E-Commerce: Regulatory, Ethical, and Social Environments

15

Contents

Learning Objectives

Upon completion of this chapter, you will be able to:

1. Understand the foundations for legal and ethical issues in EC.
2. Describe intellectual property law and understand its adjudication.
3. Explain privacy and free speech issues and their challenges.
4. Describe types of fraud on the Internet and how to protect against them.
5. Describe the needs and methods of protecting both buyers and sellers.
6. Describe EC-related societal issues.
7. Describe Green EC and IT.
8. Describe the future of e-commerce.

OPENING CASE: WHY WAS DISNEY FUNDING CHINESE PIRATES?

In 2006, Disney's funding arm, Steamboat Ventures, invested $10 million in one of the largest Chinese video- and file-sharing site called 56.com (**56.com**). The site is very popular in China, Taiwan, Singapore, and Hong Kong.

The Problem

In May 2008, The Walt Disney Company released its animated film *Wall-E*; the film was released on DVD in November 2008. However, immediately

Electronic supplementary material The online version of this chapter (doi: 10.1007/978-3-319-10091-3_15) contains supplementary material, which is available to authorized users

E. Turban et al., *Electronic Commerce: A Managerial and Social Networks Perspective*, Springer Texts in Business and Economics, DOI 10.1007/978-3-319-10091-3_15,

after the movie release in May, the robot love story was available to download and watch for free on the Chinese video site 56.com. In other words, Disney was funding a Chinese site that bootlegs its own work.

A major reason that pirated movies are difficult to detect is that the same movie may appear under different names. Although 56.com managed to remove some of the full-length bootlegged copies, many others still remain. The 56.com site is often referred to as a Chinese version of YouTube. However, unlike YouTube, 56.com and similar sites like Youku Tudou Inc. (China's leading Internet television company) do not impose 15-minute limits on uploaded videos, which makes them a haven for illegally uploaded videos, including full-length movies and TV episodes. Note, it is possible today to upload videos longer than 15 minutes by using special procedures.)

If 56.com were located in the United States, we would expect the Motion Picture Association of America (MPAA) and similar organizations in other countries to pressure the "bootlegging" company to remove copyrighted materials. However, China has not had a very solid record of enforcing intellectual property rights. Therefore, the Chinese government is turning to harsher punishments for piracy of copyrighted material. In 2011, they discovered over 2,000 cases of copyright infringement and arrested 4,000 people. The government has vowed to create harsher punishments to combat the problem (see Billboard Biz 2011).

The Solution

Before Disney's affiliate, Steamboat Ventures, invested in 56.com, they knew they faced a battle preventing pirated movies and TV shows from being shown on the 56.com site. However, Steamboat Ventures said that they were attracted to the site's 'refined, controlled, and effective technology platform,' as well as its large user base. Although Steamboat was aware of the piracy issue, they thought that they "could promote legal content on the site and work towards eliminating pirated materials" (see McBride and Chao 2008).

In the United States, you can take legal action against companies such as 56.com for copyright violations. For example, in 2007, Viacom sued YouTube for $1 billion, requesting access to the viewing habits of YouTube users On March 18, 2014, Google (owner of YouTube) and Viacom settled out of court, finally resolving the seven-year long *Viacom v. YouTube* litigation.

Note that, in China, the government, which in the past provided only warnings to violators, is increasing penalties for violations of copyright infringement. In November 2013, several Chinese video companies, including Youko Tudou and Tencent Video, along with the Motion Picture Association of America (MPAA), joined together in Beijing to fight against video online infringement and piracy in China. Legal action had already been taken against Baidu and QVOD (see **marketwatch.com/story/joint-action-against-online-video-piracy-in-china-2013-11-13**). In 2013, Chinese authorities closed the largest piracy website and arrested 30 employees.

The Results

56.com allowed the downloading of free movies, video games, and the like until about 2010. Disney did not seem to be too concerned with this. Its investment provides 56.com with a distribution channel for its Disney products that may provide a strategic advantage to Disney in China. In March 2009, Disney allowed YouTube to run short videos as well as full episodes of its ABC (a television station) and ESPN (Internet and television sports channel) networks under an ad-revenue sharing arrangement.

In August 2009, 56.com launched 'Kankan 56' (**kankan.56.com**), a fee-based innovative video content platform that provides user-paid benefits to original video authors, video makers, and copyright owners in exchange for video sharing. Video uploaders charge users for viewing and set their own prices, with 56.com taking a 10% commission; the video can be viewed for 15 days only. By 2014, 56.com was purchased by the social network RenRen.

Sources: Based on *56.com* (2009), Albanesius (2008), and McBride and Chao (2008).

LESSONS LEARNED FROM THE CASE

Copyright violation on the Internet is a major problem for creators and distributors of intellectual property such as software, movies, music, and books. The problem arises not only because it is difficult to monitor millions of users and their posts, but also because in many countries there is not a great deal of legal protection of copyrighted material; and even if there is, it is difficult and very expensive to enforce.

Protection of intellectual property is one of the major EC legal issues presented in this chapter. An overview of other intellectual property topics, and especially privacy, are also presented. A full analysis of legal and ethical issues is far beyond the scope of one chapter. For comprehensive treatment and case studies, see Mann and Winn (2008). This chapter also covers several societal issues related to EC, especially the potential environmental impacts from what is known as *"Green EC,"* and how societal issues may affect individual privacy and enjoyment of life.

Note: For a collection of free e-books, slide shows, and files and documents about ethical, social, and political issues in e-commerce, see **pwebs.net/i/internet-ethics**.

15.1 ETHICAL CHALLENGES AND GUIDELINES

Ethics is a set of moral principles or rules of how people are expected to conduct themselves. It specifies what is considered by society to be right or wrong.

Issues of privacy, ownership, control, and security must be confronted in implementing and understanding the ethical challenges of EC.

Ethical Principles and Guidelines

Public law embodies ethical principles, but the two are not the same. Acts that generally are considered unethical may not be illegal. Lying to someone may be unethical, but it is not illegal. Conversely, the law is not a collection of ethical norms, and not all ethical codes are incorporated into public law. Online File W15.1 shows a framework for ethical issues.

One example of an ethical issue is the Facebook class action lawsuit of 2009, described next.

Example: Who Owns User-Generated Content?

In August 2009, five Facebook users filed a class action lawsuit against Facebook, claiming that Facebook violated privacy laws by gathering online users' activity and providing their personal information to third parties without the users' permission. They also alleged that Facebook engages in data mining, without informing the users.

The objective of the data collection was to enable Facebook to sell their users' data to advertisers because Facebook needed more revenue sources. The Electronic Privacy Information Center filed a complaint with the FCC, alleging that Facebook's changes in privacy settings made users' information publicly available without giving the users the option to opt out. Facebook was found to be liable for violating the privacy of their users and amended their rules (see ComputerWeekly.com 2009). Facebook has continuously been modifying and changing its privacy settings, letting its users decide how much they want to share with the public.

Business Ethics

Business ethics (also known as *corporate* or *enterprise ethics*) is a code of values, behaviors, and rules, written or unwritten, for how people should behave in the business world. These ethics dictate the operations of organizations. For details, see Ferrell et al. (2012). For implementation considerations, see Business for Social Responsibility (**bsr.org**).

The Issues of Internet Abuse in the Workplace

In 2009, 24/7 Wall St. (**247wallst.com**) conducted a workplace study about how people spend time online. Their findings revealed that actual time wasted and productivity losses were staggering; about one-fourth of the hours spent online during the workday were spent on personal matters (per blog by Mike Plitzer; **plixer.com/blog/2010/10/page/4** October 6, 2010). In general, employees spent more than one hour per week on social media alone, followed by online games and e-mails. A majority of companies have banned access to social networks such as Facebook, Twitter, MySpace, and LinkedIn. In 2013, *SFGate* (per Gouveia 2013) conducted a survey in which they found that 69% of the employees were wasting time for 30 minutes to several hours per day. The top five employee "time wasters" were: checking news (37%), social networking (14%); online shopping (12%), and online entertainment (11%). For an article see **salary.com/2014-wasting-time-at-work**.

Managing Internet Abuse

Instead of banning the use of social networks in the workplace, some employers are following less draconian measures by setting the following policies in place: employees are encouraged to check their social networks only once or twice a day, consolidate their social networking streams, develop a clear social networking policy, and utilize technology made for consolidation. A social networking policy should communicate clear guidelines from employers to employees. For example, employees should not spend more than 20 minutes per day of company time browsing social networks.

Monitoring Employees: Is It Ethical?

Google and several other software application providers have incorporated new spyware on company smartphones given to employees, which enables employers to monitor the whereabouts of their employees using the smartphones' built-in GPS tracking systems. Google's Latitude enables companies to know their employees' location at all times. The ethical question is, whether this new power will be used by governments to invade the privacy of an individual's real-time whereabouts. In other words, rules and procedures for ethical behavior are needed for business people practicing EC. Two major risks are criminal charges and civil suits. Table 15.1 lists examples of safeguards to minimize exposure to those risks (also see Yamamura and Grupe 2008).

EC Ethical and Legal Issues

There are many EC- and Internet-related ethical issues that are related to legal issues (Himma and Tavani 2008). These issues are often categorized into intellectual property rights, privacy, free speech versus censorship, and fraud protection methods.

Table 15.1 Typical safeguards to minimize exposure to risk of criminal or civil charges

1. Does the website clearly post shipping policies and guarantees? Can the selling company fulfill its policies and guarantees? Does it comply with Federal Trade Commission (FTC) rules?
2. Does the website clearly articulate procedures for customers to follow when returning a shipment or when seeking a refund for products or services not received, or received in bad or damaged condition?
3. Has the company checked partners' backgrounds before entering into agreements with third-party vendors and supply chain partners? Do those agreements include protection of the company against all possible risks?
4. Is there sufficient customer support staff, and are they knowledgeable and adequately trained to process customers' inquiries?

- **Intellectual property rights.** Ownership and value of information and intellectual property. Intellectual property is difficult to protect on the Web. Owners are losing a substantial amount of money due to piracy (see Section 15.2).
- **Privacy.** Because it is so difficult to protect the privacy of individuals on the Web, there are some countries that do not regulate privacy issues while others have strict anti-invasion rules (Section 15.3).
- **Free speech versus censorship.** Free speech on the Web may result in offensive and harmful attacks on individuals and organizations (Section 15.4). Therefore, some countries have decided to censor material on the Internet.
- **Consumer and merchant protection against fraud.** For e-commerce to succeed, it is necessary to protect all transactions and participants against fraud (Section 15.5).

Examples of ethical issues discussed elsewhere in this book are channel conflict (Chapters 3 and 13), pricing conflict (Chapter 3), disintermediation (Chapters 3, 4, and 13), and trust (Chapter 9). Two additional EC-related ethical issues are Internet use that is not work-related and code of ethics. See also **investopedia.com/terms/c/code-of-ethics.asp**.

Internet Use that Is Not Work-Related

As described earlier, a majority of employees use e-mail and surf the Web for purposes not related to work. The use of company property (i.e., computers, networks) for e-mail and Internet use may create risk and waste time. The degree of risk depends on the extent to which the company has implemented policies and procedures to prevent and detect illegal uses. For example, companies may be held liable for their employees' use of e-mail to harass other employees, participate in illegal gambling, or distribute child pornography (Gray 2010).

Code of Ethics

A practical and necessary approach to limiting Internet surfing that is not work-related is an Internet Acceptable Use Policy (AUP) to which all employees must conform. It includes EC, social networks, and any IT-related topics. Without a formal AUP, it is much more difficult to enforce acceptable and eliminate unacceptable behaviors and reprimand violators. Whenever a user signs on to the corporate network, the user should see a reminder of the AUP and be notified that online activities are monitored. Such notification should be a part of a code of ethics.

A corporate *code of ethics* sets out the rules and expected behaviors and actions of a company. Typically, the code of ethics should address the use of offensive content and graphics, as well as proprietary information. It should encourage employees to think about who should and who should not have access to information before they post it on the company's website. The code should specify whether the company allows employees to set up their own Web pages on the company intranet and provide policies regarding private e-mail usage and surfing during working hours. A company should formulate a general idea of the role it wants websites to play in the workplace. This should guide the company in developing an AUP and provide employees with a rationale for that policy. Finally, do not be surprised if the code of ethics looks a lot like simple rules of etiquette – it should. Table 15.2 lists several useful guidelines for a corporate Web policy. For a list of website quality guidelines, see Online File W15.2. For business ethics case studies, see **harpercollege.edu/~tmorris/ekin/resources.htm.**

SECTION 15.1 REVIEW QUESTIONS

1. List seven ethical issues related to EC.
2. List the major principles of ethics.
3. Define business ethics.
4. Give an example of an EC activity that is unethical but not illegal.
5. How can employees abuse the Internet? How do small companies handle this?
6. Describe the issues of monitoring employees.
7. List the major issues that should be included in a code of ethics.

Table 15.2 Corporate web policy guidelines

Issue written guidelines regarding employee use of the Internet, including e-mail, instant messaging and social network sites
Make it clear to employees that they cannot use copyrighted or trademarked material without permission
Post disclaimers concerning Web content that the company does not support
Post disclaimers of responsibility concerning content of online forums and chat sessions
Make sure that Web content and activity comply with the laws in other countries (if you are conducting business there), such as those governing intellectual property and privacy
Make sure that the company's Web content policy is consistent with your company's other policies
Appoint someone to monitor Internet legal and liability issues and have that person report to a senior executive or to a legal counsel
Have attorneys with cyberlaw expertise review Web content to make sure that there is nothing unethical or illegal on the company's website and that all required statements and disclaimers are properly included

15.2 INTELLECTUAL PROPERTY LAW AND COPYRIGHT INFRINGEMENT

The legal system is faced with the task of maintaining a delicate balance between preserving social order and protecting individual rights. Keep in mind that, when used in law, the term *individual* is broadly defined to mean a person, group of people, or other legal entity, such as an organization or corporation. In this section, we explain some types of intellectual property laws and the issues arising from EC.

Intellectual Property in E-Commerce

Intellectual property (IP) refers to property that derives from the creative work of an individual, such as literary or artistic work. Intellectual property can be viewed as the ownership of intangible assets, such as inventions, ideas, and creative work. It is a legal concept protected by patents, copyrights, trademarks, and trade secret law (known as **Intellectual Property Law**).

Intellectual property law also may be concerned with the regulation of thought-related products, including creativity. It affects such diverse subjects as the visual and performing arts, electronic databases, advertising, and video games. Creativity is a critical success factor in the business world, and is the foundation of innovation. See the World Intellectual Property Organization website (go to **wipo.int**).

There are various intellectual property law specialties, as shown in Table 15.3. Those specialty laws are interrelated and may even overlap.

Recording Movies, Shows and Other Events

A common method of infringement is to bring video cameras and video-capable cell phones to movie theaters and record the performances. PirateEye (**pirateeye.com**) is one of the companies that manufacture devices that discover and identify the presence of any digital recording device, monitor remotely in real time, and much more.

Copyright Infringement and Protection

Numerous high-profile lawsuits already have been filed regarding online copyright infringement related to EC and the Web (e.g., see the closing case in this chapter). A **copyright** is an exclusive legal right of an author or creator of intellectual property to publish, sell, license, distribute, or use such work in any desired way. In the United States, content is automatically protected by federal copyright laws as soon as a work is produced in a tangible shape or form. A copyright does not last forever; it is good for a set number of years after the death of the author or creator (e.g., 50 years in the United Kingdom). After the copyright expires, the work reverts to the public domain (or becomes publicly available). See **fairuse.stanford.edu/overview/public-domain** and **thepublicdomain.org**. In many cases, corporations own copyrights. In such a case, the copyrights will last 120 years, or even

Table 15.3 Intellectual property laws and the protections of intellectual property

Laws	Protection provided by the law
Intellectual property law	Protects the creative work of people
Patent law	Protects inventions and discoveries
Copyright law	Protects original works of authorship, such as music and literary works, artistic design and writing computer codes
Trademark law	Protects trademarks, logos, etc.
Trade secret law	Protects proprietary business information
Law of licensing	Enables owners of intellectual property to share it via licensing.
Law of unfair competition relating to counterfeiting and piracy	Protects against those who use illegal or unfair methods, or methods not available to others. Also against those pirating intellectual property

longer. The legal term for the use of a work without permission or contracting for payment of a royalty is **copyright infringement**.

