19 Electronic Commerce

Chapter Overview

Electronic Commerce Legislation

Canada's *Uniform Electronic Commerce Act*

Provincial Electronic Commerce Legislation

Contracting Online

Contract Formation

Automated Electronic Commerce

Authentication

Information Security

Jurisdiction in Electronic Commerce

Domain Names

Liability of Online Intermediaries

Internet Service Providers

Online Service Providers

P2P File-Sharing

Online Privacy

Online Consumer Protection

Objectives

After completing this chapter, you should be able to:

1. Outline the general strategies adopted in electronic commerce legislation to ensure business certainty in the online environment.

2. Define functional equivalence and its role in electronic commerce legislation.

3. State the considerations involved to ensure successful contract formation in electronic commerce.

4. Discuss the contractual issues specific to automated electronic commerce and the legislative method for correcting keystroke errors.

5. Explain the importance of authentication in online business transactions.

6. Outline the business problems arising from the domain name system.

7. Discuss the jurisdictional implications of transacting in a global medium and how to minimize exposure to liability online.

8. Describe how an online business can shield itself from intermediary liability.

9. Describe how an organization can minimize the costs and risks of privacy violations while engaged in the collection, use, or disclosure of personal information.

10. Explain how consumer protection principles can be used to promote the reputation of a business, generate goodwill, and build trusting relationships.

More and more, businesses of all types and sizes are distributing their products through various technological channels using *electronic commence*. **Electronic commerce** refers to technology-mediated business transactions. These take place across a network and usually involve the transportation of goods, services, or information—either physically or digitally—from one place to another. It is tempting to think of the Internet

when one thinks of electronic commerce, but the definition is actually much broader. It also includes, for instance, a transaction that occurs between a customer and an automated bank machine.

electronic commerce refers to technology-mediated transactions

Electronic commerce has a number of benefits. Once a system is in place, transactions become easy and affordable. Technology allows a business to reach more customers, in more places. It allows contracts to be performed more quickly. And it can reduce the expenses associated with marketing products and creating contracts. However, electronic commerce also has its costs. One such cost is uncertainty. Uncertainty causes some businesses and consumers to avoid participating in electronic commerce.

The law is a significant source of uncertainty in electronic commerce. Generally speaking, law applies to electronic commerce in the same way it applies to other business contexts. However, the basic rules of commercial law were developed many years ago, when people usually dealt face to face. Not surprisingly, existing law does not easily accommodate every aspect of the transactions that are conducted over a network. For example, unsolicited commercial e-mail—called *spam*—has caused widespread damage to businesses and individuals alike, sometimes because of wasted time and resources spent reading and filtering through spam messages, sometimes because of viruses or worms that do damage to computers and other business assets. The law in this area has struggled to address the problem. Criminal law, contract law, privacy law, tort law, and trespass law have been invoked to attempt to address spam and other countries have created entirely new laws to address spam.

1. Canada formed a task force which in May 2005 made recommendations to the government regarding ways to deal with spam. See the Task Force on Spam website at <http://e-com.ic.gc.ca/epic/internet/inecic-ceac.nsf/en/h_gv00248e.html>.

As a matter of risk management, a business that is involved in electronic commerce must be aware of potential problems. This chapter examines how the law has responded to technological changes in the business world. We begin with a survey of

recent legislation that regulates electronic commerce. We then discuss how businesses can create enforceable electronic contracts and how they can address jurisdiction issues in electronic commerce. Because jurisdictionmay be the single biggest problem encountered in electronic commerce, businesses must understand and address it. We also explore some specific issues that can arise in electronic commerce, including strategies regarding domain names, liability issues for Internet-related services, and the significance of peer-to-peer (P2P) file sharing. We conclude with an outline of business obligations and approaches to privacy and consumer protection laws.

Electronic Commerce Legislation

A defining feature of electronic commerce is that it is global—it allows business to be done around the world. It is therefore desirable to have consistent laws from place to place. If every jurisdiction had a different set of rules, it would be impossible to achieve certainty in the electronic business world. As a result, the United Nations Commission on International Trade Law (UNCITRAL) encouraged countries to create uniform legislation based on a single model—the *United Nations Model Law on Electronic Commerce*. The model law is not really a law. It does not create rights, powers, obligations, or immunities. It merely provides a *model* for the creation of a consistent set of laws. Ultimately, it is up to each government to decide how much of the model to adopt. Its goal is to remove barriers that technology may impose upon the creation of traditional commercial relationships.

2. The United Nations Model Law on Electronic Commerce: <www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce/1996Model.html>.

Canada’s *Uniform Electronic Commerce Act*

Because our Constitution states that commerce is generally a provincial matter, electronic commerce legislation has been enacted on a province-by-province basis. Still, the co-ordination of these rules was inspired on a national level. The strategy was similar to the international approach. A special working group of the Uniform Law

Conference of Canada created its own model law—the *Uniform Electronic Commerce Act* (*UECA*). Like UNCITRAL's model law, *UECA* has no legal force, but it has formed the basis for most electronic commerce laws in Canada. Some provinces have adopted all of it; others have adopted specific parts. Following this review of *UECA*, we will briefly describe how some provinces have adopted provisions different from *UECA*. However, because of the similarity between the key provisions of UECA and the actual laws adopted in each province, we will first examine *UECA*'s most important provisions in detail. In particular, we will consider:

its *scope*

the role of *consent*

the notion of a *functional equivalent*

the rules pertaining to *electronic contracts*

the rules pertaining to *sending and receiving electronic documents*

the treatment of *government documents*

3. The *Uniform Electronic Commerce Act* (*UECA*): <www.ulcc.ca/en/us/index.cfm?sec=1_&sub=1u1>.

4. J Gregory "The *Uniform Electronic Commerce Act,*" *Lex Electronica* 6(1) printemps 2000: <www.lex-electronica.org/articles/v6-1/gregory.htm>.

