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 of 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 fake content on the Web and what can be done about it.
5. Describe EC-related societal issues and loss of jobs in particular.
6. Describe Green EC and IT.
7. Describe the future of e-commerce.

E. Turban et al., *Electronic Commerce 2018*, Springer Texts in Business and Economics, DOI 10.1007/978-3-319-58715-8_15

OPENING CASE
FAKE NEWS: THE AUSTIN, TEXAS, FIASCO

For a period of 3 days, November 9–11, 2016, fake news created unintentionally went viral exponentially on the Web.

The Initial Step

On November 9, a Mr. Tucker of Austin, Texas, posted a tweet about "paid protesters bused to demonstrations against President-elect Trump." Mr. Tucker read about the anti-Trump demonstration in his own city. When he saw an unusually large group of buses in downtown Austin earlier that day, he thought it was related to the demonstrations. Therefore, he took photos of the buses, and when he came home, he tweeted the pictures with his interpretation of what he saw. The truth was that there were no buses packed with paid protestors. The unusual numbers of buses were those hired by Tableau Software to bring participants to their company's conference.

The Story Goes Viral

The fake news went viral very quickly. Mr. Tucker had 40 followers on Twitter. However, within hours, the post was shared over 16,000 times on Twitter and 350,000 times on Facebook. Clearly, speed took over the truth.

Within a few hours, the tweet was also posted to the main "Reddit Community for Mr. Trump." Members went to check and found that the buses were parked just blocks away from the Austin protestors. Therefore, the members spread the fake news even further. Some even implied that George Soros, the liberal billionaire, paid for the busing and the participation. Within 15 h, the story was all over the Internet. Within a few hours after that, the bus company denied the story. However, by that time, the news spread like wildfire. In addition, Mr. Tucker admitted that he just *assumed* that the buses brought demonstrators, but he actually had not seen any. This admission also came too late.

However, Mr. Tucker repeated that the buses were near the demonstrators.

Within 24 h, a conservative blog posted the story, with the Soros money story added on. The entire conservative blogosphere continue to spread the story. The story now was inflated as "a story from an eyewitness."

Further Events

Within 24 h, President-elect Trump tweeted that it is unfair that "professional protestors that were incited by the media are protesting against the election results." This tweet angered Mr. Tucker, who decided not to delete his tweet.

The next morning, more denials from Tableau Software and others came, including the local TV stations. However, the tweet continued to generate many thousands of retweets and comments.

False Rumors Spread Much Faster Than True Ones

Within a few hours after the last denial, Mr. Tucker decided to delete his message. He posted the original message with the word "false" stamped on it. Unfortunately, after a week, that message had only 29 retweets and 27 likes. In section "Fake Content on the Web," we will discuss this phenomenon.

Source: Condensed from Maheshwari (2016), Roberts (2017a, b), and Stetler (2016).

LESSON LEARNED FROM THE CASE

Fake news is one aspect of the fake content phenomenon. We learned from this case that fake news also can be generated unintentionally and can spread very rapidly through several channels on the Web. Fake content and products constitute a major problem on the Web. In this concluding chapter, we also describe other issues that relate to the e-commerce business. They include ethics, privacy, intellectual property and piracy, legal issues, public policy regarding the Web, and social impacts. The chapter concludes with a presentation about the future of e-commerce.

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.

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. 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 implementation considerations, see Business for Social Responsibility (**bsr.org**).

The Issues of Internet Abuse in the Workplace

The actual time wasted and productivity losses due to employees spending time on the Web during working hours are very high. In general, employees spent more than 1 h per week during working hours on social media alone, followed by online games and e-mails. Many companies have banned access to social networks such as Facebook, Twitter, 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 min to several hours per day. The top four employee "time wasters" were: checking news (37%), social networking (14%), online shopping (12%), and online entertainment (11%). For more information, 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 min 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 businesspeople practicing EC. Two major risks are criminal charges and civil suits. Table 15.1 lists examples of safeguards to minimize exposure to those risks.

Table 15.1 Typical safeguards to minimize exposure to risks 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?

EC Ethical and Legal Issues

There are many EC- and Internet-related ethical issues that are related to legal issues (see Lewis 2014). These issues are often categorized into intellectual property rights, privacy, free speech versus censorship, and fraud protection methods.

- **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 (section "Intellectual Property Law and Copyright Infringement").
- **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 "Privacy Rights, Protection, and Free Speech").
- **Free speech versus censorship.** Free speech on the Web may result in offensive and harmful attacks on individuals and organizations. 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 (see Chap. 1).

Examples of ethical issues discussed elsewhere in this book are channel conflict (Chap. 3), pricing conflict (Chap. 3), disintermediation (Chaps. 3 and 4), and trust (Chap. 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**.

Other Issues

Lunka (2015) lists the following ethical issues in EC, asking: Are you violating any of them? The issues are selling counterfeit products (section "Fake Content on the Web"), Web accessibility (section "Public Policy, Taxation, and Political Environments"), accurate product listing (section "Fake Content on the Web"), and the use of EC best practices. Lunka (2015) provides some guidelines on the ethical behavior of the above.

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, tablets, 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.

According to McCafferty (2016b), Internet distractions are the top productivity killers.

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.

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. 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**).

There are various intellectual property law specialties, as shown in Table 15.2. 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, stadiums, etc. and record the performances. PirateEye (pirateeye.com) is one of the companies that manufactures devices that discover and identify the presence of any digital recording device, monitor remotely in real time, and much more.

A common problem is the illegal copying of e-books, which, according to Scott (2016), is damaging not only to authors and publishers but also to our culture. This situation requires international collaboration.

For intellectual property in social media, see Kankanala (2015).

Copyright Infringement and Protection

Numerous high-profile lawsuits already have been filed regarding online copyright infringement related to EC and the Web. 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 up to 120 years, or even longer. The legal term for the use of a work without permission or contracting for payment of a royalty is **copyright infringement**.

Example

One artist made $90,000 by selling someone's Instagram photos without permission. See details at Instagram (2015).

Table 15.2 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 protects against those pirating intellectual property

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 this chapter's closing case). 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. However, the site was relaunched in January 2013 under the domain name **mega.co.nz**.

Illegal Visits to Torrent, Streaming, and Download Sites (i.e., Piracy)

There are billions of visits to websites that provide free videos, music, books, and other media to people that do not pay for the legal versions. Known as piracy, this phenomenon is performed worldwide. In some countries (e.g., Latvia), almost half of the population visit pirate sites (see this chapter's closing case and **torrentfreak.com**; news site).

Legal Aspects of Infringement

In November 2010, the US 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." 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.

The RIAA Industry Versus the Violators

To protect its interests, the RIAA uses selective lawsuits to stamp out rampant music piracy on the Internet. However, 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. Given that there are thousands of pirate sites, to fight them is not a simple task.

Sometimes legal actions against the owners of pirate websites can be successful. However, while the actions about the Pirate Bay illegal site (closing case) ended with imprisoning the owner, the site is still alive. According to Mello, Jr. (2016b), the owner of Kickass Torrents (KAT), another popular piracy site, was arrested and is facing 20 plus years in jail. However, the site opened again in late 2016.

Note, since 2009, the number of lawsuits has been declining for several reasons. Viacom sued YouTube (Google) for $1 billion for copyright violations. 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 as through federal legislation.

Globalization

Much of the media piracy occurs in other countries (e.g., Russia, China, and Sweden, and many developing countries). Therefore, it is difficult to combat piracy, as per the closing case of Pirate Bay.

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. 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).

Patents

According to **wipo.org**, a **patent** is "an exclusive right to a particular invention, which is a product or a process that provides, in general, a new way of doing something, or offers a new technical solution to a problem." 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.

There is some discrepancy between the United States and Europe over the way certain patents are granted. For example, in 1999, Amazon.com successfully obtained a US 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 United States 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**.

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 US Supreme Court and lost.

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. In 2014, Oracle won the case (see McLaughlin 2014).

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 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-getting-started/trademark-basics/trademark-patent-or-copyright**).

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 US 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."

Protecting Intellectual Property on Websites

According to Verbauwhede (2015), "[a] company's website can be a great tool for promoting business online and generating sales. However, as Web commerce increases, so does the risk that others may copy the look and feel of your website, some of its features or the content on your website. The risk also increases that you may be accused of unauthorized use of other people's intellectual assets."