File Sharing

One of the major methods of violating copyrights is *file sharing*. File sharing became popular in the late 1990s through facilitating companies such as Napster. One of the players in this area is The Pirate Bay (see the closing case to this chapter). The loss to copyright holders is estimated to be several billion dollars annually. The Recording Industry Association of America (RIAA) is fighting back.

Examples

The file sharing business is a major target of the RIAA, which shut down popular sites LimeWire LLC and Kazaa. Additionally, another popular file sharing site, Megaupload.com, was shut down in January 2012 (see Barakat 2012). However, the site was re-launched in January 2013 under the domain name **mega.co.nz**.

Legal Aspects of Infringement

In November 2010, the U.S. Senate Judiciary Committee approved the controversial Combating Online Infringement and Counterfeits Act (COICA) that provides the Attorney General with the power to shut down websites without a trial or court order if copyright infringement is considered to be the "central activity of the site" (see Gustin 2010). The problem is that, under this bill, most business websites are considered publishers (e.g., even when publishing an online sales brochure), and may be subject to disruptive investigations. (e.g., see Fogarty 2010). Note, this bill was still in debate as of May 2015.

The RIAA Industry Versus the Violators

To protect its interests, the RIAA uses selective lawsuits to stamp out rampant music piracy on the Internet. The RIAA spent more than $58 million in pursuit of targeted infringers between 2006 and 2008, yet collected less than $1.4 million (less than about 2%) from judgments (Frucci 2010).

However, since 2009, the number of lawsuits has been declining for several reasons. For example, see Bambauer (2010). Another example is Google's victory against Viacom's $1 billion copyright violation lawsuit. In 2013, Viacom lost its case against YouTube (the appellate court ruled in favor of Google). Finally, pending copyright infringement lawsuits are not favored because they are lengthy and very costly. As an alternative to direct lawsuits, the entertainment industry has begun developing digital rights management (DRM) policies to be enforced through the court system as well through federal legislation.

Globalization

Much of the media piracy occurs in other countries (e.g., Russia, China, and Sweden, as per the closing case of Pirate Bay), and therefore it is difficult to regulate. According to Doctorow (2012), most piracy occurs in developing countries.

Digital Rights Management (DRM)

Digital rights management (DRM) describes a system of protecting the copyrights of data circulated over the Internet or digital media. These arrangements are technology-based protection measures (via encryption or using watermarks). Typically, sellers own the rights to their digital content. In the past, when content was analog in nature, it was easier to buy a new copy of a copyrighted work in the form of a physical medium (e.g., paper, film, tape) than to produce such a copy independently. The quality of most copies often was inferior. Digital technologies make it possible to produce and distribute a high-quality duplicate of any digital recording with minimal effort and cost. The Internet virtually has eliminated the need for a physical medium to transfer a work, which has led to the use of DRM systems for protection. For details, see **eff.org/issues/drm**. However, DRM systems may restrict the *fair use* of material by individuals. In law, **fair use** refers to the limited use of copyrighted material, without paying a fee or royalty, for certain purposes (e.g., reviews, commentaries, teaching).

All is not simple when implementing DRM system applications. For example, Apple has a controlled ecosystem called 'jailbreaker.' In Apple's losing argument, the company claimed that jailbreaking should not be considered fair use, even though it provides great value to consumers (see Kravets 2010 and Anderson 2010).

Patents

According to Fedcirc.us, a **patent** is "an exclusive right to a particular invention. Patents are granted by states or governments to the creator of an invention, or to someone who has been designated by them to accept the rights over the invention. The holder of the patent has sole rights over the invention for a specified period of time" (e.g., 20 years for applications filed on or after June 8, 1995 in the United States and 20 years in the United Kingdom). Patents serve to protect the idea or design of the invention, rather than any tangible form of the invention. (For details, see **money.howstuffworks.com/question492.htm**, **internetpatentscorporation.net**, and the United States Patent and Trademark office (**uspto.gov**).

There is some discrepancy between the U.S. and Europe over the way certain patents are granted. For example, in 1999, Amazon.com successfully obtained a U.S. patent for its "1-Click" ordering and payment procedure. Using this patent, Amazon.com sued Barnes & Noble in 1999, alleging that its rival had copied its patented technology. Barnes & Noble was enjoined by the courts from using their "Express Lane" payment procedure. However, on May 12, 2006, the USPTO ordered a reexamination of the "1-Click" patent. In March 2010, the Amazon patent was rewritten in the U.S. to include only a shopping cart, and was approved as such. Nevertheless, Expedia and many other e-tailers use similar "checkout" systems today. See **en.wikipedia.org/wiki/1-Click**.

There is a big debate about granting patents for *business methods*. Companies may unknowingly use a business method, unaware that there is already a patent for that method. An example of a business method that was involved in litigation is Amazon's '1-click' ordering system. More than 13 years after Amazon's patent application, the patent was approved in Canada. For a discussion, see Kalanda (2012).

In legal cases involving business methods, some companies were allowed to avoid paying royalties, because they were unaware a patent for the business method already existed. The business methods patent is meant to protect new ways of doing business. In 2010, the Supreme Court ruled that patents cannot cover abstract ideas.

Another example of a legal case involving patents is when Canadian firm i4i Corporation sued Microsoft, for patent infringement, alleging that Microsoft had infringed i4i's patent relating to text manipulation software. Microsoft wanted the standard changed by which patents would be deemed invalid. Microsoft took the case all the way to the U.S. Supreme Court and lost. For details, see Greene (2011).

Oracle Versus Google

In following its legal right of enforcement, Oracle has been mining its newly acquired patent portfolio and actively seeking and suing infringers. In 2012, Oracle sued Google over its Android product for using Oracle's Java technology (copying Java code) without a license. While the trial court

ruled that APIs are not subject to copyright, the appeals court disagreed, holding that Java's API packages were copyrightable, although it sent back the case to the trial court to determine whether or not Google's copying was a violation of the Fair Use Doctrine. As of June 2014, Google has not appealed this decision to the U.S. Supreme Court.

Trademarks

According to the USPTO, 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 trademark is used by individuals, business organizations, or other legal entities to notify consumers of a unique source, and to tell the difference between a company's products or services and those of others. Although federal registration it is not necessary, there are several advantages, such as informing the public that the trademark belongs to the registrants, and giving them exclusive right of use (see **uspto.gov/trademarks/basics/definitions.jsp**.)

Trademark dilution is the use of a "famous" trademark by a third party, which causes the lessening (or dilution) of the 'distinguishing quality' of the mark (see **bitlaw.com/trademark/dilution.html**). In 1996, the Federal Trademark Dilution Act (FTDA) was enacted to safeguard well-known trademarks from third-party users. In 2006, the Trademark Dilution Revision Act (TDRA) was passed, which amended the earlier law. For details and a comprehensive discussion on trademark dilution, see Owens (2011).

In 2008, eBay won a landmark trademark case against Tiffany, a leading jewelry retailer, who had sued eBay alleging that many of the items being advertised on eBay as Tiffany merchandise were actually fakes. The U.S. court ruled in 2008 that eBay cannot be held liable for trademark infringements "based solely on their generalized knowledge that trademark infringement might be occurring on their websites" (Savitz 2008).

Fan and Hate Sites

Fan and hate websites are part of the Internet self-publishing and user-generated content (UGC) phenomena that includes blogging. Fan sites may violate intellectual property rights. For example, some people illegally obtain copies of new movies or TV shows and create sites that compete with the legal sites of the movie or TV producer, even before the legal site is activated. Although the producers can get a court order to shut such sites down, new sites can appear the next day. In contrast with fan websites, there are *hate websites* that disseminate negative comments about corporations and individuals, and can cause problems for them.

Many hate sites are directed against large corporations (e.g., Walmart, Microsoft, Nike).

Cyberbashing

Associated with hate sites is **cyberbashing**, which is the registration of a domain name that criticizes (normally maliciously) an organization, product, or person (e.g., **paypalsucks.com**, **walmartsucks.org**, **verizonpathetic.com**).

SECTION 15.2 REVIEW QUESTIONS

1. What is intellectual property law? How is it helpful to creators and inventors?
2. Define DRM. Describe one potential impact on privacy and one drawback.
3. What is meant by "fair use"? How does the "jailbreaking" of iPhones fall under "fair use"?
4. Define trademark infringement and discuss why trademarks need to be protected from dilution.
5. Describe fan and hate sites. How do they benefit society? Should they be more regulated?
6. Define cyberbashing. Should attempts to expose unscrupulous corporate activities be banned?

15.3 PRIVACY RIGHTS, PROTECTION, AND FREE SPEECH

Privacy has several meanings and definitions. In general, privacy is the state of not being disturbed by others, being free from others' attention, and having the right to be left alone and not to be intruded upon. (For other definitions of privacy, see the Privacy Rights Clearinghouse at **privacyrights.org**.) Privacy has long been a legal, ethical, and social issue in most countries.

The reason for privacy concerns stems from the fact that in using the Internet, users are asked to provide some personal data in exchange for access to information (such as getting coupons, other downloads, etc.). Data and Web mining companies receive and gather the collected data. As a result, users' privacy may be violated (e.g., Stein 2011; and a slide presentation titled "Your Data, Yourself" by Justyne Cerulli at **prezi.com/fgxmaftxrxke/your-data-yourself**).

Privacy rights protection is one of the most debated and frequently emotional issues in EC and social commerce. According to Leggatt (2012), in a survey conducted by TRUSTe, 90% of Internet users "were found to worry about their online privacy." Here we explore the major aspects of the problem as it relates to social networking. Many EC activities involve privacy issues ranging from collection of information by Facebook to the use of RFID. Here is an example.

Example: Google Glass

In May 2013, eight lawmakers, concerned about Google Glass (and other smart glasses), wrote a letter to Google asking what the company planned do to protect people's privacy. See Guynn (2013) for a description.

Social Networks Changing the Landscape of Privacy and Its Protection

Today's youth seem to be less concerned about privacy than they were in the past. The younger generations are more interested in blogs, photos, social networking, and texting. Attitudes about what constitutes private information are changing. As a result, there are new opportunities for marketers and marketing communication, mainly in offering experiences that are better personalized, which do not violate Internet user privacy. See Bhargava (2010) for a discussion.

This problem has been articulated by Andrews (2012), who studied privacy protection in social networks and concluded that very little privacy protection exists (e.g., college applicants are being rejected because of what they posted on the social networks; criminals read posts about vacations to know when to break into an empty house).

However, in May 2014, Facebook announced the addition of the 'Anonymous Login' feature and changes in login procedures, which allow users to try apps without sharing personal information from Facebook.

Information Pollution and Privacy

Information pollution (presented in Chapter 14), the adding of irrelevant, unsolicited information, may raise privacy issues such as the spreading of misinformation about individuals. In addition, polluted information used by decision makers or by UGC may cause invasion of privacy.

Global View

Note that the issue of privacy on the Internet is treated differently in different countries. For example, in November 2009, Google was sued in Switzerland over privacy concerns regarding its Street View application (Pfanner 2009). In 2012, the Swiss highest court ruled that Google may document residential street fronts with its Street View technology, but imposed some limitations on the kinds of images the company can take (e.g., lowering the height of its Street View cameras so they would not peer over garden walls and hedges). For more about the court's decision and the reaction of the parties, see O'Brien and Streitfeld (2012). In June 2013, the European Union highest court determined that government agencies cannot force Google to remove links to personal material. However, in May 2014, Europe's highest court ruled that people should have the right to say what information is available when someone Googles them. The ruling applies to 28 nations and all search engines (Google, Bing) in Europe. The decision does not apply to the U.S. or any other country outside Europe (see Sterling 2014).

Privacy Rights and Protection

Today, virtually all U.S. states and the federal government (and many other countries) recognize the right to privacy, but few government

agencies actually follow all the statutes (e.g., citing reasons of national security). One reason is that the definition of privacy can be interpreted quite broadly. However, the following two rules have been followed closely in past U.S. court decisions: (1) the right to privacy is not absolute. Privacy must be balanced against the needs of society; (2) the public's "right to know" is superior to the individual's right to privacy. The vagueness of the two rules shows why it is sometimes difficult to determine and enforce privacy regulations.

Section 5 of the Federal Trade Commission Act protects privacy. For an explanation of the FTC Act, see **ftc.gov/news-events/media-resources/protecting-consumer-privacy**. Those practices extend to protecting consumer privacy, including the "do not track" option, protecting consumers' financial privacy, and the Children's Online Privacy Protection Act (COPPA).

Opt-In and Opt-Out

Privacy concerns have been overshadowed by post-9/11 counterterrorism activities, but consumers still want their data protected. One way to manage this issue is the *opt-in* and *opt-out* system, generally used by direct marketing companies. **Opt-out** is a method that gives consumers the choice to refuse to share information about themselves, or to avoid receiving unsolicited information. Offering the choice to opt-out is good customer practice, but it is difficult to opt out in some industries, either because consumer demand for opting out is low or the value of the customer information is high.

In contrast, **opt-in** is based on the principle that consumers must approve in advance what information they receive from a company, or allow a company to share their information with third parties. That is, information sharing should not occur unless customers affirmatively allow or request it.

See also the Direct Marketing Association (**thedma.org**) for information and resources on consumers' ad choices, opt-in and opt-out, privacy, identity theft, and more.

According to IBM (2008a), the following six practices for implementing a successful privacy project are:

1. **Get organized.** This can be done by creating a cross-functional privacy team for guidance.
2. **Define the privacy protection needs.** Decide what needs to be protected.
3. **Conduct inventory of data.** List and analyze all data that need protection.
4. **Select solution(s).** Choose and implement a solution that protects privacy.
5. **Test a prototype system.** Create a prototype of the system and test it under different conditions.
6. **Expand the project scope.** Expand the project to encompass other applications.

For further information on privacy protection, see IBM (2008a) and the International Association of Privacy Professionals (**privacyassociation.org**).

Some Measures of Privacy Protection

Several government agencies, communities, and security companies specialize in privacy protection. Representative examples in the U.S. include the Consumer Privacy Guide (**consumerprivacyguide.org/law**), Privacy Protection (**privacyprotect.org/about-privacyprotection**), Privacy Choice (**privacychoice.org**), and Home PC Firewall Guide (**firewallguide.com/privacy.htm**). Finally, Cagaoan et al. (2014) describe the issue of privacy awareness in e-commerce. Other issues are reported by Shah et al. (2013).

Free Speech Online Versus Privacy Protection

Although the First Amendment of the U.S. Constitution grants the right to free speech, as with many rights, the right to free speech is not

unlimited. The First Amendment does not give citizens the right to say absolutely anything to anyone. Defamation laws (including privacy violations), child pornography, fighting words, and terrorist threats are some of the traditional restrictions on what may be said freely. For example, it is illegal to scream "fire" in a crowded theater or make bomb threats in an airport, but there is no law against taking pictures in public places. Free speech often conflicts with privacy, protection of children, indecency, and so forth. For a discussion of the First Amendment and the ten rights it does not grant, see **people.howstuffworks.com/10-rights-first-amendment-does-not-grant.htm#page=1**.

Even in the United Kingdom, there is an increasing risk of police stopping citizens for taking photographs in a public place. In 2010, police questioned amateur photographer Bob Patefield under "anti-terrorist legislation," and later arrested him for "antisocial behavior" (e.g., taking pictures of Christmas decorations, which the police deemed to be "suspicious behavior"). Patefield videotaped his arrest and posted it on the Internet for public viewing (see Lewis and Domokos 2010 for the video and **theguardian.com/uk/2010/feb/21/photographer-films-anti-terror-arrest** for the story).

Example

Anthony Graber, a motorcyclist in Maryland was stopped by a plainclothes state police officer driving an unmarked car. He filmed his own traffic stop by using a camera attached to his motorcycle helmet. He posted his video on YouTube in March 2010, and as a result, was charged with violating state wiretap laws for audio recording the officers and posting the video on the Internet without police consent. Graber was arrested and faced up to 16 years in prison for this undisclosed recording. He pled guilty to speeding, but fought the charge of illegal monitoring, citing Freedom of Speech as a defense. The court ruled that the state trooper had "no legal expectation of privacy," and that videotaping is protected under the First Amendment. The court dismissed all of Graber's charges, except for the traffic violations. See **youtube.com/watch?v=QNcDGqzAB30&feature=related**.