Scope

UECA has a broad scope. Rather than listing all of the transactions to which it applies, it lists those to which it does *not* apply. For instance, it follows UNCITRAL's model law by

specifically excluding wills and dealings in land. Those sorts of arrangements are still governed by traditional legal rules. The list of exclusions differs, however, between jurisdictions. To manage risk, it is therefore important for a business involved with electronic commerce to know which exclusions apply in every jurisdiction in which it does business.

Consent

UECA does *not* require a business to use or accept electronic documents. Parties to a particular transaction may agree that they will not use or accept electronic documents. It is meant only to facilitate electronic commerce for those people who *choose* to engage in it. It is important to realize, however, that your consent may be express or implied. The courts may decide that you consented to use *UECA* if you behave in a way that supports that inference.

Functional Equivalence

As we saw in Chapters 10 and 16, some types of contract traditionally were enforceable only if they were in writing. That is still true. *UECA*, however, recognizes that the writing requirement can sometimes be satisfied through *functional equivalence*. **Functional equivalence** identifies the essential purpose of a traditional rule and indicates how that purpose can be accomplished electronically.

functional equivalence identifies the essential purpose of a traditional rule and indicates how that purpose can be accomplished electronically

For example, some statutes that regulate the enforcement of contractual terms require certain documents to be signed. That signature is intended to demonstrate the signer's willingness to be bound by the terms. However, that same purpose may be achieved through the click of a mouse. For instance, a dialogue box may appear on a computer screen that contains a box that says, "I accept these terms." Clicking on that box may be the functional equivalent of signing a document.

5. There are many other examples. The essential function of writing is memory, which can also be satisfied by electronic information, as long as it is accessible for future reference. See Case Brief 19.1.

Electronic Contracts

UECA does more than permit functional equivalents. It even allows transactions to be achieved, without human intervention, by computer programs. For instance, contracts may be created by shopping bots and other automated electronic devices.

Sending and Receiving Electronic Documents

UECA also facilitates electronic commerce by removing uncertainty about *where* and *when* a message is sent or received.

A message is deemed to be sent from the sender's place of business and received at the recipient's place of business. Suppose your place of business is in Alberta, but you send a message through your Internet server in Manitoba, while you are travelling in the Yukon. It can plausibly be said that your message was sent from any one of three places. *UECA* therefore eliminates the uncertainty and promotes commerce by consistently choosing one of those possibilities.

6. The rules are more complicated if a company has several places of business or no place of business.

UECA also contains clear rules that determine *when* a message is *sent* or *received*. A message is deemed to be *sent* when it leaves the sender's control. Consequently, once you push a button and can no longer stop the message from being sent, that message is considered sent, even if it is never received. A message is deemed *received* when it reaches an information system in the control of the person to whom it is sent. That rule can be tough on recipients because they can be held responsible for messages even if

they never actually read them. However, a recipient can claim that a particular message was never received by proving, for instance, that it could not be downloaded from the server. The best way for a business to avoid disputes about the transmission of its messages is to either require acknowledgment that communications have been received or invoke a system of automated confirmation.

Note that *UECA*'s provisions do not change the common law rules regarding the communication of acceptance. As we saw in Chapter 7, contractual acceptance must be communicated to be effective. Furthermore, the time and the place of the acceptance depend upon the *medium of communication*. *UECA* has avoided the issue of instantaneous versus non-instantaneous communication, recognizing that the decision about whether to treat a particular electronic transmission as similar to a phone call or first-class mail depends upon the circumstances and must be determined on a case-by-case basis.

The rules eliminating uncertainty about where and when a message is sent or received are merely default rules. In other words, parties can choose, mutual consent, to adopt their own rules that are different from *UECA*.

Government Documents

Governments electronically exchange an enormous amount of information with businesses and citizens. They will do so even more as Canada's *Government Online*, and similar provincial initiatives, are fully implemented. *UECA* therefore contains a number of provisions regarding electronic documents that are sent to government. Some provisions protect governments from being swamped by electronic documents that arrive in various incompatible formats. A government can, for instance, specify the formats that it is willing to accept.

7. For the purposes of *UECA*, the term "government" does not include Crown corporations, but it may include municipalities, if the provincial or territorial legislature so decides.

8. Some jurisdictions, including Ontario, Nova Scotia, and the Yukon have adopted those provisions. Others, such as British Columbia and New Brunswick, have not.

Provincial Electronic Commerce Legislation

UECA is a model for provincial electronic commerce legislation. Many provinces have adopted that model entirely or with minor variations. Others have attempted to overcome the same problems by other means. Although it is impossible to provide a detailed comparison of each jurisdiction's approach, we can mention a few important differences.

9. Bill 21, *Electronic Transactions Act*, 1st Sess 25th Parl, Alberta, 2001; *Electronic Transactions Act*, SBC 2001, c 10; *The Electronic Commerce and Information Act*, CCSM 2000, c E55, amending *The Manitoba Evidence Act*, RSM 1987, c E150 and amending *The Consumer Protection Act*, RSM 1987, C200; Bill 70, *Electronic Transactions Act*, 3d Sess, 54th Parl, New Brunswick, 2001; *Electronic Commerce Act*, SNS 2000, c 26 (NS); *Electronic Commerce Act*, SO 2000, c 17 (Ont); *Electronic Commerce Act*, SPEI 2001, c 31 (PEI); *Act to Establish a Legal Framework for Information Technology*, SQ 2001, c 32 (Que); *Electronic Information and Documents Act*, SS 2000, c E-722 (Sask); *Electronic Commerce Act*, SY 2000, c 10 (Yuk).

10. That is true of Alberta, British Columbia, Manitoba, Nova Scotia, Ontario, Prince Edward Island, Saskatchewan, and the Yukon.

The most substantial differences occur in New Brunswick and Quebec. For example, unlike most of its counterparts, the New Brunswick legislation does not regulate the process of offer and acceptance. And the Quebec legislation is much more extensive than its counterparts. It contains, for example, a number of detailed provisions regarding the consultation and transmission of documents that have legal implications for third parties, like online service providers. As a matter of risk management, businesses that are not confined to a single province or territory should consult the relevant legislation to avoid difficulties.