Verbauwhede (2015) lists the following elements that need to be protected: EC systems, search engines, software, website design, creative content, databases, trademark-protected items, graphic-related items, and confidential information.

(a) Verbauwhede (2015) also suggests the following protecting measures:
- Register your trademarks.
- Register a domain name that is user-friendly and reflects your trademark, business name, or character of your business.
- Think about patenting online business methods, in countries where such protection is available.
- Register your website and copyright material in countries which provide this option at the national copyright office.
- Take precautions about disclosure of your trade secrets. Make sure that all who might get to know about your confidential business information (such as employees, maintenance contractors, website hosts, Internet providers) are bound by a confidentiality or nondisclosure agreement.
- Consider to take an IP insurance policy that would cover your legal costs should you need to take enforcement action against infringers.

(b) Letting people know that the content is protected. Many people assume that material on websites can be used freely. Remind viewers of your IP rights.
- It is a good idea to mark your trademark with the trademark symbol ®, TM, SM, or equivalent symbols. Equally, you can use a copyright notice (the symbol © or the word "Copyright" or abbreviation "Copr."
- Another option is to use watermarks that embed copyright information into the digital content itself.
- Provide access control and encryption (Chap. 11).

More suggestions can be found in the article.

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.

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. Digital privacy is a world of complex paradoxes (see the infographic by EMC 2014).

One issue is the increasing use of online surveillance and knowing who is watching whom (see Angwin 2015).

Privacy in E-Commerce

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, allowing downloads, etc.). Data and Web mining companies receive and gather the collected data. As a result, users' privacy may be violated (see the slide presentation titled "Your Data, Yourself" by Justyne Cerulli at **prezi.com/fgxmaftxrxke/your-data-yourself**). Privacy concerns limit EC according to Adhikari (2016a, b).

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." Many EC activities involve privacy issues ranging from collection of information by Facebook to the use of RFID. Here we only explore the major aspects of the privacy problem in EC. For many issues of EC privacy, see Kenyon (2016) and Gupta and Dubey (2016).

Example: Google Glass

In May 2013, eight US lawmakers, concerned about Google Glass (and other smart glasses), wrote a letter to Google asking what the company planned to do to protect people's privacy. See Guynn (2013) for a description. A similar example is that stores can see where you go while you are in the store or at the shopping mall.

Here we explore the major aspects of the problem as it relates to social networking.

Social Networks Changing the Landscape of Privacy and Their Protection

Today's youth seem to be less concerned about privacy than young people 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.

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. For more about Facebook and users' privacy, see Fox-Brewster (2016).

Information Pollution and Privacy

Information pollution, the adding of irrelevant, fake, or 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 an 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. In 2012, Switzerland's highest court ruled that Google may document residential street fronts with its Street View technology (now Google Maps), 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's 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 United States or any other country outside Europe (see Sterling 2014).

Privacy Rights and Protection

Today, virtually all US 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 US 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).

In 2016, the federal government sued Apple in order to force the company to allow the government to open the secured iPhone of an alleged terrorist. Apple refused to cooperate. The government dropped the suit after it was successful in breaking into the phone. In a similar case Amazon claimed that Alexa's speech is protected by the First Amendment, refusing to allow the government to open the files related to a murder case.

Amazon agreed to give the data only after the murder's suspect gave a permission to do so.

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, because either consumer demand for opting out is low or the value for 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, 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 and the International Association of Privacy Professionals (**iapp.org**).

Some Measures of Privacy Protection

Several government agencies, communities, and security companies specialize in privacy protection. Representative examples in the United States include the Privacy Protection (**privacyprotect.org/about-privacyprotection**), Privacy Choice (**avg.com**), and Home PC Firewall Guide (**firewallguide.com/privacy.htm**). Finally, Cagaoan et al. (2014) describe the issue of privacy awareness in e-commerce. For a complete guide to Internet privacy, anonymity, and security, see Bailey (2015).

Free Speech Online Versus Privacy Protection

Although the First Amendment of the US 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**.

For comprehensive coverage of the legal aspects of privacy vs. defamation, see Kenyon (2016). As demonstrated in a study by Gupta and Dubey (2016), privacy is related to security and trust.

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 officer 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. 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. 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 Hollywood 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: EC APPLICATION 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 **courthousenews.com/judge-tells-school-to-stop-spying** (accessed February 2017).

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 US 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.

The Future of ePrivacy

With advances in technology come more concerns regarding privacy protection. For example, Valerio (2016) suggests that there will be many changes in data privacy issues in 2016 (and probably in 2017). These changes relate to technological developments and the way people interact with technology. Brown (2016) lists the following areas for privacy in 2016: Data localization laws, IoT and ubiquitous computing, more FCC regulations, government surveillance and investigation, cybersecurity standards, big data, trans-Atlantic data transfer framework, more class action suits, and more regulations in Europe regarding data protection.

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. Comprehensive coverage of how data are collected, the users involved, and the individual rights are provided by Schneier (2016). 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 finding out where you are by knowing the location
- By reducing your phone and e-mail texts
- 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 (Chap. 6), including invisible ones
- By using a smart TV that records an individual's behavior

For the hidden battles to collect your data and control your world, see Schneier (2016).

Cookies

A popular way for a website to gather information about an individual is by using cookies. *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 United States. FTC hearings on online privacy. 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 Chap. 11, we described **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.

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 Microsoft security essentials (**support.microsoft.com/en-us/help/14210/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.

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 Chap. 13 and Online Tutorial T2, privacy advocates fear that the information stored on RFID tags or collected with them may violate an individual's privacy.

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, including

postings on social network walls. One tool that enables companies to monitor their employees is Google Location, which works in combination with a compatible device (e.g., Android, iOS).

For workplace privacy and employee monitoring, see PRC (2014).

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**.

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 (Chap. 10).
- **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.

Privacy Protection by Information Technologies

Dozens of software programs and IT policies and procedures are available to protect your privacy. Some were defined in Chap. 11. Representative examples are:

- **Platform for Privacy Preferences Project (P3P)**. Software that communicates privacy policies (described later in this chapter). This will be discussed later.
- **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 and Regulations

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

E-privacy is especially an important topic in Europe. For regulations and their impact on e-commerce, see Press (2017).

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 Wave (formerly 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. 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**.

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. During 2013 and 2014, it was found that the US government did spy on its citizens. In 2014 and 2015, 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 (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 US 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.

Note: According to Ranger (2016), the battle over privacy technologies could define the future of the Web.

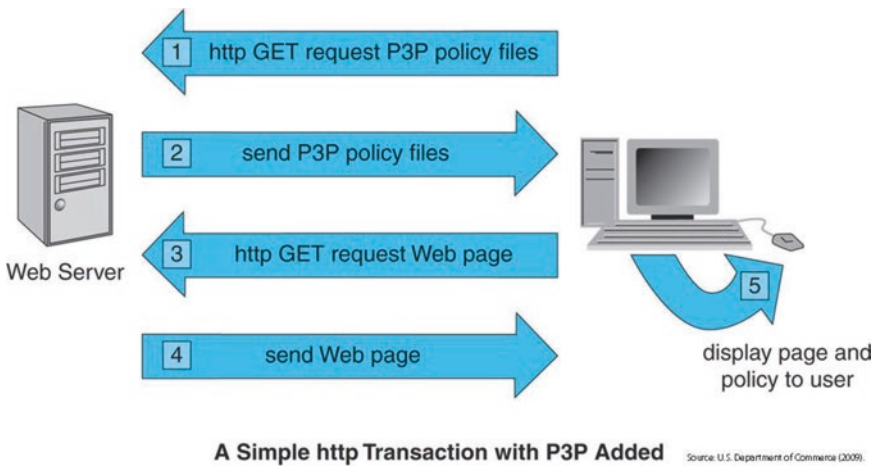

Fig. 15.1 How P3P works

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

In addition to the EC law related to privacy, piracy, patents, and other topics discussed in sections "Ethical Challenges and Guidelines," "Intellectual Property Law and Copyright Infringement," and "Privacy Rights, Protection, and Free Speech," there are many other laws related to EC. In this section we will list a sample of them and discuss two in detail.

Note that legal issues are country- or even state-dependent. For comprehensive coverage of these, see Todd and Craig (2017) and Howell (2015). 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., Todd and Craig 2017).

