not violate laws that prohibit specific actions (such as trespassing, libel, or professional malpractice). A tort is an intentional or negligent action (other than breach of contract) 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 to hear a matter if it has both subject-matter jurisdiction and personal jurisdiction.

Jurisdiction in International Commerce

Jurisdiction issues that arise in international business are even more complex than the rules governing personal jurisdiction across state lines within the United States. The exercise of jurisdiction across international borders is governed by treaties between the countries engaged in the dispute. Some of the treaties that the United States has signed with other

countries provide specific determinations of jurisdiction for disputes that might arise. However, in most matters, U.S. courts determine personal jurisdiction for foreign companies and
people in much the same way that these courts interpret the long-arm statutes in domestic matters. Non-U.S. corporations and individuals can be sued in U.S. courts if they conduct business or commit tortious acts in the United States. Similarly, foreign courts can enforce decisions against U.S. corporations or individuals through the U.S. court system if those courts can establish jurisdiction over the matter.

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.

Creating Contracts: Offers and Acceptances

People enter into contracts on a daily, and often hourly, basis. Every kind of agreement or exchange between parties, no matter how simple, is a type of contract. Every time a consumer buys an item at the supermarket, the elements of a valid contract are met, for example, through the following actions:

- The store invites offers for an item at a stated price by placing it on a store shelf.
- The consumer makes an offer by indicating a willingness to buy the product for the stated price. For example, the consumer might take the item to a checkout station and present it to a clerk with an offer to pay.
- The store accepts the customer's offer and exchanges its product for the consumer's payment at the checkout station.

Contracts are a key element of traditional business practice, and they are equally important on the Internet. Offers and acceptances can occur when parties exchange e-mail messages, engage in electronic data interchange (EDI), or fill out forms on Web pages. These Internet communications can be combined with traditional methods of forming contracts, such as the exchange of paper documents, faxes, and verbal agreements made over the telephone or in person. The requirements for forming a valid contract in an electronic commerce transaction are met, for example, through the following actions:

- The Web site invites offers for an item at a stated price by serving a Web page that includes information about the item.
- The consumer makes an offer by indicating a willingness to buy the product for the stated price by, for example, clicking an "Add to Shopping Cart" button on the Web page that displays the item.
- The Web site accepts the customer's offer and exchanges its product for the consumer's credit card payment on its shopping cart checkout page.

As you can see, the basic elements of a consumer's contract to buy goods are the same whether the transaction is completed in person or online. Only the form of the offer and acceptance are different in the two environments. The substance of the offer, acceptance, and the completed contract are the same.

When a seller advertises goods for sale on a Web site, that seller is not making an offer, but is inviting offers from potential buyers. If a Web ad were considered to be a legal offer to form a contract, the seller could easily become liable for the delivery of more goods than it has available to ship. A summary of the contracting process that occurs in an online sale appears in Figure 7-4.

Step	Contract element	Participant	Action	
1.	Invites offers	Seller	Promotes product through Web page and states conditions under which offers will be accepted (for example, price and shipping terms)	
2.	Offer	Buyer	Clicks button to make offer to purchase product	
3.	Acceptance	Seller	Accepts buyer's offer, processes payment, and ships product	

When a buyer submits an order, which is an offer, the seller can accept that offer and create a contract. If the seller does not have the ordered items in stock, the seller has the option of refusing the buyer's order outright or counteroffering with a decreased amount. The buyer then has the option to accept the seller's counteroffer.

Making a legal acceptance of an offer is quite easy to do in most cases. When enforcing contracts, courts tend to view offers and acceptances as actions that occur within a particular context. If the actions are reasonable under the circumstances, courts tend to interpret those actions as offers and acceptances. For example, courts have held that a number of different actions—including mailing a check, shipping goods, shaking hands, nodding one's head, taking an item off a shelf, or opening a wrapped package—are each, in some circumstances, legally binding acceptances of offers. An excellent resource for many of the laws concerning contracts, especially as they pertain to U.S. businesses, is the Cornell Law School Web site, which includes the full text of the Uniform Commercial Code (UCC).