Contracting Online

It is important to note that, for the most part, contract law applies to electronic commerce exactly as it applies to traditional commerce. Although *UECA* and the statutes that it inspired remove many sources of uncertainty about electronic commerce, including the application of contract law to electronic commerce, a number of difficulties remain. In this section we will look at three issues:

contract formation

automated electronic commerce

authentication and security

Contract Formation

The fact that commerce is conducted electronically creates certain problems for traditional rules governing the formation of contract. Some pertain to *shrink-wraps*, *click-wraps*, and *web-wraps* (or *browse-wraps*), while others pertain to the basic process of *offer and acceptance*.

Shrink-Wraps, Click-Wraps, and Web-Wraps

A *shrink-wrap licence* occurs in the context of mass-marketed software. The software is placed in a package that is wrapped in clear plastic wrap. Underneath the wrapping is a card, which states the rules that are attached to the use of the software. That card also informs consumers that, by removing the wrapper, they are agreeing to abide by those

rules—they can use the software, but they must honour the terms of the *licence* that has been created. In general terms, a license is a form of contract that grants permission to use a product in particular ways. In this case, the license allows the customer to use the manufacturer's software on specific terms. Licenses are used in the software industry and in electronic commerce where a business wishes to retain a degree of control over the use of their products. For example, software licenses often prohibit the user from making copies or reselling the product.

The same basic process can be used for online commerce. A *click-wrap licence* is created when a person agrees to accept the terms of an online contract by clicking a mouse or touching an icon that says, "I accept." A **click-wrap licence** can be any licensing agreement triggered by the click of a mouse. A *web-wrap licence* is similar, but more specific. A **web-wrap licence** is triggered by some form of online interaction. For example, while viewing a document online, you try to download or install software, or order goods or services. A window pops up that (i) contains the terms of a contract, (ii) asks you to read those terms, and (iii) tells you to click on one box to accept those terms or on another to reject them. If you click on the first box, you may be bound by a contract. Canadian courts have said that, when properly constructed, such agreements are "afforded the same sanctity that must be given to any agreement in writing." Case Brief 19.1 illustrates this.

a **click-wrap licence** can be any licensing agreement triggered by the click of a mouse

web-wrap licence is triggered by some form of online interaction

11. *Rudder v Microsoft* (1999) 47 CCLT (2d) 168 at para 17 (Ont SCJ).

Case Brief 19.1

Rudder v Microsoft (1999) 47 CCLT (2d) 168 (Ont SCJ)

Microsoft Network (MSN) provides online information services to members of its network. The plaintiffs were two Canadian law students who had entered into an online contract to receive MSN's services. They started a lawsuit in Ontario against MSN when they believed that they had been improperly charged for certain services.

MSN pointed to a provision in the online contract that it had created with the plaintiffs. That provision required any disputes to be resolved through the courts in the State of Washington. MSN therefore said that the case could not be heard in Canada. In response, the plaintiffs argued that they had not noticed the "forum selection clause" and argued that the clause should be treated as "fine print," since only a portion of the agreement was on screen at any given time.

The court held that the plaintiffs had agreed to obey the terms of the online contract when they clicked on the button that said, "I agree." The court then rejected the argument that any terms not wholly in view must be understood as fine print. Such a claim, it held, was no different from saying that only the terms and conditions that appear on the signature page of a printed document should apply. The court also said that ignorance of the relevant term was no excuse since MSN's agreement required potential members to view its terms on two occasions and signify acceptance on each occasion. In fact, the second display of the terms advised users that, "If you click 'I agree' without reading the membership agreement, you are still agreeing to be bound by all of the terms . . . without limitation."

12. In Chapter 9, we considered how courts deal with the "fine print" terms in standard form agreements.

The court in *Rudder v Microsoft* stressed the fact that click-wrap and web-wrap agreements are similar to traditional contracts in one important way—the terms of a contract are effective only if they are sufficiently brought to the parties' attention. The boundaries of this concept were tested in a more recent case. In *Kanitz v Rogers Cable Inc*, an Ontario court had to decide whether unilateral changes to the terms of a contract were valid when they were merely posted on a website. The court held that the changes to the contract were valid because the original contract stated that the defendant could

make changes if it sent customers a notice by e-mail or postal mail, or if it posted the changes on its website. Although the court noted that the defendant could have done more to notify its customers of the changes to the contract, the defendant's posting of the changes on its website was found to be sufficient, given the wording of the original contract.

The decision in *Kanitz v Rogers Cable Inc* suggests that businesses may be able to make binding changes to a contract if they reserve the right to do so and fulfill any notice requirements set out in the contract. In order to manage risk, however, businesses should strive to make contractual terms and changes to such terms as conspicuous as possible. If terms are hidden in a remote hyperlink or camouflaged in small fonts or footnotes, they may not be effective.

13. That was traditionally true in the "ticket cases," which were discussed in Chapter 9.

14. *Kanitz v Rogers Cable Inc* (2002) 58 OR (3d) 299 (Ont Sup Ct).

Offer and Acceptance

Online contracts also create challenges for the traditional rules regarding offer and acceptance. For instance, if a website proposes a contract, does it create an *offer* or merely an *invitation to treat*? As we saw in Chapter 7, if an offer is made to the world at large, it may be accepted by many people. The offeror may therefore be required to fulfill many contracts, even if it really wanted to create only one. As a matter of risk management, you should design your website so that it merelyextends an invitation to treat. You could, for example, require potential customers to place their orders as offers, which you are entitled to accept or reject. Your website should also clearly state that you reserve the right to accept or reject all offers made.

Electronic commerce also raises issues about the communication of acceptance. Chapter 7 explained how the traditional common law rule depends upon whether the communication is instantaneous (like a telephone call) or non-instantaneous (like a

letter). Most jurisdictions in Canada do *not* specify whether particular forms of communication are instantaneous or non-instantaneous. Businesses should prepare for the possibility that an e-mail may be lost or delayed in cyberspace. The safest route is to use various means of communication. For example, if an e-mail message is important, it might be backed up by a fax, regular letter, or telephone call. While electronic commerce is generally intended to avoid that inconvenience, it is still sometimes better to have a back-up plan. In some situations, the extra effort may avoid the time and expense of litigation. Admittedly, however, such safety mechanisms may become impossible as transactions become completely automated.