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 (see Phillips, et al. 2016). A major application of e-discovery is its use of finding evidence in legal cases. For details, see **en.wikipedia.org/wiki/Electronic_discovery**. For a primer on litigations, see Bennion (2016).

E-discovery frequently deals with e-mail archives. E-mail is the prime target of e-discovery requests. E-discovery must have features such as a full-content index, keyword search, and metadata index. For e-discovery tools for healthcare issues aiding compliance and saving money, see Johnson (2016).

Note: Johnson has several other books for other industries.

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 Secret Valet (**secretvalet.com**), an automated system that sends the subscriber's personal information to another person, at a specific time, such as upon the subscriber's death. See also the password manager, PasswordBox. For more, see Ciobanu (undated). For types of e-discovery collections, see Burney (2016).

EDRM

According to Duke Law School, EDRM is a community of e-discovery and legal professionals who create practical resources to improve e-discovery and information governance. The technology is expected to radically transform litigation and the legal profession. EDRM members collaboratively develop vital frameworks, standards, educational tools, and other resources to guide the adoption and use of e-discovery technologies (see **edrm.net/about-us**).

This model illustrates the process of e-discovery; see Fig. 15.2.

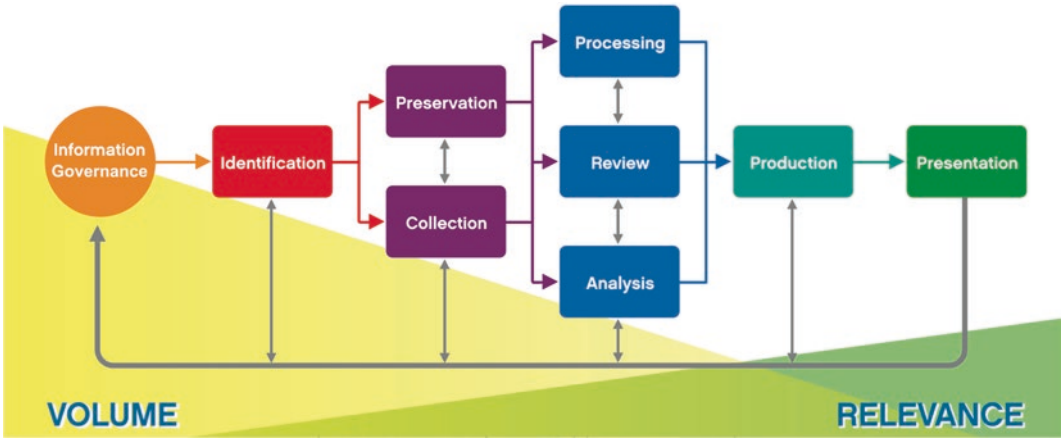

Fig. 15.2 The process of e-discovery

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**). For comprehensive coverage, see Harris (2016).

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.org** and **stopcyberbullying.org**.

For more about cyberbullying protection and Internet trolls (section "Fake Content on the Web"), see Elicksen (2015).

Note: In 2016, the First Lady Melania Trump promised to focus on combating cyberbullying if her husband won the election.

Top 10 Internet and EC Legal Issues in 2016

According to Broadcast (2016), the following are the top ten legal issues:

1. Internet privacy
2. Data security
3. The Internet of things
4. The move to mobile and BYOD
5. SaaS and cloud computing
6. Bid data
7. Internet defamation
8. The new generic top-level domains
9. Copyright in the Internet age and the DMCA
10. Online contracting and terms of service

According to Morgan (2016), the IoT introduces many legal issues related to privacy, data ownership, security, and protection of intellectual property.

A Sample of Other Issues

Here is a list of other EC legal issues:

- Disputes between companies regarding patents.
- Legalizing Internet gambling.
- Web monopoly by giant companies (e.g., Google, Tencent in China).
- Use of social media sites for prostitution.
- Regulating online P2P money lending.
- Who has the right to sell?
- Online advertising compliance.
- Laws regarding data protection.
- Refunding policy.

Note: There are many other legal cases related to the Internet and EC. For example, Amazon's e-book business was investigated in 2015/2016 by the European Antitrust regulators (Scott 2015).

Protection is needed not only for buying goods but also from buying services. For a comprehensive collection of legal issues to consider before you open a B2C store, see Guide (2016).

Drivers of EC and Internet Laws

The following are the major drivers of EC and Internet laws:

- Cars as computers
- The Internet of things
- Government policies
- Cracking down on offensive content
- Stronger geographic borders on the Internet
- The ad blocker war
- Who is considered an employee online
- The copyright and piracy battles

We add to the issue of fake information and Internet trolls (see section "Fake Content on the Web").

A Final Note

To illustrate the diversity of the legal issues related to the Internet and EC, consider the following incidents:

According to AP News (2016), a Georgia couple (the Maynards) is suing Snapchat and the driver of a car that crashed into their car (Ms. McGee). "The lawsuit says that in September [2015], McGee was driving down a highway south of Atlanta using a Snapchat filter that places the rate at which a vehicle is traveling over an image. It says McGee was trying to reach 100 miles an hour in her car, which struck the Maynards' car, sending it across the left lane and into an embankment." Mr. Maynard suffered brain damage.

According to Smith (2017), a French man sued Uber for $48 million (USD) for allegedly breaking up his marriage. A notification bug in an Uber app allowed his wife to spy on him without his knowledge. The husband used his wife's iPhone to order Uber trips and then signed out. However, a computer bug made the notifications for the husband's account arriving to the wife's iPhone. As a result, the wife figured out that the husband was lying about certain trips. In addition, she saw all of the Uber drivers' information. Therefore, his "working late at the office" excuse was not good anymore when the wife found out what he was doing late in the day. Therefore, the wife divorced the man who blamed Uber.

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?
4. Enter **hg.org/busecommerce.html**. How do they relate to this section?

15.5 FAKE CONTENT ON THE WEB

The opening case illustrated to us how fake content is produced and spread on the Web. The problem received considerable attention in November 2016. Unfortunately, fake news is only one type of fake content. In this section, we will describe some of the other types as well as some possible solutions.

Fake News

A major type of online fake content is fake news. Fake news can be intentionally set or, as shown in the opening case, be unintentional. In addition to one-time fake news, there are fake news sites. Many claim that the Internet is loosening society's grip on the truth (e.g., Manjoo 2016). Tim Cook, of Apple, said that, "fake news is killing people's minds." Fake news can hurt individuals and/or organizations. One problem is that the fake news spreads very fast. In addition, using bots (Chap. 7), it is possible to send, for example, a huge number of tweets and people can post news on multiple social networks, at once. For how this is done in politics (e.g., 2016 election), see Mello, Jr. (2016a). For a comprehensive discussion, see Shane (2017).

Google and Facebook Actions

Tucker's opening case resulted in continued criticism for companies not addressing the fake news problem. Google responded by banning websites that peddle fake news from using its online advertising service. Facebook changed its Facebook Audience Network policy, saying that it will not display ads in sites that show misleading or illegal content. The Facebook Audience Network policy covers all fake news sites.

Facebook has been at the epicenter of the turmoil. Some accused it for trying to influence voters to vote for President Trump. For details, see Wingfield et al. (2016).

Other Fake Content Types and Activities on the Internet

- In Chap. 11, we presented several methods of fraud involving fake content, products, and sites. Fake sites are used extensively to trick people into providing private information (social engineering). Goel (2016) reported that Russian cyberforgers stole millions of dollars each day with fake sites. They tricked advertisers to pay for video ads on fake sites (the ads were never watched).
- Plummer (2016a) describes the problem of celebrities that are being attacked by Internet trolls.
- Viner (2016) describes a fake news situation that started in a newspaper, but then went viral on the Internet. (This is similar to the opening case, where fake news was spread both online and offline.)
- Fake reviews are a common problem discussed in Chaps. 8 and 14.
- Amazon.com is trying to fight fake reviews by going after both individuals and website operators. Amazon was able to legally shut down such websites. For details, see Editorial Board (2016).

Internet Trolls

According to Moreau (2016), "an **Internet troll** is a member of an online social community who deliberately tries to disrupt, attack, offend, or generally cause trouble within the community by posting certain comments, photos, videos, graphic interchange formats (GIFs) or some other form of online content.

You can find trolls all over the Internet—on message boards, in your YouTube video comments, on Facebook, on dating sites, in blog comment sections and everywhere else that has an open area where people can freely post to express their thoughts and opinions." A common platform for trolling is Twitter. Trolls have been around since 2010. They do appear in a variety of forms.