Free Speech Online Versus Child Protection Debate

The debate over free speech versus child protection began in December 2000, after the *Children's Internet Protection Act (CIPA)*, which mandated the use of filtering techniques in libraries and schools that receive federal funding, was signed into law. For details of the debate regarding public libraries, see ACLU of Washington State (2006). In June 2003, the Supreme Court handed down a ruling that the CIPA was constitutional, allowing Congress to require some kinds of blocking, but the filters must not block too much material. Their review represented the third time justices had heard arguments pitting free speech against attempts to protect children from offensive online content. In 2001, the FCC issued rules implementing CIPA, and updated those rules in 2011. (For background and requirements of CIPA, see the FCC Children's Internet Protection Act at **fcc.gov/guides/childrens-internet-protection-act**.)

The Price of Protecting an Individual's Privacy

In the past, gathering information about individuals, that was residing in government agencies' databases, was difficult and expensive to do, which helped protect privacy. The Internet, in combination with powerful computers, and targeting algorithms with access to large-scale databases, have in all practical terms, eliminated the barriers of protecting citizens' privacy.

In the UK in 2010, Heathrow airport security officials were caught circulating printouts of a Bollywood star's full naked body scans downloaded from the full-body security scanners. However, authorities feel that the scanning process is necessary for airport security. Today's technology even enables monitoring people's activities from a distance, which may be considered a violation of their privacy, as shown in Case 15.1.

CASE 15.1: SCHOOL ADMINISTRATORS USED WEBCAMS TO SPY ON STUDENTS AT HOME

Unbeknownst to the students in a Pennsylvania high school, administrators were caught spying on the activities of the underage students. The administrators did this by remotely activating webcams built into each laptop that was issued to the students by the Lower Merion School District, without the permission or knowledge of the students or their parents.

The continued surveillance of the students, even while they were at home, by school officials at Harriton High School revealed that one student was conducting what the school defined as "improper behavior." Based on the video taken at his home, the student was confronted at the school by the assistant principal, and shown "photographic evidence." The school told the parents that they can do such monitoring. As a result, one student filed a class action lawsuit representing all the students who received laptops, for invasion of privacy and illegal interception of private information. The case was settled in October 2010 and the school district paid $610,000. In 2011, the same school district was sued by a former student over the secret monitoring of laptops in 2009.

Sources: Based on Hill (2010), Schreiber (2010), Lattanzio (2010), and **courthousenews.com/2010/02/18/Eyes.pdf** (accessed June 2014).

Questions

1. What legitimate excuse could be made to justify this behavior? Why should the school's actions be stopped?
2. What federal laws were broken? What rights in the U.S. Constitution were violated?
3. What precedent did this decision set? Can you see a way that schools will be allowed to continue this behavior for a narrowly construed purpose?
4. Find other similar cases.

Here is another example of freedom of speech on the Internet conflicting with public safety.

Example: Sheriff Sues Craigslist to Curb Prostitution

The Sheriff of Cook County, Illinois, filed a federal lawsuit in March 2009, alleging that Craigslist had become the top provider of prostitution services in the United States.

The sheriff wanted Craigslist to shut down the erotic services category of its website and compensate his department for the cost of prosecuting website-related prostitution cases. However, advocates for free speech on the Web argued that existing laws insulate Craigslist from any illegal activities related to its ads, and they predicted the sheriff's legal action would not prevail. For details, see San Miguel (2009). Nonetheless, in May 2009, Craigslist removed the "erotic services" category altogether. Craigslist then developed an "adult services" section where they vetted all material before allowing it to be posted. Moreover, in September 2010, Craigslist closed all adult services ads on its site (Miller 2010).

How Information About Individuals Is Collected and Used Online

An individual's private data can be gathered in a number of ways over the Internet. Representative examples of the ways that the Internet can be used to find information about an individual are provided next; the first three are the most common ways of gathering information on the Internet.

- By a user completing a registration form including personal data
- By tracking users' movement on the Web (e.g., by using cookies)
- By using spyware, keystroke logging, and similar methods
- By website registration
- By reading an individual's blog(s) or social network postings
- By looking up an individual's name and identity in an Internet directory or social network profile

- By reading an individual's e-mail, IM, or text messages (hacking)
- By monitoring employees in real time
- By wiretapping conversations over communication lines
- By using wearables such as smart glasses (Chapter 6), including invisible ones (see Leonhard 2014).

We describe some of the above issues next.

Website Registration

Virtually all B2C sites, marketing websites, online magazines, vendors, government sites, and social networks ask visitors to fill out registration forms. During the process, individuals voluntarily provide information such as their name, address, phone number, e-mail address, hobbies, likes or dislikes, and other personal information in order to participate in some free activity, download a paper or read an article, win a lottery, or receive some other benefit. The site might use the information it collected to improve customer service, or it might sell the information to third parties (e.g., other businesses), where it is possible that the information could be used inappropriately.

Internet users are not too happy about giving such information to online businesses. Most people dislike registering at websites they visit and 15% refuse to register. Many do not trust companies that request such information and do not want to share their personal information. In 2012, Facebook was accused by a German advocacy group of allegedly violating privacy laws in Germany. The group wanted Facebook to stop giving to third parties Facebook users' private information until Facebook receive explicit consent from the users. Although Facebook did not admit any wrongdoing, they agreed to cooperate.

Cookies

A popular way for a website to gather information about an individual is by using cookies. As described in Chapter 9, *cookies* enable websites to keep track of users' online movements without asking the users for permission.

Originally, cookies were designed to help with personalization and market research; however, cookies can also be used to disseminate unsolicited commercial information. Cookies allows vendors to collect detailed information about a user's online behavior. The personal data collected by cookies often are more accurate than information provided by users, because users have a tendency to falsify information while filling out registration forms. Although the ethical use of cookies is still being debated, concerns about cookies reached a peak in 1997 at the U.S. FTC hearings on online privacy. Following those hearings, Netscape and Microsoft introduced options enabling users to *block cookies.* Since that time, the uproar surrounding cookies has subsided because most users accept cookies or know how to delete them. The problem with deleting or disabling cookies is that the user will have to keep reentering information each time she or he return to a website, because of not being recognized and, in some instances, may be blocked from viewing useful pages.

Cookies can be successfully deleted by informed users with programs such as: Cookie Monster and CCleaner; to delete and manage flash cookies, see **flashcookiecleaner.com**. By setting the privacy levels on Web browsers very high, cookies from all websites are blocked, and existing cookies cannot be read.

Spyware as a Threat to Privacy and Intellectual Property

In Chapter 10, we discussed **spyware** as a tool that some merchants use to gather information about users without their knowledge. Spyware infections are a major threat to privacy and intellectual property.

Spyware may enter the user's computer as a virus or as a result of the user clicking some innocent looking, but harmful, links. Spyware is effective in illegally tracking users' Internet surfing habits. Using spyware clearly is an invasion of the computer user's privacy and may be illegal. It can also slow down computer performance. While specific spyware can harvest data, it can also be used to take pictures from an unsuspecting user's Webcam and e-mail or post the photos all over the Internet.

Sophisticated tracking technology is being installed into the computers of unsuspecting Internet users. While most are innocuous, some tools include malware, which can cause major damage. The information collected on individuals by spyware is frequently exchanged or sold on the online black market (Chapter 10).

Unfortunately, antivirus software and Internet firewalls cannot always detect all spyware; therefore, extra protection is needed. Many free and low-cost antispyware software packages are available. Representative free antispyware programs are Lavasoft's Ad-Aware (**lavasoft.com**), Microsoft security essentials (**windows.microsoft.com/en-us/windows/security-essentials-download**), and AVG (**avg.com**). Programs that charge a fee include Trend Micro (**trendmicro.com**) and Kaspersky Lab (**usa.kaspersky.com**). Upgraded versions of free programs are also available for a fee. Symantec and other companies that provide Internet security services also provide anti-spyware software.

Even if you use antispyware on your home computer, your smartphone and your PC or tablet that use public Wi-Fi connections may be giving out your personal information by transmitting your location back to your cell phone/Internet provider about every seven seconds. Government supercomputers are capable of reading every e-mail sent, listening to every mobile conversation, reading every text message, knowing every user's location (e.g., GPS), and following every credit card purchase besides tracking every website visited by Internet users around the globe. Records about when you are at church, school, work, a political rally, or a hospital or clinic are stored for months or even years.

RFID's Threat to Privacy

Although several states have mandated or are considering legislation to protect customers from loss of privacy due to RFID tags, as mentioned in Online Tutorial T2 and in Chapter 12, privacy advocates fear that the information stored on RFID tags or collected with them may violate an individual's privacy.

Other Methods

Other methods of collecting data about people are:

- **Site transaction logs.** These logs show what users are doing on the Internet.
- **EC ordering systems and shopping carts.** These features permit sellers to know buyers' ordering history.
- **Search engines.** Search engines can be used to collect information about users' areas of interest.
- **Web 2.0 tools**. Blogs, discussion groups, chatting, social networks, etc. contain a wealth of information about users' activities and personalities.
- **Behavioral targeting.** Using tools to learn people's preferences (Chapter 9).
- **Polling and surveys.** People's demographics, thoughts, and opinions are collected in surveys.
- **Payment information and e-wallets.** These may include sensitive information about shoppers.

Monitoring Employees

There are several issues concerning Internet use at work and employee privacy. In addition to wasting time online, employees may disclose trade secrets and possibly make employers liable for defamation based on their actions on the corporate website. In response to these concerns, many companies monitor their employees' e-mail and Web surfing activities. One tool that enables companies to monitor their employees is Google Location, which works in combination with a compatible device (e.g., Android, iOS).

Example: The Ontario Versus Quon Case

In 2003, a police sergeant named Jeff Quon and three other officers sued the City of Ontario, California, alleging Fourth Amendment violations. The case involved text messages sent and received by Sergeant Quon and his colleagues on pagers issued to them by the City. Because Quon

exceeded the allotted number of messages allowed by the City, the City conducted an audit by reviewing the text messages and found that the vast majority of Quon's messages (as many as 80 per day while he was on duty) were not work-related, and many were sexually explicit. However, the City claimed that since the text messages fell under the City's public information policy, they would be eligible for auditing. While a lower court in California sided with the City, in 2008, the appellate court reversed the decision, ruling that the search was unreasonable. However, the City appealed to the U.S. Supreme Court, which issued a ruling in 2010, holding that the City's review of the text messages did not violate Quon or his co-plaintiffs' Fourth Amendment rights (see Sager et al. 2010 and **oyez.org/cases/2000-2009/2009/2009_08_1332**).

The issue of monitoring employees is complex and debatable because of the possibility of invasion of privacy. For comprehensive coverage, see PRC (2014). For more about employers and Internet usage monitoring, see **wisegeek.org/how-do-employers-monitor-internet-usage-at-work.htm**.

Privacy Protection by Information Technologies

Dozens of software programs and IT policies and procedures are available to protect your privacy. Some were defined in Chapter 10. Representative examples are:

- **Platform for Privacy Preferences Project (P3P)**. Software that communicates privacy policies (described later in this chapter).
- **Encryption.** Software programs such as PKI for encrypting e-mail, payment transactions, and other documents.
- **Spam blocking.** Built into browsers and e-mail; blocks pop-ups and unwanted mail.
- **Spyware blocking.** Detects and removes spyware and adware; built into some browsers.
- **Cookie managers.** Prevents the computer from accepting cookies; identifies and blocks specific types of cookies.
- **Anonymous e-mail and surfing.** Allows you to send e-mail and surf without leaving a history.

Privacy Policies

A useful practice for companies is to disclose their privacy policies to their customers. For an example, see **arvest.com/pdfs/about/arvest_bank_privacy_notice.pdf.**

Privacy Issues in Web 2.0 Tools and Social Networks

The rise in social network use raises some special issues of privacy and free speech. Here are a few examples.

Presence, Location-Based Systems, and Privacy

Establishing real time connections in the social networking world is an important activity. For example, Facebook offers Nearby Friends, an app that enables users to know where their friends are.

IBM has presence capabilities in its Lotus Software Connections (now called IBM Connections; **ibm.com/software/products/en/conn**), while Microsoft offers similar capabilities with SharePoint (**office.microsoft.com/en-us/sharepoint**). Apple, Google, and other companies offer similar features. Several social networks enable people to share their location with others. What are the privacy implications of such capabilities if used by businesses to locate customers and goods? Who will be held responsible or legally liable for unforeseen harm resulting from so much awareness and connectivity?

Obviously, clear policies are needed to govern what social networks can do with all the data they collect about people.

Privacy Protection by Ethical Principles

Some ethical principles that exist for the collection and use of personal information also apply to information collected in e-commerce. Some of these principles were discussed in Sections 15.1 and 15.2. Examples are: proper notification about the possible use of personal data, option of opting-in and/or opting-out, accessibility to stored data, keeping consumers' data secured, and the ability to enforce related policies.

The broadest law in scope is the Communications Privacy and Consumer Empowerment Act (1997), which requires, among other things, that the FTC enforces online privacy rights in EC, including the collection and use of personal data. For the status of pending legislation in the United States, see **govtrack.us/congress/bills/subjects/right_of_privacy/5910**.

The USA Patriot Act Versus Privacy

The USA PATRIOT Act (abbreviation of 'Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism') was passed in October 2001, in the aftermath of the 9/11 terrorist attacks. Its intent is to give law enforcement agencies broader capabilities in their efforts to protect the public. However, the American Civil Liberties Union (ACLU), the Electronic Freedom Foundation (EFF), and other organizations have raised grave concerns, including (1) expanded surveillance with reduced checks and balances, (2) overbreadth with a lack of focus on terrorism, and (3) rules that would allow U.S. foreign intelligence agencies to spy on Americans more easily.

A report by the U.S. Department of Justice (DOJ) in March 2007 found that the FBI had misused the Act to obtain thousands of telephone, business, and financial records from Americans without prior judicial approval. The result was that Congress amended some parts of the Act to require judicial approval prior to the FBI accessing sensitive information.

For highlights of the USA Patriot Act, see the U.S. Department of Justice website (go to **justice.gov/archive/ll/highlights.htm**).

Government Spying on Its Citizens

At issue here is the proper balance between personal privacy and national security, whereby innovation and commerce is not stifled. The claim is that social networking sites have technology that has outpaced government law enforcement capabilities. The laws on the books do not cover new communication methods (i.e., texting and social networking). Opponents see this as nothing more than unbridled government eavesdropping (Nakashima 2010). For other aspects, see Mercola (2012). During 2013 and 2014, it was found that the U.S. government did spy on its citizens. In 2014, efforts were taken to minimize such government surveillance.

P3P Privacy Platform

The **Platform for Privacy Preferences Project (P3P)** is a protocol for privacy protection on the Web developed by the World Wide Web Consortium (W3C). According to W3C, an international standards organization for the Web, the "Platform for Privacy Preferences Project (P3P) enables websites to express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents" (per **w3.org/P3P**). The W3C also explains that P3P is useful because "P3P uses machine readable descriptions to describe the collection and use of data. Sites implementing such policies make their practices explicit and thus open them to public scrutiny." This exposure can increase users' trust and confidence in e-commerce sites and vendors. Figure 15.1 shows the process of P3P.

Privacy Protection in Countries Other than the United States

In 1998, the European Union passed a privacy directive (EU Data Protection Directive) reaffirming the principles of personal data protection in the Internet age. This directive protects privacy more than U.S. protection laws do.

In many countries, the debate about the rights of the individual versus the rights of society continues. In some countries, like China, there is little protection of an individual's Internet privacy.