Automated Electronic Commerce

The cornerstone of traditional contract theory, the notion of *consensus ad idem* (a "meeting of the minds") becomes more difficult to apply in electronic commerce. Electronic commerce transactions may not be created and performed exclusively by humans. Many transactions are initiated and completed by computer software programs and do not easily fit within traditional notions of contract. In fact, part of the point of developing technologies that automate electronic commerce is to allow transactions to take place without any need for humans to review or even be aware of particular transactions. As demonstrated by Case Brief 19.2, a business must take care in the way that it designs and implements automated services.

Case Brief 19.2

Zhu v Merrill Lynch HSBC, 2002 BCPC 0535

Zhu was a stock trader who used Merrill Lynch's NetTrader automated online stock trading system to buy and sell stocks. Immediately after selling stocks on one occasion, Zhu attempted to cancel the sale. He received an automated confirmation that some stocks had already been sold but that the sale of the remaining stocks was cancelled. In fact, the remaining stocks had also been sold. Zhu did not know this and sold the remaining stocks through another transaction. This meant that Zhu had sold the same

stocks twice. Zhu had to buy back the stocks under the second transaction. However, by the time he was required to do that, the price of the stock had increased, causing him a loss of nearly $10 000. Merrill Lynch argued that the cancellation notice did not indicate that the cancellation was successful and that Zhu should have called to confirm that the cancellation was complete before making further sales.

The court held that Zhu was entitled to rely on the online prompts: “Surely common sense dictates that ‘cancelled’ means ‘cancelled’ and [Zhu] is entitled to treat that as a confirmation that his cancellation has been completed. It strikes me that [Merrill Lynch’s] system could easily have issued a prompt saying ‘cancellation pending’ or ‘please wait until advised that cancellation is completed before placing another order.’” Because of the high risk of loss of investment funds, the court also held that Merrill Lynch owed its customers a higher duty of care and performance in providing the automated online service. This decision suggests that businesses providing online services should design their systems and automated notices in a way that consumers can readily understand. This is particularly important for services where there is a high risk of loss to customers.

Most Canadian electronic commerce statutes allow contracts to be created by automated electronic devices. However, it may be dangerous to rely on such systems. Most of the statutes also say that transactions are unenforceable when purchasers make a *keystroke error* when dealing with an automated system. A **keystroke error** occurs when a person mistakenly hits a wrong button or key. For instance, you may order 1000 items instead of 100, or you may hit the “I agree” button instead of the “I decline” button. An automated system normally cannot recognize subsequent messages that you send in an attempt to correct a mistake. It will simply fill your order as originally received. The legislation may allow you to escape the consequences of your error in certain circumstances. Basically, you must prove that (i) the automated system did not provide an opportunity to prevent or correct the error, (ii) you notified the other party of the error as soon as possible, (iii) you took reasonable steps to return any benefit that you received under the transaction, and (iv) you have not received any other

material benefit from the transaction. An online business can avoid those sorts of situations by creating an automated mechanism to correct such errors. The simplest tactic is to require the purchaser to confirm the order by repeating the important steps (for instance, by retyping the number of items that the purchaser wants to receive).

a **keystroke error** occurs when a person mistakenly hits wrong buttons or keys

15. Section 21 of *UECA* states: “A contract may be formed by the interaction of an electronic agent and a natural person or by the interaction of electronic agents.”

Authentication

In our earlier discussion of functional equivalents, we saw that a signature can serve the important goal of demonstrating a person’s willingness to be bound to a contract. But a signature can also provide an *authenticating function*. An **authenticating function** identifies the signatory and ties that person to the document. In many situations, contractual parties are not concerned about each other’s identity. If you buy a bowl of matzo ball soup from my deli, I do not care who you are, and you do not care who I am. However, a party’s identity is often important, especially in electronic commerce. Suppose we create a contract online that requires you to pay $10 000 and that requires me to deliver an Internet server. Without some form of authentication, either you will have to pay and trust me to send the server, or I will have to send the server and trust you to pay. Although people often do business on the basis of trust, it can be a dangerous practice, especially among strangers. Risk management therefore suggests the need for authentication. At least one of us has to be satisfied that the other can be trusted. *Electronic signatures* can be used for that purpose.

an **authenticating function** identifies the signatory and ties that person to the document

Electronic Signatures

An **electronic signature** is electronic information that people can use to identify themselves. The process in which a person uses an electronic signature usually involves two components: a trusted third party known as a *certification authority* and technology known as *public key cryptography*. A discussion of public key cryptography technology is largely a technical matter beyond the scope of this chapter. We will, however, review the role of certification authorities below.

an **electronic signature** is electronic information that people can use to identify themselves

Certification Authorities An electronic signature is reliable if it is used in conjunction with a *trusted third party*. A **trusted third party** is a person or other entity whom both contractual parties can trust. That trusted third party therefore uses a *digital certificate* to verify the identity of the person who provided the electronic signature. A **digital certificate** is an electronic document that authenticates the identity of a particular person. In many ways, it is like an electronic credit card—it is used to establish your credentials when doing business online. A trusted third party who provides that sort of certificate is known as a *certification authority*. There are a number of businesses in Canada and around the world that provide certification authority services.

a **trusted third party** is a person whom both contractual parties can trust

a **digital certificate** is an electronic document that authenticates the identity of a particular person

Note that a certification authority need not be limited to verifying a person's identity for electronic signatures in online contracts. Digital certificates can also be used to certify a person's age, whether that person holds a licence to use certain online services, whether a person's level of security clearance authorizes access to an information system, and so on.