Note: Trolls in Internet slang refers to Internet trolls (which are people) or sometimes to the content produced by the Internet trolls themselves. For an overview, see **lifewire.com/what-is-internet-trolling-3485891**.

Types of Trolls

Moreau (2016) lists the following types of trolls:

1. The grammar and spell check troll
2. The forever offended troll
3. The show off, know-it-all troll
4. The one word only troll
5. The exaggeration troll
6. The off-topic troll
7. The insult troll
8. The persistent troll

There are many other classifications of trolls.

Controlling Trolls

It is not easy to control trolls. Moreau (2016) observed that "controlling them can be difficult when there a lot of community members, but the most common ways to get rid of them includes either banning/blocking individual user accounts (and sometime IP addresses altogether) or closing off comment sections entirely on a blog post, video page, or topic thread." Roberts (2017a, b), who was attacked by trolls, describes an ongoing project at Google that tries to use an AI-based tool called a Jigsaw to control trolls, even those generated by bot.

Difficulties Controlling Fake Content

It is not easy to control fake content due to variety of shapes it takes and the way that the fake content is structured. Here are some related issues:

- Even the clever students of Stanford University have had trouble judging the credibility of information published online (Donald 2016).
- Lies spread much faster than truths, as shown in a study of viral content (Silverman 2015).
- The plague of fake content is getting worse.

Despite the difficulties, there are many possible solutions.

Controlling Fake Content

Many experts make suggestions about how to control fake content. Here are some:

- Kiely and Robertson (2016) provide suggestions on how to spot fake content.
- Kercher (2016) provides a list of fake and misleading news sites to watch videos on AI and their potential role in controlling fake news.
- Stelter (2016) provides suggestions on how to protect against fake news.
- Nicholas (2016) provides advice regarding finding out if an EC website is legitimate.

What to Do When There Is Fake Content About Your Company?

Several years ago, employees of Domino's Pizza in Conover, NC, created five fake videos showing unclean food preparation including food contamination practices at the company. The videos featured Domino's employees in the company's uniform and were posted on YouTube. The videos went viral and within 6 h were featured on a consumer advocacy site (**consumerist.com**). The videos were seen by millions of viewers by the time the company found about them. Damage control worked fast; YouTube removed the videos. The employees lost their jobs and faced criminal charges. However, the reputation of Domino's was damaged. In Chap. 10, we described the issue of reputation management in general. A question was raised by Alaimo (2017): "what to do when the fake news [and content] is about your company[?]" Alaimo reports that "in December 2016, a

28-year-old man drove 6 h to a Washington, D.C., pizza parlor and fired a rifle after reading fake news claiming that Hillary Clinton was leading a child sex slavery operation there" (at the Pizza Parlor). Alaimo suggests that companies plan for and address the possibility of fake content against their businesses. Specific suggested actions are:

- Communicate values in advance.
- Use employees as advocates.
- Do not inadvertently fund nonmainstream new sites.
- Write responses in advance (response time must be very fast).
- Choose your battles.
- Consider legal action (like Domino's did).

Tips for Analyzing and Dealing with Various Types of Fake News

Zimdars (2016) provides a huge list of tips and creative comments to handle the situation. Here we provide only some.

- "Avoid websites that end in 'lo' ex: Newslo. These sites take pieces of accurate information and then packaging that information with other false or misleading 'facts' (sometimes for the purposes of satire or comedy).
- Watch out for common news websites that end in 'com.co' as they are often fake versions of real news sources (remember: this is also the domain for Colombia!)
- Watch out if known/reputable news sites are not also reporting on the story. Sometimes lack of coverage is the result of corporate media bias and other factors, but there should typically be more than one source reporting on a topic or event.
- Odd domain names generally equal odd and rarely truthful news.
- Lack of author attribution may, but not always, signify that the news story is suspect and requires verification.
- Some news organizations are also letting bloggers post under the banner of particular news brands; however, many of these posts do not go through the same editing process (ex: BuzzFeed Community Posts, Kinja blogs, *Forbes* blogs).
- Check the 'About Us' tab on websites or look up the website on Snopes or Wikipedia for more information about the source.
- Bad Web design and use of ALL CAPS can also be a sign that the source you're looking at should be verified and/or read in conjunction with other sources.
- If the story makes you REALLY ANGRY it's probably a good idea to keep reading about the topic via other sources to make sure the story you read wasn't purposefully trying to make you angry (with potentially misleading or false information) in order to generate shares and ad revenue. Thanks to ED Brayton for this tip!
- If the website you're reading encourages you to DOX individuals, it's unlikely to be a legitimate source of news.
- It's always best to read multiple sources of information to get a variety of viewpoints and media frames. Sources such as *The Daily Kos*, *The Huffington Post*, and Fox News vacillate between providing important, legitimate, problematic, and/or hyperbolic news coverage, requiring readers and viewers to verify and contextualize information with other sources."
- For more tips on analyzing the credibility and reliability of sources, please check out School of Library Journal (they also provide an extensive list of media literacy resources) and the Digital Resource Center.

SECTION 15.5 REVIEW QUESTIONS

1. Define fake news and explain the potential damage.
2. What are Google and Facebook doing to combat the problem?
3. List all major types of fake content.
4. Define Internet trolls and list several of their variations.
5. How can one control Internet trolls?
6. Why is it difficult to control fake content on the Web?
7. List some solutions to control fake content.
8. Describe the problem for enterprises and list some solutions.

15.6 PUBLIC POLICY, TAXATION, AND POLITICAL ENVIRONMENTS

Public policy rules and actions made by elected officials and regulators around the world can impact how EC is conducted. Stay informed of the policy issues facing the EC community and the opportunities to engage your government officials. 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 all Internet 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. For more on net neutrality and its impact, see Gross (2014) and Sommer (2014). Note that implementation of net neutrality is not simple; it involves Web companies, lawmakers and government agencies, fiber-optic 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 April 2014, the FCC announced new rules that might have abolished 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!

Since 2014, there has been an ongoing battle and pressures on the FCC by those who are for and against changes in the net neutrality regulation concept. The Trump administration may reverse the situation. See Reilly (2017) and Breland (2017) for details.

The international implementation of EC taxation is very complicated due to each country's regulations. The trend is to move to destination-based taxes. For details, see Schwanke (2016).

Taxation of EC Transactions in the United States

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 **libertytax.com/online/taxbrain/**. One development was the 1998 Internet Tax Freedom Act that placed a moratorium on special taxation on the Internet for 1 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 US Senate passed the Marketplace Fairness Act (**marketplacefairness.org**), a law that will require all online and catalog sellers in the United States 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.

By 2017, Amazon.com agreed to collect tax in some states (e.g., California) but not in others (e.g., Hawaii).

According to Lowry and Lunder (2016), "in certain instances, the taxes are not included in the online prices due to constitutional limitations on the states' authority to require that out-of-state sellers collect them.

Two public policy issues are typically raised concerning the effects of current law.

First, differential tax treatment of similar items creates an economic distortion that affects producer and consumer decisions. Remote sellers may locate operations based on potential sales and use tax consequences, not traditional market factors. Additionally, consumers may choose out-of-state vendors to evade taxes.

Second, current law limits the ability for state and local government to require the collection and use of taxes on goods and services that would otherwise be subject to such collection if sold by a local vendor. This is particularly a significant issue for states that rely relatively more on general sales tax as part of their overall revenue mix."

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 US 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 United States 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. For examples and infographics of censorship in countries around the world, see **en.wikipedia.org/wiki/Internet_censorship_by_country**.

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 US federal and state governments are attempting to close this gap within the United States 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 nonprofit 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 2017, Amazon.com offered its cheapest Fire tablet for $39.00.

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 developing countries. For a list of potential benefits, see Table 15.3. For example, one benefit of working from home is that people who live in the suburbs can save one to 2 h of time per day by not having to commute to work (Enviro Boys 2010).

Table 15.3 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
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

Example: Ascend One Corporation

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 h 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.

Does EC Increase Unemployment?

In January 2017, Amazon.com opened its first physical store (Amazon Go) without cashiers (see Chap. 7). The question is: "Will Amazon Go replace jobs?" While the specific issue is still debatable, the more general question is "will robots take our jobs?" or in general: Where and when can machines replace humans?