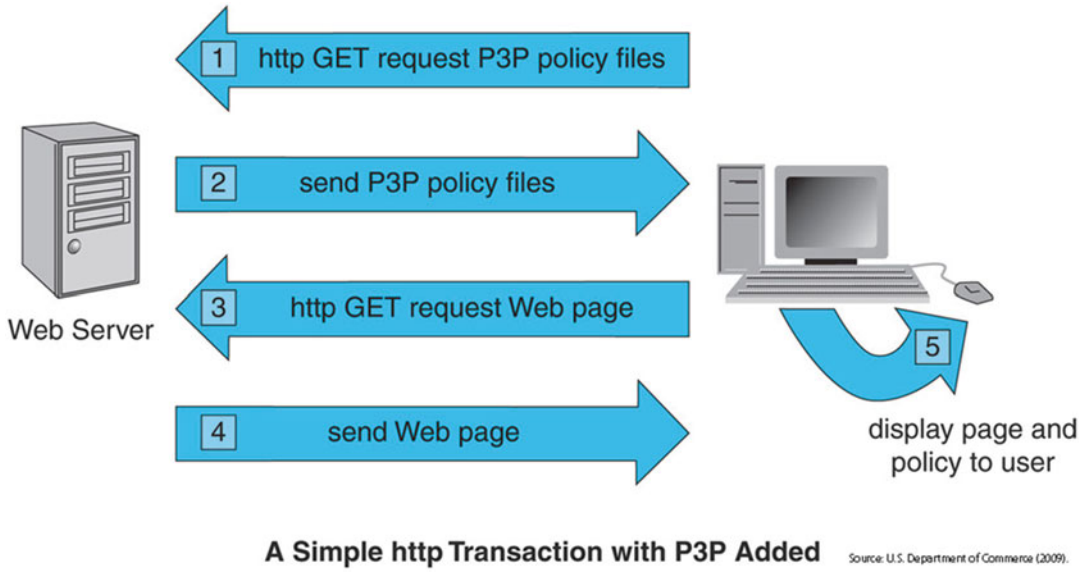

Figure 15.1 How P3P Works

SECTION 15.3 REVIEW QUESTIONS

1. Define privacy and free speech. Do your definitions depend on technology?
2. List some of the ways that the Internet can collect information about individuals.
3. What are cookies and spyware, and what do they have to do with online privacy?
4. Describe information pollution and privacy.
5. List four common ethical principles related to the gathering of personal information.
6. Describe privacy issues in social networks. What are the dangers?
7. Define P3P and describe its objectives and procedures.

15.4 OTHER EC LEGAL ISSUES

During the last 10 years, a large number of laws dealing with EC and the Internet have been enacted. Representative major issues are listed in Online File W15.3.

Note that we discussed some of these issues in previous sections. Note also that legal issues are country or even state-dependent. For comprehensive coverage of these, see Davidson (2009) and Mallor et al. (2009). You can find a comprehensive e-commerce law blog at **ecommercelaw.typepad.com.**

Selected Legal and Regulatory Environment: E-Discovery and Cyberbullying

The legal and regulatory environment related to EC is very broad (e.g., see Alghamdi 2011).

Here, we briefly describe two issues: e-discovery and cyberbullying.

E-Discovery

Electronic discovery (e-discovery) refers to the process of finding any type of electronic data (e.g., text, images, videos) by using computerized systems. A major application of e-discovery is its use of finding evidence in legal cases. For details, see **en.wikipedia.org/wiki/Electronic_discovery**.

E-discovery deals frequently with e-mail archives. E-mail is the prime target of e-discovery requests. E-discovery must have features such as full-content index, keyword search, and metadata index. For e-discovery tools for aiding compliance and saving money, see Kontzer (2012).

E-Discovery and Social Networks

Speaking of discovery, should families of the recently deceased get access to their loved one's social network(s) after they die? How do you manage privacy in the afterlife?

Several social networks have developed policies for such cases. For example, Facebook has developed several policies for the accounts of its users who have passed away. A useful tool is Deathswitch (**deathswitch.com**), an automated system that sends you password requests on a regular schedule to make sure you are still alive. Also see the password manager, PasswordBox.

Cyberbullying

According to **stopybullying.gov**, **cyberbullying** is "bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as cell phones, computers and tablets as well as communication tools including social media sites, text messages, chat, and websites." Examples of cyberbullying include mean text messages or e-mails, rumors sent by e-mail or posted on social networking sites, and embarrassing pictures, videos, websites, or fake profiles (per **stopbullying.gov/cyberbullying/what-is-it/index.html**). Bullying means "unwanted, aggressive behavior among school aged children that involves a real or perceived power imbalance." Examples of bullying are "actions such as making threats, spreading rumors, attacking someone physically or verbally, and excluding someone from a group on purpose" (per **stopbullying.gov/what-is-bullying/definition/index.html**). Unfortunately, adults can also be victims of bullying (see **bullyingstatistics.org/content/adult-bullying.html**).

The National Science foundation (**nsf.gov**) published a series titled "Bullying in the Age of Social Media," which describes how cyberbullying is done, its possible damage to people (some commit suicide), and how to manage it. For legislation and awareness campaigns see **cyberbullying.us** and **stopcyberbullying.org**.

A Sample of Other Issues

Here is a list of other EC legal issues:

- Legalizing Internet gambling (Parry 2013)
- Web monopoly by giant companies (Google, Tencent in China).
- Use of social media sites for prostitution
- Regulating online P2P money lenders.

Protection is needed not only for buying goods, but also from buying services. In Chapter 3, we describe online stock trading as an example.

SECTION 15.4 REVIEW QUESTIONS

1. List some of the issues that EC will face in the coming years that will affect your daily life.
2. Define e-discovery. How is it related to the law? To e-commerce?
3. Define cyberbullying. What damages can it cause?

15.5 CONSUMER AND SELLER PROTECTION FROM ONLINE FRAUD

The 2013 Internet Crime Report issued by the FBI Internet Crime Complaint Center (IC3) (**ic3.gov/media/annualreport/2013_IC3Report.pdf**) revealed that in 2013, the IC3 received 262,813 complaints, with a total adjusted dollar loss of about $781 million.

It is necessary to protect EC consumers, which the IC3 attempts to do, by informing the public about Internet scams by publishing public service announcements. Auction fraud is also developing into a major issue, and is one of the main sources of overall Internet fraud (see Gavish and Tucci 2008).

Consumer (Buyer) Protection

Consumer protection is critical to the success of any commerce, especially electronic, where transactions between buyers and sellers are not face-to-face. The Federal Trade Commission (FTC) enforces consumer protection laws in the United States (see **ftc.gov**). The FTC provides a list of common online scams (see **onguardonline.gov/articles/0002-common-online-scams**). In addition, the European Union and the United States are attempting to develop joint consumer protection policies. For details, see the Trans Atlantic Consumer Dialogue website at **tacd.org.**

Representative Tips and Sources for Your Protection

Protecting consumers is an important topic for government agencies, vendors, professional associations, and consumer protection organizations. These agencies provide many tips on how to protect consumers online. A representative list follows:

- Users should make sure that they enter the real website of well-known companies, such as Walmart, Disney, and Amazon.com, by going directly to the site, rather than through a link.
- Check any unfamiliar site for an address and telephone and fax numbers. Call and quiz a salesperson about the company and the products.
- Investigate sellers with the local chamber of commerce, Better Business Bureau (**bbb.org**), or TRUSTe (**truste.com**).
- Investigate how secure the seller's site is and how well it is organized.
- Examine the money-back guarantees, warranties, and service agreements before making a purchase.
- Compare prices online with those in regular stores – prices that are too low may be too good to be true.
- Ask friends what they know about the websites. Find testimonials and endorsements (be careful, some may be biased).
- Find out what remedy is available in case of a dispute.
- Consult the National Consumers League Fraud Center (**fraud.org**).
- Check the resources available at **consumerworld.org**.
- Amazon.com provides comprehensive protection. See **webstore.amazon.com/Fraud-Protection-Power/b/9437355011.**

In addition to these tips, consumers and shoppers also have rights on the Internet, as described in the following list of sources:

- The Federal Trade Commission (**ftc.gov**): Protecting America's Consumers. Abusive e-mail should be forwarded to spam@uce.go. For tips and advice see **ftc.gov/tips-advice**.
- National Consumers League Fraud Center (**fraud.org**).
- Federal Citizen Information Center (**gsa.gov/portal/category/101011**).
- U.S. Department of Justice (**justice.gov**).
- Internet Crime Complaint Center (**ic3.gov/default.aspx**).
- The American Bar Association provides online shopping tips at **safeshopping.org.**
- The Better Business Bureau (**bbb.org**).
- The U.S. Food and Drug Administration provides information on buying medicine and medical products online (**www.fda.gov/forconsumers/protectyourself/default.htm**).
- The Direct Marketing Association (**thedma.org**).
- Privacy Rights Clearinghouse (**privacyrights.org**): Provides information on different types of privacy, including online privacy and technology, identity theft, and junk mail.

Disclaimer: This is general information on consumer rights. It is not legal advice on how any particular individual should proceed. If you require specific legal advice, consult an attorney.

Third-Party Assurance Services

Several public organizations and private companies also attempt to protect consumers. The following are just a few examples.

Protection by a Third-Party Intermediary

Intermediaries who manage electronic markets try to protect buyers and sellers. A good example is eBay, which provides an extensive protection program (see eBay Money Back Guarantee (**pages.ebay.com/coverage/index.html**) and a Dispute Resolution Center).

TRUSTe's "Trustmark."

TRUSTe (**truste.com**) is a for-profit company whose mission is to ensure that "businesses adhere to best practices regarding the collection

and use of personal information on their website" (see **truste.com/about-TRUSTe**). Exhibiting the TRUSTe Advertising Affiliate "Trustmark" (a seal of quality) facilitates consumer confidence in business conducted online. The TRUSTe seal identifies sites that have agreed to comply with responsible information-gathering guidelines. In addition, the TRUSTe website provides its members with a "privacy policy wizard," which helps companies create their own privacy policies. The site offers several types of seals for different purposes such as for privacy, children, e-health, wireless, e-mail services, and international services.

The TRUSTe program is voluntary. The licensing fee for use of the Trustmark is paid by sellers, depending on the size of the online business. Many websites are certified as TRUSTe participants, including AT&T, IBM, The Walt Disney Company, AOL, Infoseek, the *New York Times,* and eBay. However, some merchants fear that signing with TRUSTe could expose them to litigation from third parties if they fail to comply exactly with TRUSTe rules, and that fear is likely to deter some companies from joining the program.

Better Business Bureau

The Better Business Bureau (BBB), a private nonprofit organization supported largely by membership, collects and provides reports on businesses that consumers can review before making a purchase. The BBB responds to millions of inquiries each year. The BBB also handles customer disputes against businesses. Its BBBOnLine program (**bbb.org/online/customer/default.aspx**) is similar to TRUSTe's Trustmark. The goal of the program is to promote confidence on the Internet through two different seals. Companies that meet the BBBOnLine standards for the Reliability Seal are members of the local BBB and have good truth-in-advertising and consumer service practices. Those that exhibit the BBBOnLine Privacy Seal on their websites have an online privacy protection policy and standards for handling consumers' personal information. In addition, consumers are able to click on the BBBOnLine seals and instantly get a BBB report on the participating company.

Which?

Supported by the European Union, Which? (**which.co.uk**) gives consumers protection by ensuring that online traders under its Which? Web Trader scheme abide by a code of proactive guidelines. These guidelines outline issues such as product information, advertising, ordering methods, prices, delivery of goods, consumer privacy, receipting, dispute resolution, and security.

WebTrust Seal

The WebTrust seal program is similar to TRUSTe. The American Institute of Certified Public Accountants (**cpawebtrust.com**) sponsors it.

Evaluation by Consumers

A large number of sites include product and vendor evaluations offered by consumers. For example, on Yelp!, community members rate and comment on businesses.

The Computer Fraud and Abuse Act (CFAA)

The **Computer Fraud and Abuse Act (CFAA)**, passed in 1984 and amended several times, is an important milestone in EC legislation. Initially, the scope and intent of CFAA was to protect government computers and financial industry computers from criminal theft by outsiders. In 1986, the CFAA was amended to include stiffer penalties for violations, but it still only protected computers used by the federal government or financial institutions. As the Internet expanded in scope, so did the CFAA. In 1994 and 1996, there were significant revisions of the CFAA that added a civil law component and civil charges to this law that had previously applied to criminal offenses only. In 2001, it was modified by the USA PATRIOT Act, adding sections relating to cyberterrorism and adding crimes that are considered to be "Federal Acts of Terror." In 2008, the CFAA was amended again by the Identity Theft Enforcement and Restitution Act to address the malicious use of spyware to steal sensitive personal information, eliminating the financial loss requirement, and creating harsher penalties for those who intentionally access or conspire to access, computers

without authorization. See the manual titled "Prosecuting Computer Crimes" at **justice.gov/criminal/cybercrime/docs/ccmanual.pdf**.

Seller Protection

The Internet makes it easier for buyers and sellers engaging in EC to commit fraud. Sellers must be protected against:

- Customers who deny that they placed an order.
- Customers who download copyrighted software and sell it to others.
- Customers who give fraudulent payment information (false credit card or a bad check) for products and services that they buy.
- Imposters – sellers using the name of another seller (see the CyberSource Annual Reports).
- Other sellers using the original seller's names, trademarks, and other unique features, and even their Web addresses (or similar to it).
- Payment fraud by consumers and by criminals.

Sellers also can be attacked illegally or unethically by competitors.

Example

A class action lawsuit was filed against McAfee in the United States District Court for the Northern District of California (Case No. 10-1455-HRL) alleging that after the plaintiffs purchased McAfee software from McAfee's website, a deceptive pop-up ad (from one of McAfee's partners) that looks like a McAfee page appeared, and thanked the plaintiffs for their software purchase. The pop-up ad asked them to click on a "Try it Now" button, which they assumed would download the software they had just purchased, but unbeknownst to them, they received a 30-day trial subscription to Arpu, Inc. (a non-McAfee product). They found out later that McAfee transmits customer credit/debit card and billing information to Arpu (customers are charged $4.95 per month after the trial period) and collects an undisclosed fee for each customer who "tries" Arpu via the McAfee website (ClassActionLawsuitsInTheNews.com 2010). See also **courthousenews.com/2010/04/08/McAfee.pdf**.

What Can Sellers Do?

Companies like Chargeback Stopper (**chargebackstopper.com**) and Chargeback Protection (**chargebackprotection.org**) provide merchants with a database of credit card numbers that have had 'chargeback orders' recorded against them. Sellers who have access to the database can use this information to decide whether to proceed with a sale. In the future, the credit card industry is planning to use biometrics to manage electronic shoplifting. In addition, sellers can use PKI and digital certificates, especially the SET protocol, to help prevent fraud (see Chapter 11).

Other possible solutions include the following:

- Use intelligent software to identify questionable customers (or in small companies, do this identification manually). One technique, for example, involves comparing credit card billing and requested shipping addresses.
- Identify warning signals – i.e., red flags – for possible fraudulent transactions.
- Ask customers whose billing address is different from the shipping address to call their bank and have the alternate address added to their bank account. Retailers will agree to ship the goods to the alternate address only if this is done.
- Ask the customer to disclose the credit card verification code.
- Delay shipment until money is received.

For further discussion of what merchants can do to protect themselves from fraud, see Litle & Co. (2014) and CyberSource (2012). For 10 measures to reduce credit card fraud for Internet Merchants (a FraudLabs.com White Paper), see **fraudlabs.com/docs/fraudlabs_white_paper.pdf**.

Protecting Both Buyers and Sellers: Using Electronic Signatures and Other Security Features

One method to help distinguish between legitimate and fraudulent transactions is electronic signatures.

An **electronic signature** is "the electronic equivalent of a handwritten signature" (per **pcmag.com/encyclopedia/term/42500/electronic-signature**; see Chapter 10). Electronic signatures provide high level of security and are recognized by most legal entities as being equivalent to handwritten signatures. All electronic signatures are represented digitally. Signed electronic documents and contracts are as legally binding as paper-based documents and contracts. For details, see **en.wikipedia.org/wiki/Electronic_signature**. See also **e-signature.com**.

Authentication

In the online environment where consumers and merchants do not have physical contact with one another, proving the authenticity of each person is necessary since buyers and sellers do not see each other. However, if one can be sure of the identity of the person on the other end of the line, there could be more e-commerce applications. For example, students would be able to take exams online from anywhere without the need for proctors. Fraud among recipients of government payments would be minimized. Buyers would be assured who the sellers are, and sellers would know, with a very high degree of confidence, who the buyers really are. Online job interviews would be accurate because it would be almost impossible for an applicant to impersonate another person. Overall, trust in online transactions and in EC in general would increase significantly. Authentication can be achieved in several ways, including the use of biometrics (see Chapter 10).

Fraud Detecting Systems

There are a large number of fraud detection systems such as the use of data mining for credit card fraud. For other methods, see Parks (2010). CyberSource also has developed several tools for detecting fraud. For details, see Cyber Source (2012) and **authorize.net/resources/files/fdswhitepaper.pdf**.

SECTION 15.5 REVIEW QUESTIONS

1. Describe consumer protection measures.
2. Describe assurance services.
3. What must a seller do to protect itself against fraud? How?
4. Describe types of electronic signatures. Who is protected? Why?
5. Describe authentication.