The Canadian government has recognized the importance of electronic signatures and authentication in Canada. In May 2004, it released a draft of the *Secure Electronic Signature Regulations* and the *Principles for Electronic Authentication*. The former rules contain technical requirements for electronic signatures and permit the government to verify which certification authorities have the power to issue trustworthy certificates for certain purposes. On the other hand, the stated purpose of the *Principles for Electronic Authentication* is “to provide guidance [as benchmarks] for the development, implementation and use of authentication products and services in Canada.”

16. *Secure Electronic Signature Regulations*: <http://canadagazette.gc.ca/partl/2004/20040508/htmil/regle6-e.html>.

17. *Principles for Electronic Authentication*: <http://e-com.ic.gc.ca/epic/internet/inecicceac.nsf/en/h_gv00240e.html>.

Information Security

Security measures are crucial to the success of electronic commerce. Online intruders can steal information-based assets, dilute corporate brands, cause critical infrastructure failures, service breaks and system failures, and scare away customers. Security protects corporate assets from external threats. Information security can be used to protect your business against the threat of things like tampering, interception, worms, viruses, and logic bombs. **Information security** is a combination of communications security and computer security. **Communications security** protects information while it is transmitted from one system to another. **Computer security** protects information within a computer system.

information security is a combination of communications security and computer security

communications security protects information while it is transmitted from one system to another

computer security protects information within a computer system

Hardware and software are not the only means of protection. A comprehensive information security system must include other forms of control, including strict workplace policies and personnel security. For example, different employees might enjoy different levels of access to sensitive business information. Businesses can also protect themselves by using the law as a deterrent, by informing those with access to information systems that they will be punished (perhaps by the loss of Internet privileges or even summary dismissal) if they engage in illegal activities like online gambling, possessing child pornography, sexual harassment, and fraud.

Businesses should also publicize that the *Criminal Code of Canada* contains a number of provisions designed to prevent security breaches.

18. *Criminal Code of Canada,* RSC 1985, c. C-46 (Can).

Section 342.1 prohibits the *unauthorized use of a computer*, including theft of computer services, breaches of privacy, and trafficking in computer passwords.

Section 430 (1.1) prohibits *computer mischief* that (i) destroys or alters data, (ii) renders data meaningless, useless or ineffective, (iii) obstructs, interrupts or interferes with the lawful use of data, or (iv) obstructs, interrupts or interferes with any person in the lawful use of data or denies access to data to any person who is entitled to access thereto.

Sections 183 and 184 prohibit the *interception of private communications*. The definition of “private communications” is quite broad, and includes any telecommunication made in Canada or intended to be received in Canada. Business managers charged with information security will be relieved to know that an exception exists where it is reasonable to expect that the communication may be intercepted, as in the employment context.

Businesses can use contract law to protect themselves against some security risks. As we saw in Chapter 18, they can adopt confidentiality agreements. Likewise, they should create and publicize an Internet use policy that will be enforced against all company employees. That policy should include provisions governing (i) the use, disclosure, and return of confidential information, (ii) the use of the Internet, and (iii) permission to monitor employee communications. Businesses can also reduce some security risks by outsourcing to security providers, including certification authorities. By outsourcing, the security provider or its insurer will likely assume some of the risk of maintaining security.

Jurisdiction in Electronic Commerce

Problems cannot always be avoided, and disputes cannot always be settled. Litigation may be inevitable, especially if a business is engaged in global e-commerce. In that situation, it may not be enough to comply with local laws. Website owners and operators must also consider the possibility of being dragged into court in some remote place. They must factor that possibility into the cost of doing business. And while it is expensive to ensure compliance in foreign legal systems, it is sometimes even more expensive to become embroiled in a faraway legal battle. Before considering compliance issues and the kinds of liability that might result from an electronic transaction, we need to first examine the question of *jurisdiction.* **Jurisdiction**, in this context, refers to the ability of a court from a particular place to hear a case. Although the issue of jurisdiction can arise in any kind of case, it is particularly important in electronic commerce. Suppose you have a company in British Columbia with a registered trademark. You discover that a dot-com company in Saskatchewan that sells goods to people in Germany has improperly used your trademark on its website. That website is hosted by a server that is located in France. Where can you sue? British Columbia? Saskatchewan? France? Germany? At least three tests can be used to answer that question:

a real and substantial connection test

a passive versus active test

an effects-based test

jurisdiction refers to the ability of a court from a particular place to hear a case

In Canada, the courts usually use a **real and substantial connection test**. They ask whether the plaintiff's cause of action and the effects of the defendant's conduct are sufficiently linked to the place in which the plaintiff wants to sue. Unfortunately, the courts are not yet sure how to apply that test in an e-commerce context. Early cases in the US likened the Internet to a continuous advertisement. On that basis, they said that information posted on a given website is directed to *every* place capable of accessing the site. Early decisions in Canada followed suit. For example, in *Alteen v Informix*, the defendant, an American manufacturer of information management hardware, allegedly issued untrue and misleading statements that led to an inflated stock price. When Newfoundland shareholders tried to sue, Informix argued that the Newfoundland court had no jurisdiction. Informix argued that it had no real and substantial connection to Canada because it (i) did not trade shares on a Canadian stock exchange, (ii) never made press releases in Canada, and (iii) had no direct contacts with the plaintiffs. Still, the court held that the mere availability of the misleading statements on the Internet was sufficient to assert jurisdiction. Note that the stunning effect of this approach is to potentially make *every* business liable in *every* jurisdiction where the material is accessible.

a **real and substantial connection test** asks whether the plaintiff's cause of action and the effects of the defendant's conduct are sufficiently linked to the place in which the plaintiff wants to sue

19. *Tolofson v Jensen* (1994) 120 DLR (4th) 289 (SCC); *Morguard Investments Ltd v De Savoye* (1990) 76 DLR (4th) 256 (SCC). *Beals v Saldanha* (2003) 234 DLR (4th) 1

(SCC).20. The Supreme Court of Canada recently said that relevant connecting factors in the *real and substantial connection test* include the locations of the content provider, the host server, the intermediaries, and the end user: *Society of Composers, Authors and Music Publishers of Canada v Canadian Association of Internet Providers* (2004) 240 DLR (4th) 193 (SCC).