Copyright Issues

A copyright is a right granted by a government to the author or creator of a literary or artistic work. The right is for the specific length of time provided in the copyright law and gives the author or creator the sole and exclusive right to print, publish, or sell the work. Creations that can be copyrighted include virtually all forms of artistic or intellectual expression—books, music, artworks, recordings (audio and video), architectural drawings, choreographic works, product packaging, and computer software. In the United States, works created after 1977 are protected for the life of the author plus 70 years. Works copyrighted by corporations or not-for-profit organizations are protected for 95 years from the

date of publication or 120 years from the date of creation, whichever is earlier.
The idea contained in an expression cannot be copyrighted. It is the particular form in which an idea is expressed that creates a work that can be copyrighted. If an idea cannot be separated from its expression in a work, that work cannot be copyrighted. For example, mathematical calculations cannot be copyrighted. A collection of facts can be copyrighted, but only if the collection is arranged, coordinated, or selected in a way that causes the resulting work to rise to the level of an original work. For example, the Yahoo! Web Directory is a collection of links to URLs. These facts existed before Yahoo! selected and arranged them into the form of its directory. However, most copyright lawyers would argue that the selection and arrangement of the links into categories probably makes the directory copyrightable.
In the past, many countries (including the United States) required the creator of a work to register that work to obtain copyright protection. U.S. law still allows registration, but registration is no longer required. A work that does not include the words "copyright" or "copyrighted," or the copyright symbol ©, but was created after 1989, is copyrighted automatically by virtue of the copyright law unless the creator specifically released the work into the public domain.

Patent Issues

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. An inventor may decide to patent the design of an invention instead of the invention itself, in which case the patent protects the design for 14 years. To be patentable, an invention must be genuine, novel, useful, and not obvious given the current state of technology.
In the early 1980s, companies began obtaining patents on software programs that met the terms of the U.S. patent law. However, most firms that develop software to use in Web sites and for related transaction processing have not found the patent law to be very useful. The process of obtaining a patent is expensive and can take several years. Most developers of Web-related software believe that the technology in the software could become obsolete before the patent protection is secured, so they rely on copyright protection.

Trademark Issues

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. In the United States, trademarks and service marks can be registered with state governments, the federal government, or both. The name (or a part of that name) that a business uses to identify itself is called a trade name. Trade names are not protected by trademark laws unless the business name is the same as the product (or service) name. They are protected, however, under common law. Common law is the part of British and U.S. law established by the history of court decisions that has accumulated over many years. The other main part of British and U.S. law, called statutory law, arises when elected legislative bodies pass laws, which are also called statutes.
The owners of registered trademarks have often invested a considerable amount of money in the development and promotion of their trademarks. Web site designers must be very careful not to use any trademarked name, logo, or other identifying mark without the express permission of the trademark owner. For example, a company Web site that includes a photograph of its president who happens to be holding a can of Pepsi could be held liable for infringing on Pepsi's trademark rights. Pepsi can argue that the appearance of its

trademarked product on the Web site implies an endorsement of the president or the company by Pepsi.

Domain Names and Intellectual Property Issues

Considerable controversy has arisen 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 (also called typosquatting), 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. For example, a person might easily type LLBaen.com instead of LLBean.com.

Protecting Intellectual Property Online

Several methods can be used to protect copyrighted digital works online, but they only provide partial protection. One technique employs steganography to create a digital watermark. The watermark is a digital code or stream embedded undetectably in a digital image
or audio file. It can be encrypted to protect its contents, or simply hidden among the bits—digital information—composing the image or recording. Verance is a company that provides, among other products, digital audio watermarking systems to protect audio files on the Internet. Its systems identify, authenticate, and protect intellectual property. Verance's ARIS MusiCode system enables recording artists to monitor, identify, and control the use of their digital recordings.