15.6 PUBLIC POLICY, TAXATION, AND POLITICAL ENVIRONMENTS

In this chapter, we include four topics of public policy that are closely related to e-commerce.

Net Neutrality

Internet neutrality (also *network neutrality, net neutrality,* or *NN*) has been a hotly debated topic that may shape the future of the Internet (see **businessinsider.com/net-neutralityfor-dummies-and-how-it-effects-you-2014-1**). It became a high-profile topic when telecommunications network operators AT&T and Verizon announced that they wanted to charge an extra fee to deliver content on the Internet at a faster rate of speed. Currently, all Internet traffic is being treated equally (or "neutrally") by telecommunication providers. In response, numerous groups have tried to stop the extra fee. The problem here is that 5–10% of the users occupy 80–90% of the available bandwidth, partially because of the heavy peer-to-peer (P2P) traffic.

On December 21, 2010, the Federal Communications Commission (FCC) approved net neutrality. **Net neutrality** is a network design principle stating that basic protocols of the Internet should enable users to utilize the Web without being discriminated against by Internet service providers. In other words, there should be net equality. Net providers cannot dictate the types of content you see, they must treat all Internet traffic sources

equally, and consumers can access anything they want at no extra charge (see **businessinsider.com/net-neutralityfor-dummies-and-how-it-effects-you-2014-1**). Net neutrality puts in place three high-level rules for service providers (see Woyke 2010 for details). For more on net neutrality and its impact, see Gross (2014). Note that implementation of net neutrality is not simple; it involves Web companies, lawmakers and government agencies, fiber-optics owners, content providers, mobile carriers, and consumers. Opponents are fighting the authority of the FCC to enforce net neutrality by circulating and signing petitions, protesting, and so forth. For how net neutrality, or lack thereof, can affect a business, see **entrepreneur.com/article/233991**. For a discussion on the net neutrality debate, and an infographic, see **wired.com/2014/06/net_neutrality_missing**. In January 2014, a federal appeals court struck down the FCC's net neutrality rule.

In April 2014, the FCC announced new rules that may abolish net neutrality (see Mayton 2014). However, in May 2014, the FCC generated a new *proposal* that is intended to uphold net neutrality. The FCC's proposal includes keeping the Internet open and holding Internet providers to higher levels of transparency. Also in question is how the FCC plans to regulate ISPs. The FCC plans on adopting a new set of rules by the end of 2014 (see Anthony 2014). Well, it sure keeps changing!

Taxation of EC Transactions

Several types of taxes are related to e-commerce. The most debatable one is the Internet sales tax, which is imposed by individual states on products sold in their jurisdictions. See **en.wikipedia.org/wiki/Internet_taxes**.

When Internet commerce started in the mid-1990s, it was declared free of taxation in the United States at the federal, state, county, and city levels in order to encourage e-commerce. However, not imposing taxes on the Internet was seen as discriminatory against mail-order businesses and traditional retailers who must collect taxes. Over the years, there were several court challenges and modifications. You can read about the history at **taxbrain.com**. One development was the 1998 Internet Tax Freedom Act that placed a moratorium on special taxation on the Internet for one year. This meant that Internet access could not be taxed by state and local governments. The Act has been renewed by Congress periodically, with a few changes (see **money.howstuffworks.com/personal-finance/personal-income-taxes/internet-tax-freedom-act1.htm**). A bill to permanently extend the Internet Tax Freedom Act was introduced in 2013, and was passed by the House Committee on the Judiciary in June 2014. To read about the bill and track its progress, see **govtrack.us/congress/bills/113/hr3086#overview**.

Therefore, the states' budget and taxing authorities have placed the issue of collecting Internet taxes high on their agendas as a potential means of generating state revenues. Some states are suing online vendors for not collecting sales taxes. It appears that there is a consensus forming among state lawmakers that Internet taxes are inevitable. Obviously, there is consumer resistance.

A major player in the conflict between consumers that are used to not paying taxes and states that need money is Amazon.com. In 2011, California passed a tax collection bill for the Internet, and started to pressure Amazon into collecting the sales tax. In 2012, Amazon agreed to collect sales tax from its buyers in California as well as in some other states.

In 2013, the U.S. Senate passed the Marketplace Fairness Act (**marketplacefairness.org**), a law that will require all online and catalog sellers in the U.S. to collect sales tax at the time of an online transaction. However, states must simplify their sales tax laws. The bill was sent to the House Subcommittee and as of June 2014, is still being reviewed.

In addition to sales tax, there are several other taxes related to e-commerce.

For example, in July 2010, in a move to legalize Internet gambling, the United States House Committee on Financial Services approved a bill that lays the groundwork for a multibillion-dollar online gambling tax.

Internet Censorship by Countries

Internet censorship refers to restrictions on what can be seen, published, or accessed on the Internet. Internet restrictions can be imposed domestically (e.g., big businesses and corporations restricting employee Internet access), and in foreign countries. Censorship is done using different methods, ranging from blocking access to certain websites to the creation of a whole alternative Internet, as was done in Iran. A popular method of censorship is content filtering. Filtering can be based on a blacklist of offensive website content providers, or by other methods. When blacklisted, a website will have all or part of its content censored by a government agency that sees the website's content as offensive to citizens or to the government. For comprehensive information on the different types of Internet censorship in the U.S. and other countries, see **computer.howstuffworks.com/internet-censorship.htm**. In 2010, Google decided not to do business in China because the Chinese government had asked Google to block certain websites and information in Google searches. Google refused and withdrew from China.

In early 2009, President Obama appointed Cass Sunstein as the White House's "Regulatory Czar." Sunstein is an advocate for Internet censorship, having written several white papers promoting the idea (see *WorldNetDaily* 2009). For examples and an infographic of censorship in countries around the world, see **safervpn.com/blog/mapping-internet-censorship-worldwide-infographic**.

SECTION 15.6 REVIEW QUESTIONS

1. What is net neutrality and how will it affect the Internet?
2. Why is net neutrality such a hotly debated issue? Find the legal status of this issue.
3. Describe how taxes relate to e-commerce.
4. What is Internet censorship?

15.7 SOCIETAL ISSUES AND GREEN EC

At this point in the chapter, our attention turns to several societal issues of EC. The first societal topic is one that concerns many – the *digital divide*.

The Digital Divide

Despite the factors and trends that contribute to future EC growth, since the inception of the Internet, and e-commerce in particular, a gap has emerged between those who have and those who do not have the ability to engage in e-commerce. This gap is referred to, in its generic format, as the **digital divide**. According to Internet World Stats, the digital divide "is a social issue referring to the differing amount of information between those who have access to the Internet (especially broadband access) and those who do not have access" (see **internetworldstats.com/links10.htm**). The gap exists both *within* and *between* countries. The U.S. federal and state governments are attempting to close this gap within the U.S. by encouraging training and supporting education and infrastructure. The gap between countries, however, may be widening rather than narrowing. For an overview and statistics, see **en.wikipedia.org/wiki/Digital_divide**. Many government and international organizations, including the United Nations and Citizens Online, are exploring this issue.

Overcoming the Digital Divide

Governments, companies, and nonprofit organizations are trying to reduce the digital divide. One example is the "One Laptop per Child" project (**one.laptop.org**), a non-profit organization whose mission is to provide children in low-income communities and developing nations with low-cost "XO" brand laptops.

For a short video, see **laptop.org/en/video/brand/index.html**. The current cost of each laptop (2014) is around $35. For more information about the program and the capabilities of the laptops, see **one.laptop.org/about/faq**.

In Online File W11.2, we provided an example of how underprivileged farmers in India use smartphones to make payments on bank loans and to receive farm-related information.

Telecommuting

One activity of e-commerce is **telecommuting**, which is working at home using a PC, tablet, smartphone, and the Internet. Telecommuting is on the rise in the United States and in several

Table 15.4 Potential benefits of telecommuting or virtual work

Individuals	Organizational	Community and society
Reduces or eliminates travel-related time and expenses	Reduces office space needed	Conserves energy and lessens dependence on foreign oil
Improves health by reducing stress related to compromises made between family and work	Increases labor pool and competitive advantage in recruitment	Preserves the environment by reducing traffic-related pollution and congestion
Allows closer proximity to and involvement with family	Provides compliance with the Americans with Disabilities Act	Reduces traffic accidents and resulting injuries or deaths
Allows closer bonds with the family and the community	Decreases employee turnover, absenteeism, and use of sick leave	Reduces the incidence of disrupted families; telecommuters may be able to keep their job and work from home if a family member needs to relocate for business reasons, etc.
Decreases involvement in office politics	Improves job satisfaction and productivity	Increases employment opportunities for the homebound
Increases productivity despite distractions		Allows the transfer of jobs to areas of high unemployment

developing countries. For a list of potential benefits, see Table 15.4. For example, one benefit of working from home is that people who live in the suburbs can save one to two hours of time per day by not having to commute to work (Enviro Boys 2010).

Example

Ascend One Corporation, a consumer debt management business, decided to change their networking strategies in order to expand. Ascend One's success was substantially burdened by having to provide its call center agents with daily cumbersome support and application updates on their desktop computers. The company increased productivity and satisfaction of customer care employees by combining telecommuting with virtualization technology. The company stored and managed applications on virtual desktops instead of on remote computers. Call center agent productivity increased by 10%. By allowing telecommuting, there was an increase in employee productivity and a reduction in attrition rates. The technology also allowed the company to maintain high levels of communication with mobile employees. Training programs are accessible 24 hours per day to remote workers (see Park 2009 for details).

Note: Some companies do not like their employees to work from home. In 2013, Yahoo's CEO banned the work-from-home policy. For a debate on this policy, see Bercovici (2013) and Ascharya (2013). Although the ban on telecommuting is still enforced, the CEO extended Yahoo's parental leave policy.

Green EC and IT

There are many opportunities to go EC green, and here we are representative ones.

Operating Greener Businesses, Eco-Friendly Data Centers, and Cloud Computing

The growing power consumption of computing technology and high energy costs are having a direct negative impact on business profitability. Enterprises are trying to reduce energy costs and increase the use of recyclable materials. **Green computing** refers to the eco-friendly use of computing resources (e.g., see **searchdatacenter.techtarget.com/definition/green-computing**). In this section, we focus on how EC is *going green* by adopting environmentally friendly practices.

For example, energy use in data centers is a major concern to corporations. Green EC/IT is a growing movement (see Nelson 2008) that also includes data centers. According to Gartner Inc., Green IT initiatives are expanding to many other areas (see **enterpriseinnovation.net/article/gartner-green-data-center-means-more-energy-efficiency**). For guidelines on how to go green, see Table 15.5.

Table 15.5 Turning IT green: guidelines for energy-efficient computer use

Use the computer's power management options, such as setting all computers to hibernate and using the standby option
Instruct all personnel to turn off computer monitors when not in use
Shut down all computers automatically after hours or when not in use
Encourage telecommuting whenever possible
Follow the manufacturers' recommendations on all energy-related equipment
Embrace cloud computing. Replace existing servers with virtualization, as money permits
Increase cooling efficiency

For practices, see "Cooling Data Center Costs" in *Baseline*, August 13, 2010 (available online at **baselinemag.com/infrastructure/Cooling-Data-Center-Costs** (accessed June 2014).

The efforts to improve the use of EC (and IT) by minimizing damage to the environment, and at the same time saving money, are major objectives of **Green IT**. Company data center servers are also known to be both power hungry and heat generating. PC monitors consume about 80 to 100 billion kilowatt hours of electricity every year in the United States. Both Intel and AMD are producing new chips aimed at reducing this amount of energy usage. Turning off PCs when they are not in use can save a company money and add to good corporate social health by reducing the damage caused by excessive carbon dioxide release. Finally, discarded PCs and other computer equipment can cause serious waste disposal problems. An important issue is how to recycle old computing equipment and whose responsibility it is to take care of the problem (the manufacturers? the users? the government?). *Green software* assists companies save energy and/or comply with EPA requirements.

A comprehensive coverage of Green IT is provided by Murugesan and Gangadharan (2012), who distinguish between making EC (and IT) greener and using IT and EC as enabling tool to improve environmental sustainability (i.e., make it greener). They also cover implementation and strategy issues. For a guide to green IT strategy, see IBM (2008b).

How to Operate Greener Businesses, Data Centers, and Supply Chains

Chief information officers (CIOs) who are looking to operate greener businesses, data centers, and supply chains should focus on: (1) virtualization, (2) software management, and (3) harnessing the "cloud." *Virtualization* provides energy saving solutions, resulting in both energy and monetary savings. Companies seeking advice, tools, and processes can turn to software management outsourcing to help them achieve their software needs and licensing management needs. Finally, cloud computing is predicted to be included in 45% of all IT applications by 2017.

Gaining energy efficiency in business requires managing these issues: the computers, computing power of the data center, data center power/cooling, and data center storage. Many organizations are turning to server virtualization, such as cloud computing, to cut their energy costs. For more details on green computing, see Online File W15.4.

Example 1

Wells Fargo (**wellsfargo.com**) is a large financial institution that offers a wide range of banking services online. The company is data-dependent and known for its eco-friendliness. The company decided to "go green" in its two data centers. Data centers must ensure security and availability of their services, and when they are planned from scratch, they can be energy efficient with low power consumption. The two new facilities had more than 8,000 servers. After major virtualization efforts, the data centers were using significantly less power compared to the previous year.

Wells Fargo introduced several energy saving devices (see Clancy 2010). Wells Fargo constantly expands and renovates its data centers, yet shows high consideration to the environment. Wells Fargo is also eco-friendly in other ways. (For more about "green banking" at Wells Fargo, see **bankrate.com/financing/banking/green-banking-at-wells-fargo**.)

Example 2

Google aimed to reduce the power consumption of its data centers by 30%. This was done by reducing overhead costs: improving the cooling system, lighting, and the power infrastructure. Google closely followed the strategies and recommendations of the company's "Green Energy Czar." Google, whenever possible, embraces free cooling – such as cooling towers and use of fresh air. Google also purchases clean energy from several sources. For details, see Samson (2010).

Global Green Regulations

Global regulations also are influencing green business practices. Sustainability regulations such as the Restriction of Hazardous Substances Directive (RoHS) in the European Union (EU) will increasingly impact how supply chains function regardless of location (see **ec.europa.eu/environment/waste/rohs_eee** and **rohs.gov.uk**).

Eco-friendly practices reduce costs and improve public relations in the long run. Not surprisingly, demand for green computing is on the rise. A tool to help companies find greener computers and other electronics is the Electronic Product Environmental Assessment Tool (EPEAT).

The Electronic Product Environmental Assessment Tool

Maintained by the Green Electronics Council (GEC), the **Electronic Product Environmental Assessment Tool (EPEAT)**, according to their website, rate electronic products against a range of environmental performance criteria. They are a comprehensive global rating system for greener electronics. For more on e-commerce for a better environment, see **rainforestagencies.com.au/egreen.html**.

Telecommuting, which was discussed earlier, also offers several green benefits, including reducing rush-hour traffic, improving air quality, improving highway safety, and even improving health care by reducing pollution.

Other Societal Issues

Many other societal issues can be related to EC. Three in which EC has had a generally positive impact are mentioned here: education, public safety, and health.

Education

E-commerce has had a major impact on education and learning. Virtual universities are helping to reduce the digital divide. Companies can use the Internet to help retrain employees, enabling them to defer retirement.

Public Safety, Surveillance, and Homeland Security

With increased concerns about public safety after September 11, 2001, many organizations and individuals have started to look at technologies that will help deter, prevent, or detect criminal activities of various types. Various e-commerce tools can help increase both safety at home and in public places. These include e-911 systems; global collaborative commerce technologies (for collaboration among national and international law enforcement units); e-procurement (of unique equipment to fight crime); e-government efforts at coordinating, information sharing, and expediting legal work and cases; intelligent homes, offices, and public buildings; and e-training of law enforcement officers.

An issue to consider is whether the financial, functional, and social impact of surveillance systems is worth the public's perceived intrusion of privacy. The fact remains that most cities that use the surveillance cameras do so more for the retrieval of images rather than for active monitoring. Thus, as a crime deterrent, these cameras make little financial sense since only one person can effectively monitor 10 cameras at one time. The City of Chicago, for example, has installed more than 10,000 cameras. For real time monitoring, the city would need to hire an additional 1,000 city employees, which is impossible with budget shortages and lower tax revenues (per Gallio 2010). Machine interpretation of videos, which is getting more and more accurate, will make surveillance a more cost-effective tool in the future. However, Chicago is adding more surveillance cameras. As of 2014, Chicago has 24,000 cameras, which is raising privacy concerns with citizens and the ACLU (see **foxnews.com/politics/2014/05/12/security-camera-surge-in-chicago-sparks-concerns-massive-surveillance-system**).