21. *Inset Systems Inc v Instruction Set Inc* 937 F Supp 161 (D Conn 1996)**.**

22. (1998) 164 Nfld & PEIR 301 (Nfld SC TD).

Online business activity can take many forms, and the analogy between a website and a continuous advertisement is not always appropriate. Consequently, some courts now examine the online interaction to determine (i) the level of interactivity between the parties, and (ii) the commercial nature of the exchange of information that occurs on the website. Under this **passive versus active test**, a court looks at the way in which each party does business online. Is it merely posting information, or does it require customers to interact through the exchange of information online? Does its website send e-mail to particular places? Does it encourage customers from foreign places to call by providing a local or toll-free number? The more interactive a website is in a particular country, the more likely that a court in that country has jurisdiction to hear a case. There is an important point for risk management. If a company does not want to be involved in litigation in a particular place, it should avoid interacting online with people in that place. This issue is highlighted in You Be the Judge 19.1.

the **passive versus active test** requires a court to look at the way in which the parties do business online.

23. *Zippo Manufacturing Co v Zippo Dot Com Inc* 952 F Supp 1119 (WD Pa 1997); *Braintech Inc v Kostiuk* (1999) 171 DLR (4th) 46 (Ont CA).

You Be the Judge 19.1

Dow Jones & Company Inc v Gutnick (2002) 210 CLR 575 (HCA)

Joseph Gutnick was a resident of Australia. In October 2000, *Barron's* magazine, and its website *Barron's Online*, published a story about Mr Gutnick entitled "Unholy Gains." Among other things, the article implied that Mr Gutnick had engaged in money laundering. Mr Gutnick sued Dow Jones & Company Inc (the company that owned *Barron's)* in the Supreme Court of Victoria for defamation.

Dow Jones applied to the court to have the action set aside. Dow Jones claimed that the publication of the article had taken place in New Jersey because its servers containing the article were located in that state. In response, Mr Gutnick argued that the publication took place in Australia because the article could be downloaded there and because Australia was the place where he experienced harm to his reputation.

The High Court rejected Dow Jones' arguments and held that, for the purpose of defamation, publication takes place on the Internet when an article is downloaded and comprehended. The court stated that publication does not take place when an article is loaded onto a server. For the purpose of determining jurisdiction, the court stated that "[t]he most important event so far as defamation is concerned is the infliction of the damage, and that occurs at the place (or the places) where the defamation is comprehended."

Questions for Discussion

1. Do you agree with the decision of the Australian High court? Why or why not?

2. What are some possible global ramifications of this decision? Should a person be able to sue in each jurisdiction where he or she suffers harm?

3. If your managerial duties included overseeing a website that publishes online content, what changes might you make to the availability of your site in foreign jurisdictions?

Several courts have moved away from a test that examines the specific characteristics, or the *potential impact*, of a particular website. Instead, they have adopted a broader **effects-based approach** that focuses on the *actual impact* that a website has in the place where jurisdiction is being sought. This type of approach was adopted in *Dow Jones & Company Inc v Gutnick* (discussed in You Be the Judge 19.1) and has more recently been followed in Canadian courts. To the extent that the courts are tempted to look at *where* the harm is done rather than *how* it is done, it will be very difficult for businesses to insulate themselves from possible liability in remote jurisdictions.

an **effects-based approach** focuses on the actual impact that a website has in the place where jurisdiction is being sought

24. *Bangoura v Washington Post* (2004), 235 DLR (4th) 564 (Ont Sup Ct Jus).

One way a business can protect itself from liability in specific jurisdictions is to avoid *targeting a location*. **Targeting a location** means specifically choosing to create relationships with people within that location. A business that targets individuals or corporations within a particular place is more likely to have the courts in that place take jurisdiction.

targeting a location means specifically choosing to create relationships with people within that location

25. M Geist “Is There a There There? Toward Greater Certainty for Internet Jurisdiction” (2001) Berkeley Tech LJ 1345.

Concept Summary 19.1

Managing and Minimizing Internet Jurisdiction Risks

Assess, minimize, and eliminate any connections your business might have with jurisdictions in which it does not wish to face potential liability. These connections might include physical assets, bank accounts, country code domain names, host servers, and intermediaries.

Insert a jurisdiction clause into contracts that requires any disputes arising from the agreement to be heard by the courts in a specified place in accordance with the laws of that place. As we saw in our investigation of click-wrap and web-wrap contracts, such a clause will only be effective if adequate notice is given and if the other party is capable of agreeing to it.

Use geo-location targeting technologies. Such technologies allow a company to manage the legal risks of e-commerce by restricting the geographical area in which it does business. For example, for legal or business reasons, a website based in Canada might wish to sell goods to customers in Canada and the United States, but not European countries. Geo-location technologies can help achieve this end, thereby minimizing the possibility of legal liability in non-targeted countries.

Domain Names

We have examined the core contractual aspects of electronic commerce. Now we will investigate other legal issues that can arise as a business migrates to the online terrain. Although a key benefit of electronic commerce is that geography becomes less important, the marketing slogan—location, location, location—is still relevant online. Perhaps the most important real estate in cyberspace is the *domain name*. A **domain name** locates an organization's website(s) on the Internet. For example, by entering www.pearsoned.ca into an Internet browser or search engine, you will locate the website of the company Pearson Education Canada, the publisher of this book. Because of the enormous number of domains on the Internet, several national and international organizations regulate their acquisition and use.

a **domain name** locates the website(s) of an organization or other entity on the Internet

26. Like many other international companies, Pearson Education has registered several other domain names, such as <pearsoneducation.com>.