Automation and Job Losses

The arguments that automation takes jobs started with the *Industrial Revolution*. What is really happening is difficult to assess. While certain jobs disappear, others are created. Therefore, proponents of automation believe that there is actually total job increase. Opponents say the opposite. The problem is that today the pace of automation is much faster than in the past and the magnitude is much broad. Let us see the implication in EC-related fields, especially robotics.

The Current Automation Impact

If all merchants will replace their checkout employees with robots, there will be millions of additional unemployed people in the world. Foxcom, an iPhone manufacturer in Taiwan, plans to replace almost all of their employees with robots (Statt 2016). The company itself produces 10,000 robots each year for this purpose. A study done in the United Kingdom (cited in Chap. 7) predicts that robots will take 50% of all jobs in about 10 years. Egan (2015) reports that robots already threaten the following jobs: marketers, toll booth operators and cashiers, customer service, financial brokers, journalists, lawyers, and phone workers. Note that automation may affect portions of almost all jobs to a greater or lesser degree. According to Hiner (2016), about 80% of IT jobs will be eliminated by software (i.e., software agents in AI).

According to Manyika et al. (2017), automation is spreading because "robots and computers can only perform a range of routine physical work activities better and more cheaply than humans, but they are also increasingly capable of accomplishing activities that include cognitive capabilities once considered too difficult to automate successfully, such as making tacit judgments, sensing emotion, or even driving. Automation will change the daily work activities of everyone, from miners and landscapers to commercial bankers, fashion designers, welders, and CEOs." When all of this is going to happen will depend on many factors, primarily on human-computer interaction and collaboration.

Amazon.com and other e-tailers are trying to automate operations to stay competitive. Inventions in the IoT, for example, will result in automatic ordering. The more inventions are made, the more competitive advantage of EC against traditional retailers.

So What Can Be Done?

Given that EC is unstoppable, replacement of humans by machines will accelerate. The solutions depend on organizational, political, social, economic, training ability, and other factors. This issue is outside the boundaries of this book.

Note: In February 2017, Bill Gates suggested that industrial robots should be taxed like workers. The tax should be imposed both on manufacturers of robots and on users of the robots. The collected money will be used for retraining displaced employees (see details in Morris 2017).

Green EC and IT

There are many opportunities to make EC green, and here we present some 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.

Table 15.4 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 February 2017)

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 15.4.

For practices, see "Cooling Data Center Costs" in *Baseline*, August 13, 2010 (available online at **baselinemag.com/c/a/IT-Management/Cooling-Data-Center-Costs-368334** (accessed February 2017).

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 excess 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.

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 an 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 (2008).

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.

Example 1: Wells Fargo

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 8000 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). It 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

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 **www.gov.uk/government/organisations/national-measurement-and-regulation-office**).

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, rates 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 healthcare 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 safety both 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 ten 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 1000 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 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 United States) have begun prevention and reeducation 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 healthcare. 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 healthcare (see Chap. 6). Intelligent systems facilitate medical diagnoses. Healthcare advice can be provided from a distance. Finally, intelligent hospitals, doctors, and other healthcare 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.

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 to 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 overall direction of the field: full speed ahead! Companies such as Amazon.com, eBay, Alibaba Group, Priceline, and Newegg.com are growing rapidly.

EC will grow all over the globe.

Some Key Factors for the Future of E-Commerce

The future of EC depends on how many factors will have impacts in the future. TrueShip (2016) made the following ten predictions:

1. Amazon will become bigger than Walmart.
2. EC will be 10% of all retail.
3. Facebook will overtake YouTube for branding.
4. Emotionally driven shopping will become a standard.
5. In-store pickup will save the large retail chains (as in the case of Target).
6. Competitors will create Amazon Prime-like shopping portals.
7. Drones will start to deliver.
8. Marketplaces for selling goods will become very popular.
9. Mobile shopping will overtake desktop shopping. It may be required for survival.
10. Hassle-free returns will be mainstreams in EC.

Other factors cited are:

- The shape of net neutrality.
- The extent of developing easy-to-shop and smart applications (e.g., Google's DeepMind).
- The competition between EC giants (e.g., Amazon, Alibaba) and large retailers that are going "brick-and-click" (e.g., Walmart) is intensifying.
- Multichannel shopping is increasing.
- Beacon technology integrates online and offline systems.
- Huge images and videos deliver stunning homepages.
- Real-time analytics become the norm.

For comprehensive reports, see Knight (2016), McCafferty (2016a), and Zorzini (2015).

New Trends That Are Shaping the Future of B2C

According to Smeaton (2016), the following are the six trends that are shaping the future of B2C e-commerce:

1. New EC product categories will take over computer and consumer electronics.
2. Developing countries will become the largest EC markets (mostly Asia Pacific, China, Indonesia, and India).
3. Will Amazon and Alibaba keep up against new EC trends? Yes, but niche players will play a leading role in certain market sectors.
4. Marketplaces vs. direct websites: which business model is the future of EC?
5. Is the future of EC mobile? Yes, but slowly, new technologies make it easier to shop online.
6. Product visualization will become a crucial EC trend, especially for more complicated products.

The B2C Road to 2016

Ovum (2016) outlined the road of B2C EC for the year 2016. In their free e-book, the company talks about the following seven major categories:

1. Consumers of the future.
2. Online retailing is growing more than three times faster than regular retailing.
3. The blurring boundaries of retail and e-tail.
4. Mobile-centric retail experience.
5. Context is King.
6. Key technologies that will shape retail.
7. How to prepare for the future (a guide).

The Future of B2B

B2B is much larger than B2C, but the ratio is getting smaller. From a 6:1 ratio in the 1990s, the ratio will be only 2:1 in a few years. Columbus (2016) provides the following predictions:

- B2B EC will top $1.1 billion, accounting for over 12% of all B2B commerce. (B2C is under 8% of all B2C.)
- New cloud-based platforms are increasing, selling speed, scale, and simplicity.
- There is a conversion of B2B and B2C.

Zorzini's List of Trends for 2016 and Beyond

Zorzini (2015) made the following predictions:

1. Multichannel shopping may make or break your business (namely, you better have one).
2. Connecting with customers through social media is not enough.
3. An integration of online and offline will be done with beacon technology.

4. The pop-up may make an effective comeback (or may not).
5. Huge images and videos deliver stunning homepages.
6. The virtual salesforce becomes highly implemented.
7. Mobile is required for survival.
8. Real-time analytics become the norm.

Other Predictions

Other predictions for 2017 and beyond are:

1. E-commerce competition will increase.
2. President Trump could be good for e-tailers.
3. M-commerce will outperform desktop commerce.
4. EC delivery will get better and faster (Chap. 13).
5. The payment landscape will evolve (Chap. 11).
6. For more predictions, see DeMarco (2016).

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).

The consumers prefer to have the choice where to shop. As of 2015, consumers love the combination of ordering online and picking up the merchandise in the physical store. Some believe that such a combination saves retailers from extinction (e.g., see Chap. 13 and Douglas 2014).

M-Commerce

There is almost a 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. For details, see Chap. 6 and Kemp (2016).

With the advances of the IoT, we see many increasing applications (e.g., see the closing case in Chap. 7).

Social Commerce

Recently, the use of mobile social networks has been accelerating. The increasing number of new wireless Web 2.0 services has assisted many social networks to go wireless, enabling more interactions between people. Nielsen's September 2012 release of its *Social Media Report* indicated that 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 with time.

Social commerce is growing rapidly on Facebook, Twitter, Google, Instagram, and many other companies. Mobile advertising and promotions are major areas of growth. For details, see Turban et al. (2016) and Kemp (2016).

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 (based on Scollay (2015) and McCafferty (2016a)):

- 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 (will become a platform to m-commerce)
- Possibility of free Internet access 3D printing will grow (Chap. 13).
- Wide applications of AI technologies.
- Using augmented reality (e.g., in order fulfillment; see DHL 2015).
- Going further into the IoT.
- Next generation data centers.
- The proliferation of AI applications (also see Adhikari 2016a, b).

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; see Constantin (2017).
- **Lack of agreement on 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. The issue is still in limbo.
- **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.

Consumer Behavior

The future of B2C EC depends on consumer behavior. The young people that are more computer-oriented will buy more online, especially if they can save time and money. The consumers will interact with AI apps and probably love them. For more on the consumer of the future, see Ovum (2016).

Conclusion

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.