Health Aspects

Is EC a health risk? Generally speaking, it is probably safer and healthier to shop from home than in a physical store. However, some believe that exposure to cellular mobile communication radiation may cause health problems. It may take years before the truth of this claim is known. Even if communication's radiation may cause health problems, the damage would probably be insignificant due to the small amount of time most people spend on wireless shopping and other m-commerce activities. However, given the concern of some about this issue, protective devices are now available that would minimize this problem (e.g., see **safecell.net**).

Another health-related issue is the addiction to online games, social networks, and EC/Internet-related applications. Several countries (including the U.S.) have begun prevention and re-education programs and some have opened inpatient treatment and recovery centers (e.g., see Geranios 2009 and **netaddiction.com**).

EC technologies such as collaborative commerce can help improve health care. For example, using Web technologies during the review process and the approval process of new drugs has been shortened, saving lives and reducing suffering. Wireless computing helps in the delivery of health care (see Chapter 6). Intelligent systems facilitate medical diagnoses. Health care advice can be provided from a distance. Finally, intelligent hospitals, doctors, and other health care facilities use EC tools. In 2009, the major social networks and Twitter were tracking the outbreak of the Swine Flu Pandemic, advising people where not to travel and how to protect themselves. Finally, in Israel and Europe, an ongoing major multinational, collaborative research project called "MOBIGuide" combines monitoring patients from a distance and generating medical decisions according to the data collected. For details, see **newmedia-eng.haifa.ac.il/?p=5593**.

Make Cities More Livable

In Chapter 6, we described smart cities. The objective is to make cities more livable. Chia (2012) discusses research on how to make cities like Singapore more intelligent. Gaylord (2013) describes the use of big data and government transparency in big cities.

SECTION 15.7 REVIEW QUESTIONS

1. Define the digital divide.
2. Describe the One Laptop per Child project.
3. Describe how EC can improve safety and security.
4. Describe the impact of EC on health services.
5. What is green computing?
6. List three examples in which green computing can help protect the environment or conserve resources.
7. What is a green supply chain? Give one example.
8. How do the new data centers help us "go green"?
9. How does telecommuting or virtual work conserve the environment?

15.8 THE FUTURE OF E-COMMERCE

Generally speaking, the consensus is that the future of EC is positive. EC will become an increasingly important method of trading, reaching customers, providing services, and improving organizations' operations. In addition, EC facilitates collaboration, innovation, and people-to-people interactions. Analysts differ in their predictions for the anticipated growth rate of EC and the length of time it will become a substantial portion of the economy. There is also disagreement about the identification of industry segments that will grow the fastest. However, there also is a consensus about the direction of the field: full speed ahead! Companies such as Amazon.com, eBay, Alibaba Group, Priceline, and Newegg.com are growing rapidly.

The Enterprise Innovation Editors (2013) made predictions regarding EC for 2014 and beyond. These include many topics cited in this book, ranging from mobility to medical information systems and security. Gerber (2013) made 10 predictions about the future of EC, ranging from comprehensive customer-engagement to custom design.

Integrating the Marketplace with the Marketspace

Throughout this book, we have commented on the relationship between the physical marketplace and the online marketspace. We have pointed out conflicts in certain areas, as well as successful applications. The fact is that, from the point of view of the consumer, as well as of most of the merchants and suppliers, these two entities exist, and will continue to exist, together.

Probably the most noticeable integration of the two concepts is in the click-and-mortar organization. In the near future, the click-and-mortar organization will be the most prevalent model (e.g., see Sears.com, Target.com, Costco.com, and Walmart.com), although the model may take different forms. Some organizations will use EC as just another sales channel, as most large retailers, airlines, and banks are doing today. Others will use EC only for some products and services, and sell other products and services the conventional way (e.g., LEGO Group).

M-Commerce

There is almost a 100% consensus that the role of m-commerce in e-commerce will increase significantly. There already are millions of innovative mobile apps and their numbers are growing rapidly. The area where we will see the fastest growth in EC is the proliferation of apps. Many m-commerce start-ups are entering the field.

Social Commerce

Recently, the use of mobile social networks has been accelerating. The increasing number of new wireless Web 2.0 services have assisted many social networks to go wireless, enabling more interactions between people. Nielsen's September 2012 release of its *Social Media Report* indicated four out of five active Internet users visit social networks and blogs. The report also shows that nearly 82% of social media users access these websites using their mobile phones (Nielsen 2012). These numbers continue to grow.

Social commerce is growing rapidly on Facebook, Twitter, Google, and many other companies. Mobile advertising and promotions are major areas of growth.

Future Technological Trends that May Accelerate the Speed of E-Commerce

The following are a few examples that will facilitate the use of e-commerce:

- Much wider broadband of technologies and faster networks
- More powerful search engines (intelligent agent-based)
- Better batteries for mobile devices
- Development in quantum computing and the semantic Web
- The arrival of flexible computer screens
- Better cloud applications
- Wide use of smartphones and tablets
- Increased use of wearable devices
- Possibility of free Internet access

Future Trends That Are Limiting the Spread of EC

The following trends may slow down the growth of EC and Web 2.0, and may even cripple the Internet:

- **Security concerns.** Both shoppers and users of e-banking and other services worry about online security. The Web needs to be made safer.
- **Lack of net neutrality.** If the big telecom companies are allowed to charge more for faster access, small companies that cannot pay extra may be at a disadvantage.

- **Copyright violations.** The legal problems of YouTube, Wikipedia, and others may result in a loss of vital outlets of public opinion and creativity.
- **Lack of standards.** There is still a lack of standards for EC, especially for global trade.

In conclusion, many people believe that the impact of EC on our lives will be as much as, and possibly more profound than, that of the Industrial Revolution. No other phenomenon since the Industrial Revolution has been classified in this category. It is our hope that this book will help you move successfully into this exciting and challenging area of the digital revolution.

Enjoy Some Interesting Videos About the Future of E-Commerce

The following are some suggested videos about e-commerce:

1. "E-Commerce's Future Ain't What It Used to Be; It's Even Better" (7:48 minutes) at **youtube.com/watch?v=mJtw1027FYs**
2. "Future of E-Commerce: Trends, Challenges, and Opportunities for Telecom and the Mobile Industry" (7:41 minutes) at **youtube.com/watch?v=wCZXif3MUEw**

SECTION 15.8 REVIEW QUESTIONS

1. How is EC related to traditional commerce?
2. Describe the role of mobility in the future of EC.
3. How will social networks facilitate EC?
4. Which future trends will help EC?
5. Which trends slow down the growth of EC?

MANAGERIAL ISSUES

Some managerial issues related to this chapter are as follows:

1. **What legal and ethical issues are of concern in an EC initiative?** Key issues to consider include the following: (1) What type of proprietary information should we allow and disallow on our site? (2) Who will have access to information that visitors post on our site? (3) Do the content and activities on our site comply with laws in other countries? (4) What disclaimers do we need to post on our website? (5) Are we using trademarked or copyrighted materials without permission? Regardless of the specific issues, an attorney should periodically review the website content, and someone should be responsible for monitoring legal and liability issues.
2. **What are the most critical ethical issues?** Negative or defamatory articles published online about people, companies, or products on websites or blogs can lead to charges of libel – and libel can stretch across countries. Issues of privacy, ethics, and legal exposure may seem tangential to running a business, but ignoring them puts the company at risk of fines, customer dissatisfaction, and disruption of an organization's operations. Privacy protection is a necessary investment.
3. **How can intellectual property rights be protected when it comes to digital content?** To protect intellectual property rights such as video, music, and books online, we need to monitor what copyrights, trademarks, and patents are infringed upon over the Internet. Portal sites that allow pirated video and music files should be monitored. This monitoring may require a vast amount of work, so software agents should be employed to continually inspect any pirated material. The risk to the business that can be caused by the infringement and the possibility of legal protection as well as technical protection by current regulation and potential new common law should be analyzed. Consider settling any suit for damages by negotiation.
4. **How can a patent in EC be purchased?** Some people claim that patents should not be awarded to businesses or computer processes related to EC (as is the case in some European countries). Therefore, investing large amounts of money in developing or buying EC patents may be financially unwise in cases where patents may not be granted or protected properly. Some companies that own many business

model patents have been unable to create business value out of these patents.

5. **What is the ethical principle of protecting the privacy of customers?** To provide personalized services, companies need to collect and manage customers' profile data. In practice, the company has to decide whether to use spyware to collect data. Collecting data may make customers unhappy (as in the cases of Google Street View or Facebook privacy settings). The company needs well-established principles of protecting customer privacy: Notify customers before collecting their personal information; inform and get consent on the type and extent of disclosures; allow customers to access their personal data and make sure the data are accurate and securely managed; and apply some method of enforcement and remedy to deter privacy breaches. In this manner, the company can avoid litigation and gain the long-term trust of customers.
6. **How can a company create opportunities in the global trend toward green EC?** Reducing carbon emissions and saving energy are global issues. (1) EC can save carbon emissions by reducing the need for transportation. This is a generic contribution of EC. (2) EC can provide an electronic exchange platform for trading CO_2 emission rights. This is a new business opportunity. (3) The IT hardware manufacturers may try to earn the Energy Star Excellence Award from the Environmental Protection Agency to prove that their products are contributing to the protection of the environment.

SUMMARY

In this chapter, you learned about the following EC issues as they relate to the chapter's learning objectives.

1. **Understanding legal and ethical challenges and how to contain them.** The global scope and universal accessibility of the Internet create serious questions as to which ethical rules and laws apply. Ignoring laws exposes companies to lawsuits or criminal charges that are disruptive, expensive, and damaging to customer relations. The best strategy is to avoid behaviors that would expose the company to these types of risks. Important safeguards are a corporate code of ethics stating the rules and expected behaviors and actions and an Internet acceptable use policy.
2. **Intellectual property law.** EC operations are subject to various types of intellectual property (IP) laws, some of which judges have created in landmark court cases. IP law provides companies with methods of compensation for damages or misuse of their property rights. IP laws passed by Congress are being amended to better protect EC. These protections are needed because the theft or replication of intellectual works on the Internet is both simple and inexpensive. These actions violate or infringe upon copyrights, trademarks, and patents. Although the legal aspects seem clear, monitoring and catching violators remains difficult.
3. **Privacy, free speech, defamation, and their challenges.** B2C companies use CRM and depend on customer information to improve products and services. Registration and cookies are two ways to collect this information. The key privacy issues are who controls personal information and how private it should remain. Strict privacy laws have been passed recently that carry harsh penalties for any negligence that exposes personal or confidential data. There is ongoing debate about censorship on the Internet. The proponents of censorship feel that it is up to the government and various ISPs and websites to control inappropriate or offensive content. Others oppose any form of censorship; they believe that control is up to the individual. In the United States, most legal attempts to censor content on the Internet have been found unconstitutional. The debate is not likely to be resolved any time soon.
4. **Fraud on the Internet and how to protect consumers against it.** Protection is needed because there is no face-to-face contact between buyers and sellers; there is a great possibility of fraud; there are insufficient legal constraints; and new issues and scams appear constantly. Several organizations, private and

public, attempt to provide the protection needed to build the trust that is essential for the success of widespread EC. Of note are electronic contracts (including digital signatures), the control of gambling, and what taxes should be paid to whom on interstate, intrastate, and international transactions. The practice of no sales tax on the Internet is changing. States are starting to collect sales tax on Internet transactions.

5. **Protection of buyers and sellers.** Many procedures are used to protect consumers. In addition to legislation, the FTC tries to educate consumers so they know the major scams. The use of seals on sites (such as TRUSTe) can help, as well as tips and measures taken by vendors. Sellers can be cheated by buyers, by other sellers, or by criminals. Protective measures include using contacts and encryption (PKI, see Chapter 10), keeping databases of past criminals, sharing information with other sellers, educating employees, and using artificial intelligence software.
6. **Societal impacts of EC.** EC brings many societal benefits, ranging from improved security, transportation, and education to better healthcare delivery and international collaboration. Although the digital divide still exists between developed and developing countries, the advent of mobile computing, especially through smartphones, is beginning to close the gap.
7. **Green EC.** EC requires large data centers, but these data centers waste energy and create pollution. Users of large data centers (e.g., Google) are using innovative methods to improve the situation. Other environmental concerns are also caused by the use of EC. There are several ways to make EC greener, including working from home (telecommuting).
8. **The future of EC.** EC is growing steadily and rapidly, expanding to include new products, services, business models, and countries. The most notable areas of growth are the integration of online and offline commerce, mobile commerce (mostly due to smartphone apps), video-based marketing, and social media and networks. Several emerging technologies, ranging from intelligent applications to wearable devices, are facilitating the growth of EC. On the other hand, several factors, are slowing down the spread of EC such as security and privacy concerns; limited bandwidth, and lack of standards in some areas of EC.

KEY TERMS

Business ethics
Computer Fraud and Abuse Act (CFAA)
Copyright
Copyright infringement
Cyberbashing
Cyberbullying
Digital divide
Digital rights management (DRM)
Electronic discovery (e-discovery)
Electronic Product Environmental Assessment Tool (EPEAT)
Electronic signature
Ethics
Fair use
Green computing
Green IT
Intellectual property (IP)
Intellectual property law
Internet censorship
Net neutrality
Opt-in
Opt-out
Patent
Platform for Privacy Preferences Project (P3P)
Spyware
Telecommuting
Trademark dilution

DISCUSSION QUESTIONS

1. What can EC websites and social networks do to ensure the safeguarding of personal information?
2. Privacy is the right to be left alone and free of unreasonable personal intrusions. What are some intrusions that you consider "unreasonable"?
3. Who should control minors' access to "offensive" material on the Internet – parents, the government, or ISPs? Why?

4. Discuss the conflict between freedom of speech and the control of offensive websites.
5. Discuss the possible insufficient protection of opt-in and opt-out options. What measures would satisfy you?
6. Clerks at some convenience stores enter their customers' data (gender, approximate age, and so on) into the computer. These data are then processed for improved decision making. Customers are not informed about this, nor are they being asked for permission. (Names are not keyed in.) Are the clerks' actions ethical? Compare this with the use of cookies.
7. Why do many companies and professional organizations develop their own codes of ethics? After all, ethics are generic and "one size may fit all."
8. Cyberpromotions, Inc. attempted to use the First Amendment in defense of its flooding AOL subscribers with junk e-mail, which AOL tried to block. A federal judge agreed with AOL that unsolicited e-mail is annoying, a waste of Internet time, and often inappropriate and, therefore, should not be sent. Discuss some of the issues involved, such as freedom of speech, how to distinguish between junk and non-junk e-mail, and the similarity to regular mail. Cyberpromotions is no longer in business.
9. What contribution does TRUSTe make to e-commerce?

TOPICS FOR CLASS DISCUSSION AND DEBATES

1. Discuss what the RIAA hopes to achieve by using lawsuits against college students for copyright infringement. Research the issue of how will the proposed Copyright Enforcement Bill, if enacted, support further RIAA lawsuits? Find the status of the bill. Write a report.
2. The proposed Copyright Enforcement Bill defines everyone that creates a website as a publisher and is liable under the Act. Enforcement under this proposed bill for unintentional use or distribution of copyrighted content on business websites could result in the confiscation of a company's domain name or server, which in turn could potentially disable the company's e-mail capability – substantially killing commerce. What steps should a business take to minimize the risk? Discuss.
3. The IRS buys demographic market research data from private companies. These data contain income statistics that could be compared with tax returns. Many U.S. citizens feel that their rights within the realm of the Electronic Communications Privacy Act (ECPA) are being violated; others say that this is unethical behavior on the part of the government. Discuss.
4. Many hospitals, health maintenance organizations, and federal agencies are converting, or plan to convert, all patient medical records from paper to electronic storage (using imaging technology) in compliance with the Patient Protection and Affordable Care Act (PPAC), also known as "Obamacare." The PPAC mandates that all medical records shall be freely disseminated to insurance companies, the U.S. government, and government-approved third-party vendors. Once completed, electronic storage will enable expeditious access to most records anytime and from anywhere. However, the availability of these records in a database or on networks or smart cards may allow people, some of whom are unauthorized, to view another person's private medical data. To protect privacy fully may cost too much money or may considerably slow down the speed of access to the records. What policies could healthcare administrators use to prevent unauthorized access? Discuss.
5. The Communications Decency Act (CDA), which was intended to protect children and others from pornography and other offensive material online, was approved by the U.S. Congress but then was ruled unconstitutional by lower courts. In 2015, it is still being debated. Discuss the implications of this Act. Also, check the Supreme Court ruling.
6. Debate the pros and cons of the Marketplace Fairness Act.
7. Debate the pros and cons of net neutrality.
8. Research the potential impact of online gambling on physical casinos.