27. For instance, dot-ca (as in <www.pearsoned.ca>) is administered by the Canadian Internet Registry Authority (CIRA).

In the world of real estate, a person may buy a piece of land with a view to reselling it at a profit. The same sort of activity can happen on the Internet. A **cybersquatter** purchases a potentially valuable domain name with the intention of later selling it to the highest bidder. For example, some cybersquatters reserve domain names for common English words (like drugstore.com or furniture.com) in the hope of reselling them to companies that are interested in dealing with the relevant products online. Domain names are typically registered on a first-come, first-served basis. The first person to register it becomes the owner and has the right to resell it. Problems arise, however, when a domain is not merely a common word but rather a name in which someone else asserts some sort of proprietary interest. Although the regulating authorities have received complaints about thousands of domain names, the disputes usually fall into three groups.

a **cybersquatter** purchases a potentially valuable domain name with the intention of later selling it to the highest bidder

A person may innocently, or with some justification, register a domain name that is later disputed. For example, if your newborn nephew is named Ed Pearson, you might register the domain www.pearsoned.ca and post pictures of him at that address. You may receive a complaint from Pearson Education Canada, which holds a proprietary interest in that name.

A person may register a domain name that resembles a trademark to which both parties claim a commercial right. For example, if you hold the US trademark Pearson

International, you may register www.pearsoninternational.ca. If so, you may receive a complaint from the Greater Toronto Airport Authority, which believes that, as operator of Pearson International Airport and holder of a similar registered Canadian mark, it has a stronger claim to that domain name.

A person may register a domain name in which it has no commercial rights. For example, you might try to be the first to register www.pearsoned.ca, either to prevent Pearson Education Canada from using it, to sell it to Pearson at a price far exceeding its cost, or to offer it for sale to Pearson's competitors.

In some circumstances, a business may wish to commence trademark infringement or passing-off litigation against the offending party. However, litigation may require a considerable investment of time and money. That is especially true if the case involves a jurisdiction issue because the cybersquatter lives in some distant part of the world. These costs may be out of proportion to the value of the domain name.

As a result of these issues, the bodies that regulate domain names have adopted procedures for resolving disputes through online arbitration. As we discussed in Chapter 2, arbitration is a form of alternative dispute resolution (or ADR) that allows the parties to settle their argument without the involvement of a court. In the domain name context, arbitration can resolve disputes far more quickly and cost-effectively than court systems. Domain name arbitrators require less evidence and generally do not allow evidence to be tested. In addition, the only remedy typically available in a domain name arbitration is transfer of the domain name from the cybersquatter to the business. Damages and legal costs are not available (as they are in court proceedings. Cybersquatters may therefore operate with relatively little to fear from domain name arbitration.

28. Arbitration was discussed in Chapter 2. In some instances, a party can appeal the arbitrator's decision to a court. The rules for resolving a dispute regarding a dot-ca can be found at <www.cira.ca/en/cat_Dpr.html>.

A business with a domain claim may therefore need to choose between arbitration and litigation. In doing so, it should consider a number of risk management factors. The first factor to consider is whether arbitration is appropriate at all. Domain name dispute arbitration is typically designed only to handle a narrow category of cases—*clear cases of bad faith cybersquatting*. Disputes between two companies with competing trademark rights to a name will normally not be suited for resolution by online arbitration.

If both litigation and arbitration are options, then the claimant will need to consider a number of factors including (i) the strength of the trademark, (ii) the evidence available about the cybersquatter, (iii) the urgency of resolving the dispute, (iv) the acceptable costs of resolution, and (iv) the ultimate objectives (such as whether the business merely wants transfer of the domain or whether it also wants money damages for trademark infringement). Generally speaking, arbitration can be an efficient and low-risk way to resolve a domain name dispute where a strong case can be made out on paper. If credibility is an issue, evidence against a cybersquatter is lacking, or a claimant wants an award of money damages for trademark infringement, then litigation in court may be preferable.

Business Decision 19.1

Parody Websites

Ken Harvey was a speculator in domain names who lived in Newfoundland. Upon registering walmartcanadasucks.com and a number of similar domains, Ken created and uploaded a Web page stating that, “This is a freedom of information site set up for dissatisfied Wal-Mart Canada customers.” The site exhorted visitors to “Spill Your Guts” with a “horror story relating to your dealings with Wal-Mart Canada.” Wal-Mart responded by filing a complaint to a dispute-resolution provider, indicating that the domains were registered in bad faith. According to Wal-Mart, Ken’s free speech argument was merely a cybersquatter’s convenient and transparent dodge. On that basis, Wal-Mart sought to have control of the domain name walmartcanadasucks.com.

The dispute resolution provider held that Ken's conduct, even if distasteful, should not result in an unwarranted expansion of the domain name dispute process. According to the arbitrator, the dispute resolution process is meant to protect against bad faith domain name registrations, not provide a general remedy for all misconduct involving domain names. Having held that the walmartcanadasucks.com domain name is not identical or confusingly similar to Wal-Mart's trademarked name, the arbitrator decided that Ken did not register the domain name in bad faith. In fact, the arbitrator ruled that Ken had "a legitimate interest in respect of the domain name, to use it as a foundation for criticism of the complainant." On this basis, the request to transfer the domain name to Wal-Mart was refused.

Questions for Discussion

1. Should consumers be allowed to say whatever they want about a business, even if what they say is harmful and results in a loss of profits?

2. If you were the Wal-Mart executive charged with handling the matter, how might you have avoided arbitration?

29. *Wal-Mart Stores Inc v walmartcanadasucks.com and Kenneth J Harvey*, WIPO Arbitration and Mediation Center, Case No D2000-1104 .

As a matter of risk management, the best strategy is to avoid difficulties altogether. While that is not always possible, businesses can take steps to minimize the potential for domain name disputes. For instance, as a component part of its overall intellectual property strategy, a business should register trademarks and business names as domain names as early as possible to avoid being held hostage by a cybersquatter. This might include registering domain names that correspond to company names, brand names, slogans, and product names. While dot-com, dot-net, and dot-org domain names tend to be the most popular domain names, a business should also consider the various country-code domain names that it might wish to register, including dot-ca, dot-

uk, and dot-us. Note that a registered trademark will not guarantee your business a proprietary interest in a particular domain name.