The audio watermarks do not alter the audio fidelity of the recordings in which they are embedded. The Verance SoniCode product provides verification and authentication tools. SoniCode was originally developed by ARIS Technologies, which is now owned by Verance Corporation. SoniCode can ensure that telephonic conversations have not been altered. The same is true for audiovisual transcripts and depositions. Blue Spike produces a watermarking system called Giovanni. Like the SoniCode system, the Giovanni watermark authenticates the copyright and provides copy control. Copy control is an electronic mechanism
for limiting the number of copies that one can make of a digital work.

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 consider the specific laws in their jurisdiction (and consider consulting a lawyer) before making negative, evaluative statements about other persons or products.

Web site designers should be especially careful to avoid potential defamation liability by altering a photo or image of a person in a way that depicts the person unfavorably. In most cases, a person must establish that the defamatory statement caused injury. However, most states recognize a legal cause of action, called per se defamation, in which a court deems some types of statements to be so negative that injury is assumed. For example, the court will hold inaccurate statements alleging conduct potentially injurious to a person's

business, trade, profession, or office as defamatory per se—the complaining party need not prove injury to recover damages. Thus, online statements about competitors should always be carefully reviewed before posting to determine whether they contain any elements of defamation.

Deceptive Trade Practices

The ease with which Web site designers can edit graphics, audio, and video files allows them to do many creative and interesting things. Manipulations of existing pictures, sounds, and video clips can be very entertaining. If the objects being manipulated are trademarked, however, these manipulations can constitute infringement of the trademark holder's rights. Fictional characters can be trademarked or otherwise protected. Many personal Web pages include unauthorized use of cartoon characters and scanned photographs of celebrities; often, these images are altered in some way. A Web site that uses an altered image of Mickey Mouse speaking in a modified voice is likely to hear from the Disney legal team.

Web sites that include links to other sites must be careful not to imply a relationship with the companies sponsoring the other sites unless such a relationship actually exists. For example, a Web design studio's Web page may include links to company Web sites that show good design principles. If those company Web sites were not created by the design studio, the studio must be very careful to state that fact. Otherwise, it would be easy for a visitor to assume that the linked sites were the work of the design studio.

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 and another company for its synthetic fiber. This use is acceptable because the two products are significantly different and few consumers of credit cards or synthetic fibers would likely be confused by the identical names. 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. Thus, 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 (FTC). 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. The FTC business education campaign publications are available on its Advertising Guidance page, shown in Figure 7-9. These publications include information to help businesses comply with the law.

Any advertising claim that can mislead a substantial number of consumers in a material way is illegal under U.S. law. In addition to conducting its own investigations, the FTC accepts referred investigations from organizations such as the Better Business Bureau. The FTC provides policy statements that can be helpful guides for designers creating. electronic commerce Web sites. These policies include information on what is permitted in advertisements and cover specific areas such as these:

• Bait advertising

• Consumer lending and leasing
• Endorsements and testimonials
• Energy consumption statements for home appliances
• Guarantees and warranties
• Prices

Other federal agencies have the power to regulate online advertising in the United States. These agencies include the Food and Drug Administration (FDA), the Bureau of Alcohol, Tobacco, and Firearms (BATF), and the Department of Transportation (DOT). The FDA regulates information disclosures for food and drug products. In particular, any Web site that is planning to advertise pharmaceutical products will be subject to the FDA's drug labeling and advertising regulations. The BATF works with the FDA to monitor and enforce federal laws regarding advertising for alcoholic beverages and tobacco products. These laws require that every ad for such products includes statements that use very specific language. Many states also have laws that regulate advertising for alcoholic beverages and tobacco products. The state and federal laws governing advertising and the sale of firearms are even more restrictive. Any Web site that plans to deal in these products should consult with an attorney who is familiar with the relevant laws before posting any online advertising for such products. The DOT works with the FTC to monitor the advertising of companies over which it has jurisdiction, such as bus lines, freight companies, and airlines.

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. As you learned earlier in this chapter, determining jurisdiction can be tricky on the Internet. 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. If the crime is theft of intellectual property (such as computer software or computer files), the questions of jurisdiction become even more complex. You can learn more about online crime issues at the U.S. Department of Justice Cybercrime.gov Web site.