9. Erotic services advertising on Craigslist amounted to a significant portion of the total revenue before being taken down following national publicity over the robbery and murder of a Boston massage therapist, who had advertised on Craigslist. Craigslist denied responsibility, citing the 1996 Federal Communication Act, since Craigslist does not create the content published on its website. Later, Craigslist voluntarily removed the erotic services from its regular pages. Address the following topics in a class discussion:
   (a) Craigslist may have chosen to voluntarily remove its erotic-related advertising for political reasons, even though no laws were being broken. Discuss free speech versus public safety. Take an issue and support the pros and cons of Craigslist's action.
   (b) Do you agree that self-governing Web content is the most effective means of providing public safety or should the federal government step in to enact tougher laws?
   (c) Take the position of an erotic dancer. Determine an argument in favor of reversing Craigslist's decision to remove "erotic services" advertisements. (Use free speech and right to earn money through employment.)
10. Many sports-related leagues, including the NFL and UK Football Association, restrict the players' use of social networks. The NFL prohibits any use of social networks 90 minutes before and 90 minutes after games. Debate the issue.
11. Debate Yahoo's "no work from home" policy. Start by reading Ascharya (2013).
12. Have two groups debate the issue of ownership of user-generated content (the Facebook example). One group should be for and one against.
13. Debate: Neutrality on the Internet is good for EC.
14. Debate: Should the exchange of songs between individuals, without paying royalties, be allowed over the Internet?
15. Debate: Is the Patriot Act too loose or too tight?
16. Debate: It may be too expensive for some companies to "go green." If they "go green," they may not be able to compete against companies in countries that do not practice green EC. Should the government subsidize green EC?
17. Debate: Who should own content created by employees during their regular work hours?
18. Debate: Are privacy standards strict enough to protect electronic health records?

INTERNET EXERCISES

1. You want to set up an ethical blog. Using sites such as CyberJournalist.net: A Bloggers' Code of Ethics at **cyberjournalist.net/news/000215.php**, review the suggested guide to publishing a blog. Make a list of the top 10 ethical issues for blogging.
2. You want to set up a business-oriented website. Prepare a report summarizing the types of materials you can and cannot use (e.g., logos, graphics, etc.) without breaking copyright laws. (Consult some free legal websites.)
3. Conduct a Google search for industry and trade organizations involved in various computer privacy initiatives. One of these groups is the World Wide Web Consortium (W3C). Describe its Platform for Privacy Preferences Project (P3P) (**w3.org/P3P**). Prepare a table with 10 initiatives and describe each briefly.
4. Enter **symantec.com**. Review the services offered to topics discussed in this chapter.
5. Enter **calastrology.com**. What kind of community is this? Check the revenue model. Then enter **astrocenter.com**. What kind of site is this? Compare and comment on the two sites.
6. Enter **nolo.com**. Find information about various EC legal issues. Find information about international EC issues. Then go to **legal-compliance.org** or **cybertriallawyer.com**. Find information about international legal aspects of EC. Conduct a Google search for additional information on EC legal issues. Prepare a report on the international legal aspects of EC.
7. Find the status of the latest copyright legislation. Try **fairuse.stanford.edu** and **wipo.int/**

copyright/en. Is there anything new regarding the international aspects of copyright legislation? Write a report.

8. Enter **ftc.gov** and identify some of the typical types of fraud and scams on the Internet. List 10 of them.
9. Enter **www.usispa.org** and **ispa.org.uk**, two organizations that represent the ISP industry. Identify the various initiatives they have undertaken regarding topics discussed in this chapter. Write a report.
10. Enter **scambusters.org** and identify and list its anti-fraud and anti-scam activities.

TEAM ASSIGNMENTS AND PROJECTS

1. **Assignment for the Opening Case**
   Read the opening case and answer the following questions:
   (a) Discuss the issue of preventing movies and TV shows from being streamed online for free.
   (b) Was it ethical for Disney to invest in 56.com?
   (c) What are the business benefits to Disney if it is not in conflict with 56.com?
   (d) Discuss the global considerations of this case.
   (e) Find the status of the $1 billion lawsuit Viacom brought against YouTube.
2. The number of lawsuits in the United States and elsewhere involving EC has increased. Have each team prepare a list of five recent EC legal cases on each topic in this chapter (e.g., privacy, digital property, defamation, patents). Prepare a summary of the issues of each case, the parties, the courts, and dates. What were the outcomes of these cases? What was (or might be) the impact of each decision?
3. Form three teams. Have two teams debate free speech versus protection of children. The third team acts as judges. One team is for complete freedom of speech on the Internet; the other team advocates protection of children by censoring offensive and pornographic material. After the debate, have the judges decide which team provided the most compelling legal arguments.
4. It is legal to monitor employees' Internet activity, e-mail, and instant messages? Note that it is legal to open letters addressed to individuals sent to the company's address. Why is the monitoring necessary? To what extent is it ethical? Are employees' rights being violated? Have two teams debate these issues.
5. Amazon.com is disputing several states that are trying to force the company to collect state taxes ("Amazon laws"). Amazon cancelled its affiliate program in certain states (e.g., Colorado, Minnesota) when the sales tax for online retailing was imposed (however, they reinstated their program in California). Check the status of this law (requiring Amazon to collect taxes) and its relationship to Federal law. Start at **illinoisjltp.com/timelytech/ongoing-taxation-disputes-between-amazon-and-state-governments.**
6. Smart computer programs enable employers to monitor their employees' movements online. The objective is to minimize wasting time and computing resources, and reduce theft by employees. These actions may invade privacy, and reduce confidence and loyalty. Find the various methods used to monitor employees (list their approaches) and list all possible negative aspects. Find case studies about the benefits (including increasing productivity) and the limitations and dangers. Relate monitoring to telecommuting and debate the issue.

CLOSING CASE: THE PIRATE BAY AND THE FUTURE OF FILE SHARING

What had been considered a landmark 2009 copyright law case involving the Motion Picture Association of America (MPAA) against illegal file sharing in Sweden appears to not have significantly deterred online file sharing. In fact, just the opposite may have occurred.

An Overview

The Pirate Bay (TPB) site was launched in 2003 by hackers and computer activists as a BitTorrent tracker, make it possible to get free access to most media content (including copyrighted material) using BitTorrent peer-to-peer (P2P) file-sharing protocol services (see **en.wikipedia.org/wiki/BitTorrent**). The Pirate Bay site includes links to websites where you can download movies, TV shows, music e-books, live sport games, software, and more. TPB has been ranked as one of the most popular websites in the world. The site generates revenue by advertisements, donations, and sales of merchandise. The site is probably the most well-known among dozens of other sites that provide free access to copyrighted content.

The Legal Situation

The Pirate Bay has been involved in a number of lawsuits, both as a defendant and as a plaintiff. For an overview, see **torrentfreak.com/the-pirate-bay-turns-10-years-old-the-history-130810**. Here are some examples. In Sweden, The Pirate Bay company was raided by the Swedish police in 2006. The site was shut down, but reappeared a few days later with servers hosted in different countries. In 2008, the Swedish government began a criminal investigation against the founders of TPB for copyright theft. Three founders and a financier were charged with promoting copyright infringement by facilitating other people's breach of copyright law by using TPB BitTorrent technology. For 34 cases of copyright infringement, the damage claims could have exceeded US$12 million. The trial started on February 16, 2009, and ended on March 3, 2009, with a guilty verdict that carried a one-year prison sentence and a fine of US$3.5 million. The four founders lost on appeal in 2010 but succeeded in getting reduced prison time; however, the copyright infringement fine was increased. The site is now blocked by several countries. The U.S. government considers TPB (together with the Chinese sites Baidu and Taobao Marketplace) a top market for pirated and counterfeit goods.

Current Operation

As of June 2014, TPB continues to offer torrent files and magnet links to facilitate file sharing for those using the BitTorrent system. The site also offers downloading, watching videos, and searching for all types of media. In fact, much public support for TPB was noted. In 2003, Piratbyrån ("The Pirate Bureau"), a Swedish organization, was established to support the free sharing of information (however, they disbanded in 2010). Political parties in many European countries have adopted the label "The Pirate Party," after a party in Sweden, which was formed in 2006. Other countries followed suit, creating their own Pirate Parties. The party supports the reform of copyright and patent laws, government transparency, and net neutrality. In 2006, the International Pirate Party Movement was formed as an umbrella organization. In 2009, the Swedish Pirate Party won a seat in the European Parliament and in 2013, Iceland gained three similar seats. The Pirate Bay advocates copyright and patent law reform and a reduction in government surveillance. In the meantime, in Sweden, TPB's founders have worked on several other decentralized peer-to-peer file-sharing websites, which have flourished in filling the enormous global demand for P2P file sharing. TPB has plenty of defenders. In 2014, the supporters of TPB's jailed founder planned an online campaign to bring more attention to his situation.

All along, file-sharing technology has been one step ahead of enforcement. Since some countries block access to TPB, there are several proxy URLs now that provide indirect access to TPB website.

Despite losing its November 2010 appeal, TPB has kept growing. In 2011, TPB's founders launched a new website, called IPREDator, offering IP address anonymity to registered users by tunneling traffic into a secure server, which reassigns fake IP addresses to registered users so that they may access TPB or other BitTorrent tracking sites on the Web for file sharing without revealing their true IP addresses. Although TPB continues to thrive today as one of the most popular websites on the Internet, many countries are enacting new stricter copyright protection laws aimed directly at stopping this illegal activity.

Note that Facebook blocks all shared links to TPB in both public and private messages (however, TPB does have a Facebook page). In 2012, a UK court ordered a blockade on TPB in the UK because of its violation of copyright law (see Dragani 2012). Some countries are allowing access to TPB. For example, in 2014, the Netherlands court ordered the ban on TPB lifted (see **bbc.com/news/technology-25943716**).

In 2012, The Pirate Bay, to protect itself from raids, moved its operation from physical servers to the cloud. Serving its users from several cloud hosting providers makes it impossible to raid because there are no physical locations; the site is more portable and thus makes it more difficult to shut down. Other benefits include reducing downtime, ensuring better uptime, and cutting costs (see Van Der Sar 2012).

Discussion

The Pirate Bay is one of a multitude of websites that specializing in pirated and counterfeit content. The Pirate Bay does not host content, in contrast to sites, which allow people to upload videos, included pirated ones. The Pirate Bay only provides links to possible illegal downloads. This strategy did not help the site much in its legal battles.

The Pirate Bay case is only one part of a much broader issue of protecting intellectual property on the Internet. An interesting related issue is the hosting of content by sites such as YouTube and Justin.tv, which is more complicated.

Note that one aspect of this case is that the U.S. government is pushing the Swedish government to take a stronger stand against pirating.

Sources: Based on Stone (2011), Dragani (2012), Martin (2012), and **medlibrary.org** (accessed June 2014).

Questions

1. Compare TPB's legal problems to those of Napster between 2000 and 2005, and to those of Kazaa (file sharing companies).
2. Debate the issue of freedom of speech on the Internet against the need to protect intellectual property.
3. What is The Pirate Bay's business model? What are its revenue sources? (Find more information; start with Wikipedia.)
4. Explore the international legal aspects of this case. Can one country persuade another country to introduce stricter laws?
5. Read the Stone (2011) article and identify all the measures used to battle piracy of live sporting events. Which of these measures can be used in The Pirate Bay case? Which cannot? Why?
6. Find the status of the TPB website.

ONLINE FILES
available at **affordable-ecommerce-textbook.com/turban**

W15.1 Framework for Ethical Issues
W15.2 Website Quality Guidelines
W15.3 Summary of Important EC Legal Issues
W15.4 How to Go Green in a Data Centers

COMPREHENSIVE EDUCATIONAL WEBSITES

ftc.gov: Major source on consumer fraud and protection.
dmoz.org/Society/Issues/Fraud/Internet: Comprehensive resources on Internet fraud.
fraud.org: The National Consumers League Fraud Center.
ic3.gov: The FBI's Internet Crime Complaint Center.
www.fda.gov/ForConsumers/ProtectYourself/default.htm: Food and Drug Administration center for resources, recalls, safety, regulatory information, etc. about food, drugs, vaccines, cosmetics, and more.
business.usa.gov: A single platform to make it easier for businesses to access programs and services.
sba.gov/advo/laws/law_modeleg.html: Small Business Administration's advocacy site to stay current with federal regulations.
law.com: A comprehensive source for legal news and analysis.

lawbrain.com: A comprehensive collection of law–related material; users can share opinions and knowledge by adding to and editing existing pages.

bna.com/legal-business-t5009: Bloomberg Inc. legal and business portal that includes blogs, events, news, and more.

privacy.org: A comprehensive source of information on privacy.

epic.org: Electronic Privacy Information Center; a non-profit research center to protect privacy, freedom of expression, and more.

privacyrights.org: Privacy Rights Clearinghouse; a non-profit organization educating and empowering individuals to protect their privacy. An online clearinghouse.

www.itworld.com/green-it: A comprehensive source for green IT-related news and analysis.

digitaldivide.org: The Digital Divide Institute. A comprehensive collection material related to the digital divide.

techworld.com/green-it: A comprehensive collection of green IT-related material.

epolicyinstitute.com: A comprehensive collection of EC policy development resources.

eff.org/issues/bloggers/legal: A legal guide for bloggers.

thegreengrid.org: Comprehensive resources on efficiency in IT and data centers.

GLOSSARY

Business ethics (corporate or enterprise ethics) A code of values, behaviors, and rules, written or unwritten, for conducting business. These ethics dictate the operations of organizations.

Computer Fraud and Abuse Act (CFAA) An important milestone in EC legislation that protects government computers and other Internet-connected computers.

Copyright An exclusive legal right of an author or creator of intellectual property to publish, sell, license, distribute, or use such work in any desired way.

Copyright infringement The use of a work without permission or contracting for payment of a royalty.

Cyberbashing The registration of a domain name that criticizes (normally maliciously) an organization, product, or person (e.g., **paypalsucks.com**, **walmartsucks.org**, **verizonpathetic.com**). Usually associated with hate sites.

Cyberbullying "Bullying that takes place using electronic technology. Electronic technology includes devices and equipment such as cell phones, computers and tablets as well as communication tools including social media sites, text messages, chat, and websites." (per **stopybullying.gov**)

Digital divide The gap that has emerged between those who have and those who do not have the ability to engage in e-commerce.

Digital rights management (DRM) A system of protecting the copyrights of data circulated over the Internet or digital media. These arrangements are technology-based protection measures (via encryption or using watermarks).

Electronic discovery (e-discovery) The process of finding any type of electronic data (e.g., text, images, videos) by using computerized systems.

Electronic Product Environmental Assessment Tool (EPEAT) A comprehensive global rating system for greener electronics based on a range of environmental performance criteria.

Electronic signature "The electronic equivalent of a handwritten signature" (per **pcmag.com/encyclopedia/term/42500/electronic-signature**).

Ethics A set of moral principles or rules of how people are expected to conduct themselves.

Fair use The limited use of copyrighted material, without paying a fee or royalty, for certain purposes (e.g., reviews, commentaries, teaching).

Green computing The eco-friendly use of computing resources.

Green IT The efforts to improve the use of EC (and IT) by minimizing damage to the environment, and at the same time saving money.

Intellectual property (IP) Property that derives from the creative work of an individual, such as literary or artistic work.

Intellectual property law Area of the law concerned with the regulation of thinking-related products, including creativity that are protected

by patents, copyrights, trademarks, and trade secret law.

Internet censorship Restrictions on what can be seen, published, or accessed on the Internet.

Net neutrality A network design principle stating that basic protocols of the Internet should enable users to utilize the Web without being discriminated against by Internet service providers.

Opt-in The principle that consumers must approve, in advance, what they are willing to see. That is, information sharing should not occur unless customers affirmatively allow or request it.