For a 537 slideshow, see "Digital in 2016" at **slideshare.net/wearesocialsg/digital-in-2016** by Kemp (2016).

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 min) at **youtube.com/watch?v=mJtw1027FYs**
2. "Future of E-Commerce: Trends, Challenges, and Opportunities for Telecom and the Mobile Industry" (7:41 min) at **youtube.com/watch?v=wCZXif3MUEw**

Here are two coming applications of EC. They were taken from 10eCommerce (2017), **10ecommercetrends.com** (accessed February 2017).

L'Oréal of Paris

"L'Oréal Paris has designed five diagnostic tools: skincare, cosmetics (face and eyes), haircare, and hair color. These beauty diagnostics, typically operated on a mobile device, allow consumers to 'try on' different shades of make-up, 'scan' their hair color, etc. Not only can consumers use these tools to play with different looks in real time, but the data collected during each session allows for an unprecedented level of personalization of communications and interactions, not to mention ultra-customized discount coupons, which can have a major influence on purchasing decision."

Chatbots

According to L'Oréal business trends: "In 2017, many consumers will have their first interaction with a chatbot, a fully automated chat agent that will answer their questions and act as the first point of contact with the brand. A chatbot increases the number of platforms on which a brand can transact by offering guided, interactive browsing at all times.

Chatbots will soon become as commonplace as automated phone systems, only much more interactive and interesting. At the same time, store sales staff will become more important than ever, as they'll be increasingly involved in the online experience.

What are the potential impacts of a chatbot on e-commerce?

Live chat users spend an average of 5%–30% more.

The buyer conversion rate is 5 to 10 times higher following a chat session."

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. In addition, companies need a privacy policy.
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. Companies like IBM have patents for sale.
5. **How can you handle fake news and information about the company and its products and services?** Large companies need a reputation management strategy. Soon AI programs will be able to monitor all the material about your company. Watch for a possibility of unhappy employees that may generate fake content about the company in all types of media including videos and tweeting.
6. **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.
7. **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 remain 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. **Fake content and possible solutions.** Highlighted by fake news during the 2016 presidential election, the topic of fake content took a central stage in comments, opinions, and debate in late 2016 and 2017. While the problem is not new, fake content was considered a second priority issue until November 2016. In addition to fake websites and so forth, suggestions of how to deal with the problem depend on the types of fake content. Educating the public is important, but taking legal action against violators can be effective.
5. **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.
6. **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).
7. **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
Copyright
Copyright infringement
Cyberbullying
Digital divide
Digital rights management (DRM)
Electronic discovery (e-discovery)
Electronic Product Environmental Assessment Tool (EPEAT)
Ethics
Fair use
Green computing
Green IT
Intellectual property (IP)
Intellectual property law
Internet censorship
Internet troll
Net neutrality
Opt-in
Opt-out
Patent
Platform for Privacy Preferences Project (P3P)
Spyware
Telecommuting

DISCUSSION QUESTIONS

1. What can EC websites and social networks do to control fake content?
2. Privacy is the right to be left alone and free of unreasonable personal intrusions. What are some intrusions that you consider "unreasonable" in e-commerce?
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, etc.) 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. Cyber Promotions, 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. Cyber Promotions is no longer in business.
9. Discuss the different types of fake content on the Web.

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 US 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 have converted already or 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 US 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. In 2017, Bill Gates suggested that taxes should be put on robots and the collected money used for retraining people displaced by robots. Many disagree. Debate the issue.
6. Facebook and other Web networks should fact-check the content published by others on their websites. Debate the issue.
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 Telecommunications 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 min before and 90 min 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: Are privacy standards strict enough to protect electronic health records?
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. It was suggested to tax robots if they take American jobs. Debate the issue.

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 ten initiatives and describe each briefly.
4. Enter **defamationremovalattorneysblog.com/category/other-internet-law-issues** and find five recent posts dealing with fake content. Summarize them. What lessons did you learn?
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 **legalcompliance.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 **econsultancy.com** and find five posts related to the topics of this chapter. Summarize.
9. Enter **wispa.org** and similar organizations that represent the ISP industry. Identify the various initiatives they have undertaken regarding topics discussed in this chapter. Write a report.

TEAM ASSIGNMENTS AND PROJECTS

1. Assignment for the Opening Case
   Read the opening case and answer the following questions:

   (a) What made the initial tweet go viral so quickly?
   (b) Why does fake news sometimes spread faster than true stories?
   (c) How does fake news relate to doing business on the Internet?
   (d) What should Mr. Tucker have done after he saw the buses that could have prevented this incident?

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. Is it 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 canceled 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.
7. The new technologies will displace many employees. Research the issue and write a report.

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 not to 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, which made 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 1-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 US 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's 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. 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).

According to Plummer (2016b), "Having returned from its latest exile, The Pirate Bay now is using the Torrents Time plugin to deliver an illegal answer to Netflix. With the plugin installed on a Mac or PC, users can click the new 'Stream It!' button to access a wealth of movies an TV shows without paying a cent to the copyright holders.

Once the plugin has found enough peers, it can stream content without having to buffer—and peer acquisition takes just seconds." Finally, it looks as if The Pirate Bay is vying to become the world's largest streaming site.

Note: Whether pirated content is streamed or downloaded, accessing it is illegal in the United States and many other countries.

The Pirate Bay now uses many proxy sites and torrents. It is well and alive (Protalinski 2016).

Note. In February 2017 a court made the Pirate Bay illegal in Sweden, but OK in other countries.

Discussion

The Pirate Bay is one of a multitude of websites specializing in pirated and counterfeit content. The Pirate Bay does not host content, in contrast to sites, which allows people to upload videos, including 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, which is more complicated.

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

Sources: Based on Stone (2011), Plummer (2016b), Protalinski (2016), and **medlibrary.org** (accessed February 2017).

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 TPB's website.

REFERENCES

10ecommerce. "10 E-Commerce Trends for 2017. (2017) **10ecommercetrends.com** (accessed February 2017).

Adhikari, R. "Facebook Videos Explain AI in a Nutshell." *TechNewsWorld*, December 5, 2016a. **technewsworld.com/story/84135.html** (accessed February 2017).

Adhikari, R. "Privacy Concerns Curb Online Commerce, Communication." *E-Commerce Times*, May 17, 2016b. **ecommercetimes.com/story/83509.html** (accessed February 2017).

Alaimo, K. "When the Fake News Is About Your Company." *Bloomberg View*, February, 10, 2017. **bloomberg.com/view/articles/2017-02-10/when-the-fake-news-is-about-your-company** (accessed February 2017).

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.

Angwin, J. *Dragnet Nation: A Quest for Privacy, Security, and Freedom in a World of Relentless Surveillance*. New York: Times Books, 2015.

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 February 2017).

AP News. "Georgia Couple Sues Snapchat Over Car Crash." *AP.org*, April 28, 2016. **bigstory.ap.org/article/b67303bb20a945aeb203d986c-1d09a3e/georgia-couple-sues-snapchat-over-car-crash** .(accessed February 2017).

Ascharya, K. "Marissa Mayer and the Telecommuting Debate." March 26, 2013. **2machines.com/articles/178412.html** (accessed February 2017).

Bailey, M. *Complete Guide to Internet Privacy, Anonymity & Security*. 2nd ed. Delhi, India: Nerel Online, 2015.

Bennion, J. "E-Discovery: A Primer for Litigators." *Above the Law*, May 31, 2016.

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

Breland, A. "Net Neutrality Fix Faces Hard Sell." *The Hill*, February 11, 2017. **thehill.com/policy/technology/319051-net-neutrality-fix-faces-hard-sell** (accessed February 2017).

Broadcast. "Top Ten Internet Legal Issues, Including Social Media and Employee/Employer Issues." Federal Bar Association, September 26, 2016. **federalbarcle.org/product/top-ten-internet-legal-issues-including-social-media-employeeemployer-issues** (accessed February 2017).

Brown, C. "Top 10 Privacy Issues to Watch This Year." *Law360*, January 7, 2016. **law360.com/articles/743826/top-10-privacy-issues-to-watch-this-year** (accessed February 2017).

Burney, B. "Social Media: A Different Type of E-Discovery Collection." *Legal Tech News*, September 6, 2016.

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 February 2017).

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 February 2017).