The difficulty of prosecuting fraud perpetrators across international boundaries has always been an issue for law enforcement officials. The Internet has given new life to old fraud scams that count on jurisdictional issues to slow investigations of crimes. The advance fee fraud has existed in various forms for many years, but e-mail has made it inexpensive for perpetrators to launch large numbers of attempts to ensnare victims. In an advance fee fraud, the perpetrator offers to share the proceeds of some large payoff with the victim if the victim will make a "good faith" deposit or provide some partial funding first. The perpetrator then disappears with the deposit. In some online versions of this fraud, the perpetrator asks for identity information (bank account number, Social Security number, credit card number, and so on) and uses that information to steal the advance fee.

The most common online version of these schemes is the Nigerian scam (also called the 419 scam, after the number of the section of the Nigerian penal code that specifies penalties

for fraud in that country), in which the victim receives an e-mail from a Nigerian government official requesting assistance in moving money to a foreign bank account. The Financial Crimes Division of the U.S. Secret Service receives more than 100 reports each day about this type of fraud attempt.

Online Warfare and Terrorism

Many Internet security experts believe that we are at the dawn of a new age of terrorism and warfare that could be carried out or coordinated through the Internet. A considerable number of Web sites currently exist that openly support or are operated by hate groups and terrorist organizations. Web sites that contain detailed instructions for creating biological weapons and other poisons, discussion boards that help terrorist groups recruit new members online, and sites that offer downloadable terrorist training films now number in the thousands.

The U.S. Department of Homeland Security and international police agencies such as Interpol are devoting considerable resources to monitoring terrorist activities online. Historically, these agencies have not done a very good job of coordinating their activities around

the world. The threat posed by global terrorist organizations that use the Internet to recruit members and to plan and organize terrorist attacks has motivated Interpol to update and expand its computer network monitoring skills and coordinate global antiterrorism efforts.

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.

Ethics and Online Business Practices

Online businesses are finding that ethical issues are important to consider when they are making policy decisions. Recall from Chapter 3 that buyers on the Web often communicate with each other. A report of an ethical lapse that is rapidly passed among customers can seriously affect a company's reputation. In 1999, The New York Times ran a story that disclosed Amazon.com's arrangements with publishers for book promotions. Amazon.com was accepting payments of up to $10,000 from publishers to give their books editorial reviews and placement on lists of recommended books as part of a cooperative advertising program. When this news broke, Amazon.com issued a statement that it had done nothing wrong and that such advertising programs were a standard part of publisher–bookstore relationships. The outcry on Internet newsgroups and mailing lists was overwhelming. Two days later—before most traditional media outlets had even reported the story—Amazon.com announced that it would end the practice and offer unconditional refunds to any customers who had purchased a promoted book. Amazon.com had done nothing illegal, but the practice appeared to be unethical to many of its existing and potential customers.

In early 1999, eBay faced a similar ethical dilemma. Several newspapers had begun running stories about sales of illegal items, such as assault weapons and drugs, on the eBay auction site. At this point in time, eBay was listing about 250,000 items each day. Although eBay would investigate claims that illegal items were up for auction on its site, eBay did not actively screen or filter listings before the auctions were placed on the site. In 2009, a number of software developers complained that the Apple Apps Store (which

you learned about earlier in this book) was slow to approve software to be sold on its Web site. Apple responded that it had a responsibility to protect its customers (the owners of its iPhone product) from unscrupulous software vendors who might try to sell applications for the iPhone that do not function properly, crash the phone, or install malware. Apple argued that its testing and approval program was necessary to maintain customer confidence in its products, even though it had no legal obligation to perform such testing on software provided by third-party developers and sold on the Apps Store Web site.

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 Web sites state the organization's 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. The law was written to update an existing law that prevented the interception of audio signal transmissions so that any type of electronic transmissions (including, for example, fax or data transmissions) would be given the same protections. In 1986, the Internet was not used to transmit commercially valuable data in any significant amount, so the law was written to deal primarily with interceptions that might occur on leased telephone lines.