Opt-out A method that gives consumers the choice to refuse to share information about themselves, or to avoid receiving unsolicited information.

Patent "An exclusive right to a particular invention. Patents are granted by states or governments to the creator of an invention, or to someone who has been designated by them to accept the rights over the invention. The holder of the patent has sole rights over the invention for a specified period of time." (per Fedcirc.us)

Platform for Privacy Preferences Project (P3P) A protocol for privacy protection on the Web developed by the W3 Organization (W3C).

Spyware A tool that some merchants use to gather information about users without their knowledge.

Telecommuting Working at home using a PC, tablet, smartphone, and the Internet.

trademark dilution The use of a "famous" trademark by a third party, which causes the lessening (or dilution) of the 'distinguishing quality' of the mark.

REFERENCES

56.*com*. "56.com Launch Content C-C Platform '56 Kan Kan'." August 18, 2009. **56.com/v/about/en/intro_press_en.html** (accessed June 2014).

ACLU of Washington State. "Libraries, the Internet, and the Law: Adults Must Have Unfiltered Access." November 15, 2006. **aclu-wa.org/news/libraries-internet-and-law-adults-must-have-unfiltered-access** (accessed June 2014).

Albanesius, C. "Viacom Will Know What You've Watched on YouTube." July 3, 2008. **pcmag.com/article2/0,2817,2324635,00.aspml** (accessed June 2014).

Alghamdi, A. M. *The Law of E-Commerce: E-Contract, E-Business.* UK: AuthorHouse UK, 2011.

Anderson, N. "Apple Loses Big in DRM Ruling: Jailbreaks Are Fair Use." July 26, 2010. **arstechnica.com/tech-policy/2010/07/apple-loses-big-in-drm-ruling-jailbreaks-are-fair-use** (accessed June 2014).

Andrews, L. *I Know Who You Are and I Saw What You Did: Social Networks and the Death of Privacy.* Florence, MA: Free Press, 2012.

Anthony, S. "The FCC's Net Neutrality Proposal: What Does It Mean for You, and the Internet?" May 16, 2014. **extremetech.com/computing/182572-the-fccs-net-neutrality-proposal-what-does-it-mean-for-you-and-the-internet** (accessed June 2014).

Ascharya, K. "Marissa Mayer and the Telecommuting Debate." March 26, 2013. **2machines.com/articles/178412.html** (accessed June 2014)

Bambauer, D. "Tenenbaum and Statutory Damages." *Info/Law*, July 11, 2010. **blogs.law.harvard.edu/info-law/2010/07/11/tenenbaum-and-statutory-damages** (accessed July 2014).

Barakat, M. "Popular File-Sharing MegaUpload Shut Down." January 20, 2012. **news.yahoo.com/popular-file-sharing-website-megaupload-shut-down-232101369.html** (accessed June 2014).

Bercovici, J. "Yahoo Spins No-Work-From-Home Policy as Morale Booster. Seriously." *Forbes*, March 6, 2013.

Bhargava, R. "Social Media and the Axe Murderer: How Privacy Is Evolving Online." February 7, 2010. **socialmediatoday.com/rohitbhargava/111773/social-media-axe-murderer-how-privacy-evolving-online** (accessed June 2014).

Billboard Biz. "China Arrests 4,000, Vows Tougher Punishments for Copyright Piracy in Advance of U.S. Trade Talks." January 11, 2011. **billboard.com/biz/articles/news/global/1179729/china-arrests-4000-vows-tougher-punishments-for-copyright-piracy-in** (accessed June 2014).

Cagaoan, K.A.A, M. J. A. V. Buenaobra, A. T. M. Martin, and J. C. Paurillo. "Privacy Awareness in E-Commerce." *International Journal of Education and Research*, January 2014. Vol. 2, No. 1, **ijern.com/journal/January-2014/19.pdf** (accessed Nov 2014).

Chia, E. "City 2.0: Technology to Make Cities More Liveable." March 22, 2012. **enterpriseinnovation.net/article/city-2-0-technology-make-cities-more-liveable** (accessed June 2014).

Clancy, H. "Virtualization Core to Wells Fargo Green IT Initiative." July 6, 2010. **zdnet.com/blog/green/virtualization-core-to-wells-fargo-green-it-initiative/12852** (accessed June 2014).

ClassActionLawsuitsInTheNews.com. "McAfee Class Action Lawsuit Filed over Arpu Pop Up Advertisements." April 9, 2010. **classactionlawsuitsinthenews.com/class-action-lawsuits/mcafee-class-action-lawsuit-filed-over-arpu-pop-up-advertisements** (accessed June 2014).

ComputerWeekly.com. "Privacy Lawsuit Filed Against Facebook." August 18, 2009. **computerweekly.com/news/1280090498/Privacy-lawsuit-filed-against-Facebook** (accessed June 2014).

CyberSource. "13th Annual 2012 Online Fraud Report." CyberSource Corporation, 2012.

Davidson, A. *The Law of Electronic Commerce.* Melbourne, Australia: Cambridge University Press, 2009.

Doctorow, C. "The Curious Case of Internet Piracy." *MIT Technology Review*, June 6, 2012.

Dragani, R. "UK Court Orders Blockade on Pirate Bay." *E-Commerce Times*, May 1, 2012.

Enterprise Innovation Editors. "A Whole Host of Prediction for 2014 and Beyond." December 31, 2013. **enterpriseinnovation.net/article/whole-host-predictions-2014-and-beyond-1771618066** (accessed June 2014).

Enviro Boys. "Is Telecommuting on the Rise?" November 14, 2010. **enviroboys88.blogspot.com/2010/11/telecommuting-on-rise.html** (accessed June 2014).

Ferrell, O.C., et al. *Business Ethics: Ethical Decision Making & Cases*, 9th ed., Boston, MA: South-Western Cengage Learning, 2012.

Fogarty, K. "Copyright Infringement Bill Could Bring the FBI to Your Intranet." November 22, 2010. **www.itworld.com/legal/128550/copyright-infringement-bill-could-bring-fbi-your-intranet?page=0,0** (accessed June 2014).

Frucci, A. "RIAA Spent $58 Million Suing File Sharers, Got 2% Back." July 14, 2010. **gizmodo.com/5587306/the-riaa-spent-58-million-suing-file-sharers-got-2-back** (accessed June 2014).

Gallio, L. "Surveillance Camera: Big Brother and Big Sis are Watching!" August 29, 2010. **examiner.com/article/surveillance-cameras-big-brother-and-big-sis-are-watching** (accessed June 2014).

Gavish, B., and C. L. Tucci. "Reducing Internet Auction Fraud." *Communications of the ACM*, vol. 51 no. 5, 89–97 May 2008.

Gaylord, C., "How Big Data Helps Big Cities." *The Christian Science Monitor*, June 7, 2013.

Geranios, N. K. "Internet Addiction Center Opens in U.S." *USA Today* (by Associated Press) September 3, 2009.

Gerber, S., "10 Predictions About the Future of Ecommerce." October 1, 2013. **mashable.com/2013/10/01/future-e-commerece/** (accessed June 2014).

Gouveia, A. "2013 Wasting Time at Work Survey." July 28, 2013. **sfgate.com/jobs/salary/article/2013-Wasting-Time-at-Work-Survey-4374026.php** (accessed June 2014).

Gray, B. R. "Bullying and Harassment in the Workplace." October 13, 2010. **ezinearticles.com/?Bullying-And-Harassment-In-The-Workplace&id=5200849** (accessed June 2014).

Greene, J. "Supreme Court Rules Against Microsoft in i4i Patent Case." June 9, 2011. **cnet.com/news/supreme-court-rules-against-microsoft-in-i4i-patent-case** (accessed June 2014).

Gross, D. "Pay to Play on the Web? Net Neutrality Explained." January 15, 2014. **cnn.com/2014/01/15/tech/web/net-neutrality-explained** (accessed May 2015).

Gustin, S. "Web Censorship Bill Sails through Senate Committee." November 18, 2010. **wired.com/2010/11/coica-web-censorship-bill** (accessed June 2014).

Guynn, J., "Lawmakers ask Google's Larry Page to address Glass privacy issues." *Los Angeles Times*, May 16, 2013

Hill, K. "Lawsuit of the Day: Hey Teacher, Leave Them Kids Alone! (Or: Activating Laptop Webcams to Spy on Students at Home is Not Cool)." February 18, 2010. **abovethelaw.com/2010/02/lawsuit-of-the-day-hey-teacher-leave-them-kids-aloneor-activating-laptop-webcams-to-spy-on-students-at-home-is-not-cool** (accessed June 2014).

Himma, K. E., and H. T. Tavani (Eds.). *The Handbook of Information and Computer Ethics.* Hoboken, NJ: Wiley-Interscience, 2008.

IBM. "Data Privacy Best Practices: Time to Take Action!" A white paper (#IMW14072-USEN-00), September 2008a. *IBM Information Management Software* (see Enterprise data management solutions).

IBM. "IBM Software: A Green Strategy for Your Entire Organization." A white paper, June 2008b. New York: IBM Software Group.

Kalanda, R. "Does Amazon's 'One-Click' Success Mean Business Method Patents for All?" *E-Commerce Times*, March 31, 2012. **ecommercetimes.com/story/74719.html** (accessed June 2014).

Kontzer, T. "E-Discovery Tools Aid Compliance, Save Money." *Baseline*, July 11, 2012.

Kravets, D. "U.S. Declares iPhone Jailbreaking Legal, Over Apple's Objections."July 26, 2010. **wired.com/threatlevel/2010/07/feds-ok-iphone-jailbreaking** (accessed June 2014).

Lattanzio, V. "2nd Lawsuit Filed Over WebcamGate." July 28, 2010. **nbcphiladelphia.com/news/politics/2nd-Lawsuit-Filed-Over-Webcam-Gate-99368474.html** (accessed June 2014).

Leggatt, H. "Online Privacy Real Concern for 90% of U.S. Internet Users." February 14, 2012. **bizreport.com/2012/02/90-percent-of-online-adults-worry-about-their-online-privacy.html** (accessed June 2014).

Leonhard, G. "Is Your Wearable Tech Helping You—or Watching You?" April 29, 2014. **edition.cnn.com/2014/04/29/business/is-your-wearable-tech-helping-you----or-watching-you/** (accessed June 2014).

Lewis, P., and J. Domokos. "Caught on Camera: Lancashire Police Arrest Amateur Photographer." *The Guardian*, February 21, 2010.

Litle & Co. "Fraud Detection & Mitigation Strategies." May 2014. **litle.com/downloads/resources/Fraud-Detection-Mitigation-Strategies.pdf** (accessed June 2014).

Mallor, J., et al. *Business Law: The Ethical, Global and E-Commerce Environment,* 14th ed. New York: McGraw-Hill/Irwin, 2009.

Mann, R. J., and J. K. Winn.Electronic Commerce (Law in Commerce), 3rd ed. New York: Aspen Publishers, 2008.

Martin, R. "Supreme Court Denies Pirate Bay Right to Appeal."February 1,2012.**thelocal.se/20120201/38844#.UWTQh5M27Sg** (accessed June 2014).

Mayton, J. "RIP Net Neutrality? FCC Backs New Rules That Permit Pay-Based Internet 'Fast Lane.'" April 26,

2014. **techtimes.com/articles/6062/20140426/rip-net-neutrality-fcc-backs-new-rules-that-permit-pay-based-internet-fast-lane.htm** (accessed June 2014).

McBride, S., and L. Chao. "Disney Affiliate Is Besieged by Pirates." November 21, 2008 (Updated). **online.wsj.com/news/articles/SB122722555475645951** (accessed June 2014).

Mercola, J. "If You See This Google Warning, Act Fast: Big Brother is Watching." August 5, 2012. **articles.mercola.com/sites/articles/archive/2012/08/05/internet-security-virus.aspx** (accessed June 2014).

Miller, C. C. "Craigslist Says It Has Shut Its Section for Sex Ads." *New York Times Business,* September 15, 2010.

Murugesan, S., and G. R. Gangadharan (Eds.) *Harnessing Green IT: Principles and Practices.* Hoboken, NJ: Wiley, 2012.

Nakashima, E. "U.S. Seeks Ways to Wiretap the Internet." *The Washington Post*, September 28, 2010.

Nelson, N. "How to Estimate Energy Efficiency as Part of a Server Upgrade." *eWeek*, April 28, 2008. **eweek.com/it-management/How-to-Estimate-Energy-Efficiency-as-Part-of-a-Server-Upgrade/** (accessed June 2014).

Nielsen. "State of the Media: The Social Media Report 2012." 2012. **nielsen.com/us/en/reports/2012/state-of-the-media-the-social-media-report-2012.html** (accessed June 2014).

O'Brien, K.J. and Streitfeld, D. "Swiss Court Orders Modifications to Google Street View." June 8, 2012. **nytimes.com/2012/06/09/technology/09iht-google09.html?_r=0** (accessed June 2014).

Owens, D. "What is Trademark Dilution." May 3, 2011. **smartbusinessrevolution.com/trademark-dilution** (accessed June 2014).

Park, H. S. "Empowering Employees with Technology." *Baseline*, May 27, 2009.

Parks, L. "Just the Ticket: Detection System Helps New Era Virtually Eliminate Online Fraud." *Stores,* April 2010.

Parry, W. "Casinos Brace for Impact of Internet Gambling." May 3, 2013. **bigstory.ap.org/article/casinos-brace-impact-internet-gambling** (accessed June 2014).

Pfanner, E. "Swiss Say Google's Street View Is Too Revealing." *New York Times Technology*, November 13, 2009. **nytimes.com/2009/11/14/technology/companies/14google.html** (accessed June 2014).

PRC. "Workplace Privacy and Employee Monitoring." (Revised May 2014). **privacyrights.org/workplace-privacy-and-employee-monitoring** (accessed June 2014).

Sager, K., J. Fisher, R. Wilcox, and J. Eastburg. "City of Ontario v. Quon: United States Supreme Court Rejects Police Officer's Lawsuit Claiming That City's Review of His Personal Text Messages Was an Illegal Search." June 18, 2010. **dwt.com/advisories/City_of_Ontario_v_Quon_United_States_Supreme_Court_Rejects_Police_Officers_Lawsuit_Claiming_That_Citys_Review_of_His_Personal_Text_Messages_Was_an_Illegal_Search_06_18_2010** (accessed June 2014).

Samson, T. "GreenNet 2010: Google Shares Its Green Data Center Secrets." *InfoWorld*, April 29, 2010.

San Miguel, R. "Sheriff Sues Craigslist to Curb Prostitution." *E-Commerce Times*, March 6, 2009.

Savitz, E. "eBay Wins Tiffany Trademark Case." July 14, 2008. **blogs.barrons.com/techtraderdaily/2008/07/14/ebay-wins-tiffany-trademark-case** (accessed June 2014).

Schreiber, J. "Big Brother Is Here, Families Say." February 18, 2010. **courthousenews.com/2010/02/18/24789.htm** (accessed June 2014).

Shah, M.H., R. Okeke, and R. Ahmed. "Issues of Privacy and Trust in E-Commerce: Exploring Customers' Perspective." *Journal of Basic and Applied Scientific Research*, 3 (3) 571–577, 2013.

Stein, J. "Data Mining: How Companies Know Everything About You." *Time*, March 21, 2011, Vol. 177, No. 11.

Sterling, T. "European Court: Google Must Yield on Personal Info." May 13, 2014. **bigstory.ap.org/article/european-court-upholds-right-be-forgotten-says-google-must-edit-some-search-results** (accessed June 2014).

Stone, B. "Pro Sports versus the Web Pirates." February 24, 2011. **businessweek.com/magazine/content/11_10/b4218066626285.htm** (accessed June 2014).

Van Der Sar, E. "Pirate Bay Moves to the Cloud, Becomes Raid-Proof." October 17, 2012. **torrentfreak.com/pirate-bay-moves-to-the-cloud-becomes-raid-proof-121017** (accessed June 2014).

WorldNetDaily. "U.S. Regulatory Czar Nominee Wants Net 'Fairness Doctrine.'" April 27, 2009. **wnd.com/2009/04/96301** (accessed June 2014).

Woyke, E. "FCC Tips Net Neutrality Passage but Questions Remain." *Forbes*, December 20, 2010.

Yamamura, J. H., and F. H. Grupe. "Ethical Considerations for Providing Professional Services Online." May 2008. **nysscpa.org/cpajournal/2008/508/essentials/p62.htm** (accessed June 2014).