Columbus, L. "Predicting the Future of B2B E-Commerce." *Forbes.com*, September 12, 2016. **forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/louiscolumbus/2016/09/12/predicting-the-future-of-b2b-e-commerce/&refURL=https://www.google.com/&referrer=https://www.google.com** .(accessed February 2017).

Constantin, L. "Hard-to-Detect Fileless Attacks Target Banks, Other Organizations." *PC World*, February 9, 2017. **pcworld.idg.com.au/article/613963/hard-to-detect-fileless-attacks-target-banks-other-organizations** (accessed February 2017).

DeMarco, T. "7 Ecommerce Predictions for 2017." *Veinteractive.com*, December 16, 2016. **veinteractive.com/us/blog/7-ecommerce-predictions-2017** .(accessed February 2017).

DHL. "Vision Picking in the Warehouse-Augmented Reality in Logistics." *SupplyChain247*, January 29, 2015. **supplychain247.com/article/vision_picking_in_the_warehouse_augmented_reality_in_logistics** (accessed February 2017).

Donald, B. "Stanford Researchers Find Students Have Trouble Judging the Credibility of Information Online." Stanford Education, November 22, 2016. **ed.stanford.edu/news/stanford-researchers-find-students-have-trouble-judging-credibility-information-online** (accessed February 2017).

Douglas, M. "New Retail Strategies: It's a Store! It's a Site! It's a Warehouse!" Inbound Logistics, August 2014. **inboundlogistics.com/cms/article/new-retail-strategies-its-a-store-its-a-site-its-a-warehouse** (accessed February 2017).

Editorial Board. "Anonymity Is a Threat to E-Commerce." *Bloomberg View*, October 28, 2016. **bloomberg.com/view/articles/2015-10-26/amazon-s-case-against-fake-reviews-is-strong** (accessed February 2017).

Egan, M. "Robots Threaten These 8 Jobs." CNN News, May 13, 2015. **money.cnn.com/2015/05/13/news/economy/robots-threaten-jobs-unemployment** (accessed February 2017).

Elicksen, D. *Take Back the Internet: Empower Yourself Against Cyberbullies and Internet Trolls*, Kindle edition. Seattle, WA: Amazon Digital Services, 2015.

EMC. "Infographic: Digital Privacy – A World of Complex Paradoxes." *Enterprise Innovation*, July 7 2014. **enterpriseinnovation.net/infographic/infographic-digital-privacy-world-complex-paradoxes** (accessed February 2017).

Enviro Boys. "Is Telecommuting on the Rise?" November 14, 2010. **enviroboys88.blogspot.com/2010/11/telecommuting-on-rise.html** (accessed February 2017).

Fox-Brewster, T. "Facebook Is Playing Games with Your Privacy and There's Nothing You Can Do About It." *Forbes.com*, June 29, 2016. **forbes.com/forbes/welcome/?toURL=https://www.forbes.com/sites/thomasbrewster/2016/06/29/facebook-location-tracking-friend-games/** .(accessed February 2017).

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 February 2017).

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

Goel, V. "Russian Cyberforgers Steal Millions a Day with Fake Sites." *The New York Times*, December 20, 2016. **nytimes.com/2016/12/20/technology/forgers-use-fake-web-users-to-steal-real-ad-revenue.html** (accessed February 2017).

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 February 2017).

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 February 2017).

Gupta, P., and A. Dubey. "E-Commerce – Study of Privacy, Trust, and Security from Consumer's Perspective." *International Journal of Computer Science and Mobile Computing*, Vol. 5, Issue 6, June 6, 2016, 224–.232. **ijcsmc.com/docs/papers/June2016/V5I6201647.pdf** (accessed February 2017).

Guide. "EC Legal Considerations Before You Launch Your Store." *The Legal Side*, 2016. **ecommerceguide.com/guides/ecommerce-legals** (accessed February 2017).

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

Harris, B. C. *Cyberbully (Society of Spies)*, Volume 1″ North Charleston, SC: CreateSpace Independent Publishing Platform, 2016.

Hiner, J. "Video: Vinod Khosla Predicts 80% of IT Jobs Will be Eliminated by Software." *TechRepublic.com*, November 10, 2016. **techrepublic.com/article/video-vinod-khosla-predicts-80-of-it-jobs-will-be-eliminated-by-software** .(accessed February 2017).

Howell, R. F. "E-Commerce's Hidden Legal Issues." *The National Law Review*, May 16, 2015.

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

Instagram. "Artist Richard Prince Made $90,000 by Selling Someone's Instagram Photo Without Permission." *First Post*, May 26, 2015.

Johnson, A. *E-Discovery Nuts and Bolts: The Essentials of E-Discovery for Healthcare Professionals*. North Charleston, SC: CreateSpace Independent Publishing Platform, 2016.

Kankanala, K.C. *Social Media and IP: Social Media, Intellectual Property and Business (Intellectual Property Basics for Business Book 4)*. Kindle Edition, Seattle, WA: Amazon Digital Services, 2015.

Kemp, S. "Digital in 2016." *Wearesocial*, January 27, 2016. **wearesocial.com/uk/special-reports/digital-in-2016** (accessed February 2017).

Kenyon, A. T. *Comparative Defamation and Privacy Law (Cambridge Intellectual Property and Information Law).* New York: NY: Cambridge University Press, 2016.

Kiely, E., and L. Robertson. "How to Spot Fake News." FactCheck.org, November 18, 2016. **factcheck.org/2016/11/how-to-spot-fake-news** .(accessed February 2017).

Kercher, M. M. "An Extremely Helpful List of Fake and Misleading News Sites to Watch Out For." *NewYorkMag.com*, November 15, 2016. **nymag.com/selectall/2016/11/fake-facebook-news-sites-to-avoid.html** .(accessed February 2017).

Knight, K. "Report: Timeliness Key for Ecommerce." *BizReport*, January 28, 2016.

Leggatt, H. "Online Privacy Real Concern for 90% of U.S. Internet Users." *BizReport,* February 14, 2012. **bizreport.com/2012/02/90-percent-of-online-adults-worry-about-their-online-privacy.html** (accessed February 2017).

Lewis, M. "Ethical Issues Relating to E-commerce." *LinkedIn.com*, June 5, 2014. linkedin.com/pulse/20140605220127-310310-ethical-issues-relating-to-e-commerce (accessed August 2017).

Lowry, S., and E. K. Lunder. "Internet Sales and State Taxes: Policy Issues." CRS Insight, December 1, 2016. **fas.org/sgp/crs/misc/IN10418.pdf** (accessed February 2017).

Lunka, R. "Ethical Issues in E-Commerce: Are You Violating Any of Them?" *Nchannel.com*, April 21, 2015. **nchannel.com/blog/ethical-issues-in-ecommerce** .(accessed February 2017).

Maheshwari, S. "How Fake News Goes Viral: A Case Study." *The New York Times*, November 20, 2016. **nytimes.com/2016/11/20/business/media/how-fake-news-spreads.html?_r=0** (accessed February 2017).

Manjoo, F. "How the Internet Is Loosening Our Grip on the Truth." *The New York Times*, November 3, 2016. **nytimes.com/2016/11/03/technology/how-the-internet-is-loosening-our-grip-on-the-truth.html** (accessed February 2017).

Manyika, J., M. Chui, M. Miremadi, J. Bughin, K. George, P. Willmott, and M. Dewhurst "Harnessing Automation for a Future That Works." Report from the McKinsey Global Institute, January 2017. **mckinsey.com/global-themes/digital-disruption/harnessing-automation-for-a-future-that-works** (accessed February 2017).

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 February 2017).

McCafferty, D. "9 Significant Technology Predictions for 2016." *Baseline*, February 24, 2016a.

McCafferty, D. "Tech Distractions Are Top Productivity Killer." Baseline, July 11, 2016b. **baselinemag.com/mobility/slideshows/tech-distractions-are-top-productivity-killers.html** (accessed February 2017).

McLaughlin, K. "Oracle Wins Appeal in Google Android Suit, Court Rules It Can Copyright Java APIs." *CRN News*, May 9, 2014. **crn.com/news/applications-os/300072804/oracle-wins-appeal-in-google-android-suit-court-rules-it-can-copyright-java-APIs** (accessed February 2017).

Mello, J. P. Jr "Bot Armies Boost Candidates' Popularity on Twitter." *Technewworld.com*, October 29, 2016a. **technewsworld.com/story/84044.html** .(accessed February 2017).

Mello, J. P. Jr "Kickass Torrents Owner Faces 20-Plus Years in Stir." E-Commerce Times, July 26, 2016b. **ecommercetimes.com/story/83734.html** (accessed February 2017).

Moreau, E. "10 Types of Internet Trolls You'll Meet Online." Lifewire, Updated November 1, 2016. **lifewire.com/types-of-internet-trolls-3485894** (accessed February 2017).

Morgan, L. "IoT Raises New Legal Challenges for Business." Informationweek.com, January 10, 2016. **informationweek.com/iot/iot-raises-new-legal-challenges-for-business/d/d-id/1323926** .(accessed February 2017).

Morris, D. Z. "Bill Gates Says Robots Should Be Taxed Like Workers." *Venturebeat.com*, February 18, 2017. **venturebeat.com/2017/02/18/bill-gates-says-robots-should-be-taxed-like-workers** .(accessed February 2017).

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

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 February 2017).

Nicholas, M. "Naughty or Nice? Here's How to tell If an E-Commerce Website is Legit." Dashlane.com, December 6, 2016. **blog.dashlane.com/identifying-fake-ecommerce-websites** (accessed February 2017).

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 February 2017).

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 February 2017).

Ovum. "The Future of E-Commerce: The Road to 2026." Ovum, 2016. **criteo.com/media/4094/ovum-the-future-of-e-commerce-the-road-to-2026.pdf** (accessed February 2017).
Park, H. S. "Empowering Employees with Technology." *Baseline*, May 27, 2009.
Phillips, A., et al. *E-Discovery: An Introduction to Digital Evidence (with DVD), Loose-Leaf Version*. Clifton Park, NY: Delmar Cengage Learning, 2016.
Plummer, Q. "Traversing the Social Media Minefield." *Technewsworld.com*, December 9, 2016a. **technewsworld.com/story/84155.html** .(accessed February 2017).
Plummer, Q. "The Pirate Bay Is Now Streaming." *E-Commerce Times*, February 10, 2016b. **ecommercetimes.com/story/83094.html** (accessed February 2017).
Press. "New Proposal for a Regulation on ePrivacy: Pros and Cons for E-Commerce." *Ecommerce Europe,* January 11, 2017. **ecommerce-europe.eu/press-item/new-proposal-regulation-eprivacy-pros-cons-e-commerce** (accessed February 2017).
PRC. "Workplace Privacy and Employee Monitoring." (Revised May 2014). **privacyrights.org/workplace-privacy-and-employee-monitoring** (accessed February 2017).
Protalinski, E. "The Pirate Bay Now Uses Torrents Time to Let You Stream All Its Movies and TV Shows." *Venturebeat.com*, February 5, 2016.
Ranger, S. "The Undercover War on Your Internet Secrets: How Online Surveillance Cracked Our Trust in the Web." *Tech Republic*, February 10, 2016.
Reilly, P. "Net Neutrality: A Top Target for Trump's FCC?" *Christian Science Monitor*, January 21, 2017. **csmonitor.com/Technology/2017/0121/Net-neutrality-A-top-target-for-Trump-s-FCC** (accessed February 2017).
Roberts, J. J. "Can Artificial Intelligence Silence Internet Trolls." *Fortune.com*, February 1, 2017a. **fortune.com/2017/01/23/jigsaw-google-internet-trolls** .(accessed February 2017).
Roberts, P. C. "A Case in the Creation of False News: Delegitimize Trump's Presidency. *GlobalReseach.org*, January 6, 2017b. **globalresearch.ca/a-case-study-in-the-creation-of-false-news/5567103** .(accessed February 2017).
Samson, T. "GreenNet 2010: Google Shares Its Green Data Center Secrets." *InfoWorld*, April 29, 2010.
Scott, G. *Internet Book Piracy: The Fight to Protect Authors, Publishers, and Our Culture*. New York: Allworth Press, 2016.
Schneier, B. Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Norton and Company, 2016.
Schwanke, A. "Taxation on E-Commerce: The International Implementation." *International Tax Review*, March 2016. **internationaltaxreview.com/Article/3533682/Taxation-on-e-commerce-International-implementation.html** (accessed February 2017).
Scollay, R. "Six Business Technology Predictions for 2016." *Enterprise Innovation,* November 10, 2015. **enterpriseinnovation.net/article/six-business-technology-predictions-2016-150408718** (accessed February 2017).
Scott, M. "Amazon's E-Books Business Investigated by European Antitrust Regulators." *The New York Times*, June 12, 2015. **nytimes.com/2015/06/12/business/international/european-union-amazon-ebooks-antitrust-investigation.html** (accessed February 2017).
Shane, S. "From Headline to Photograph, a Fake News Masterpiece." *The New York Times*, January 18, 2017. **nytimes.com/2017/01/18/us/fake-news-hillary-clinton-cameron-harris.html** (accessed February 2017).
Silverman, C. "How Lies Spread Faster Than Truth: A Study of Viral Content." Mediashift.org, February 18, 2015. **mediashift.org/2015/02/how-lies-spread-faster-than-truth-a-study-of-viral-content** .(accessed February 2017).
Smeaton, C. "6 New Ecommerce Trends Shaping the Future of Online Retail." *Demo-Up video conference*, July 5, 2016. **demoup.com/blog/six-new-ecommerce-trends-shaping-the-future-online-retail** (accessed February 2017).
Smith, C. "French Man Wants $48 Million from Uber for Allegedly Breaking Up His Marriage." *BGR.com*, February 12, 2017. **bgr.com/2017/02/12/uber-iphone-notifications-bug** .(accessed February 2017).
Sommer, J. "Defending the Open Internet." *The New York Times*, May 11, 2014. **nytimes.com/2014/05/11/business/defending-the-open-internet.html** (accessed February 2017).
Statt, N. "iPhone Manufacturer Foxconn Plans to Replace Almost Every Human Worker with Robots." *The Verge*, December 30, 2016. **theverge.com/2016/12/30/14128870/foxconn-robots-automation-apple-iphone-china-manufacturing** (accessed February 2017).
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 February 2017).
Stetler, B. "The Plague of Fake News Is Getting Worse—Here's How to Protect Yourself." *CNN*, November 1, 2016. **money.cnn.com/2016/10/30/media/facebook-fake-news-plague/index.html** (accessed February 2017).
Stone, B. "Pro Sports versus the Web Pirates." February 24, 2011. **businessweek.com/magazine/content/11_10/b4218066626285.htm** (accessed February 2017).
Todd, P., and W. Craig. *E-Commerce Law*, 2nd ed. New York: Routledge, 2017.
TrueShip. "The Future of Ecommerce: 10 Predictions for 2016." January 5, 2016. **trueship.com/blog/2016/01/05/the-future-of-ecommerce-10-predictions-for-2016/#VwLle_krI2w** (accessed February 2017).
Turban, et al. *Social Commerce*, New York: Springer, 2016.
Valerio, P. "Top Data Privacy Issues to Scare You in 2016." *InformationWeek*, January 6, 2016.
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 February 2017).
Verbauwhede, L. "Intellectual Property and E-Commerce: How to Take Care of Your Business' Website." WIPO, 2015. **wipo.int/export/sites/www/sme/en/documents/pdf/business_website.pdf** (accessed February 2017).
Viner, K. "How Technology Disrupted the Truth. *The Guardian*, July 12, 2016. **theguardian.com/media/2016/jul/12/how-technology-disrupted-the-truth** (accessed February 2017).
Wingfield, N., M. Isaac, and K. Benner. "Google and Facebook Take Aim at Fake New Sites." *The New York Times*, November 14, 2016. *New York Times*. **nytimes.com/2016/11/15/technology/google-will-ban-websites-that-host-fake-news-from-using-its-ad-service.html** (accessed February 2017).
Zimdars, M. "False, Misleading, Clickbait-y, and Satirical 'News' Sources." Creative Commons, 2016. **d279m997dpfwgl.cloudfront.net/wp/2016/11/Resource-False-Misleading-Clickbait-y-and-Satirical-%E2%80%9CNews%E2%80%9D-Sources-1.pdf** (accessed February 2017).
Zorzini, C. "10 Interesting E-Commerce Trends for 2016 and Beyond." E-Commerce Platforms, December 7, 2015. **ecommerce-platforms.com/ecommerce-news/10-interesting-ecommerce-trends-for-2016-and-beyond** (accessed February 2017).