Concept Summary 19.2

Business Strategy Regarding Domain Names

-

- Avoid disputes by registering key trademarks, product names and business names as domain names before someone else does (for example, register key domain names *prior* to the launch of the relevant business or product if possible).
- Consider registering generic domains (such as dot-com), and country code domains (such as dot-ca) for the countries you do business in.
- If a dispute arises regarding a domain name, consider whether arbitration under a dispute resolution policy is an option.
- When deciding whether to pursue arbitration or litigation, consider factors such as the strength of the trademark, the evidence available about the cybersquatter, the urgency of resolving the dispute, the cost you are willing to incur, and your objectives.

-

Liability of Online Intermediaries

For the most part, the threat of liability in electronic commerce is much the same as it has always been. The elements of the tort of defamation, for instance, are identical whether committed in person or over the Internet. As discussed above and demonstrated by You Be the Judge 19.1, however, the Internet does pose unique

jurisdictional problems in the area of online defamation. It may also affect the damages that result from the tort because defamatory material in digital form may be accessed, copied, and distributed widely, with the possible effect of increasing the harm suffered. And finally, beyond posing challenges for existing law, electronic commerce may also generate new forms of liability for certain kinds of online businesses, because of the role that *online intermediaries* play in various online relationships.

An **online intermediary** is a party that enables or facilitates an online transaction between others. Think about all the things that need to happen before you can sell me stuff that is advertised on your website. First, someone has to agree to host your website. Second, unless I am fortunate enough to own an Internet server, someone needs to provide me with access to the Internet. I also need an e-mail account. So do you. Someone is probably in the business of storing or managing most of that data. There are, then, many kinds of businesses that *intermediate* our transaction. They are all considered online intermediaries. In fact, you might even be one. If your business provides employees with access to the Internet or e-mail, then you are an online intermediary in any of their transactions. Other online intermediaries might include courier companies or financial intermediaries like banks or credit card companies. Here, we will focus on two different kinds of online intermediaries:

Internet service providers

online service providers

an **online intermediary** is a party that enables or facilitates an online transaction between others

Internet Service Providers

An **Internet service provider**, sometimes called an *ISP* or an *Internet access provider*, provides others with access to the Internet. Suppose you start a business that provides Internet access for a flat fee. What happens if one of your customers uses your service to defame someone, download obscene materials, or breach copyright? As an intermediary, can you be held accountable? Generally speaking, the law says “no.” Internet access providers, like phone companies, are usually given special treatment, because they are in the business of supplying the pipeline, not monitoring its flow. That is not to say that an access provider is immune from all forms of liability. Suppose you are an Internet access provider, and your standard contract absolutely guarantees customers uninterrupted service. One day, your service will go down. When it does, you will be liable for breach of contract. You could have avoided liability if you had anticipated service interruptions and provided for them in your standard contract. Or, suppose you do not provide access for a fee, but for free to your employees. It is possible that they might do things online that attract liability to you as the access provider.

an **Internet service provider** provides others with access to the Internet

30. For example, an employee may download obscene materials in the workplace. By allowing the employee to create a hostile work environment, the employer may be held liable under human rights legislation, especially if the employer adopted a policy of monitoring employee conduct online but failed to enforce the policy.

Online Service Providers

Intermediary liability becomes much more difficult to determine in the context of *online service providers*. An **online service provider** offers goods or services, beyond mere Internet access, in exchange for something of value. Electronic commerce examples include e-mail suppliers, bulletin board operators, auction hosts, anonymous remailers, and commercial websites. Many ISPs act as both an ISP and an online service provider.

an **online service provider** offers goods or services, beyond mere Internet access, in exchange for something of value

An online service provider usually enters into a contract with its subscriber. As usual, it can be held liable to that person if it breaches their agreement. However, it can also manage that risk by inserting an exclusion clause into the contract. Significantly, however, that strategy cannot protect an online service provider from liability to a third party. Since that party is not part of any contract and is therefore not bound by any exclusion clause, it may sue the service provider *as an intermediary*. For example, when a customer uses Yahoo! or AOL Canada to distribute a defamatory statement, the victim of that tort may sue both the customer and the online service provider. The victim may also sue the service provider for failing to reveal the true identity of the customer if that statement was posted under a false name. It is important to recognize, however, that you do not have to be an Internet giant to expose your business to these kinds of lawsuits. Risk managers will want to shield their online businesses against liability for (i) publishing defamatory remarks, (ii) distributing materials that infringe copyright, (iii) disclosing personal information, (iv) infringing trademarks, (v) participating in computer mischief, and (vi) possessing or distributing child pornography, to name a few.

31. We discussed exclusion clauses and privity of contract in Chapter 8.

Case Brief 19.3

Society of Composers, Authors and Music Publishers of Canada v Canadian Association of Internet Providers (2004) 240 DLR (4th) 193 (SCC)

The Society of Composers, Authors and Music Publishers of Canada (SOCAN) is a collective society which administers Canadian copyright in music for Canadian and foreign copyright owners. SOCAN collects royalties from radio stations that play copyright songs that SOCAN is responsible for administering. In this case, SOCAN tried to collect royalties from Canadian Internet service providers on the basis that ISPs infringe the right of copyright owners to communicate their works to the public and to authorize such communication.

The Canadian Association of Internet Providers (CAIP) opposed SOCAN's attempt to collect royalties from ISPs. CAIP argued that ISPs do not communicate copyright works or authorize such communication. According to CAIP, ISPs are merely conduits for communications and do not regulate the content of communications passing over their networks.

The Supreme Court of Canada held that ISPs are not liable to pay SOCAN royalties when they merely function as content-neutral conduits. That is true when ISPs do not have knowledge of the infringing content and when, from a technical and economic standpoint, they cannot practically monitor the vast amount of content passing over their networks. "Caching" (the temporary storage) of content by an ISP is a conduit function because it is content-neutral and it is motivated by the need to deliver faster and more economical Internet access service. The court did not, however, rule out the possibility that ISPs might have to pay royalties when they act as more than mere conduits.

Finally, the court held that an ISP does not "authorize" an infringement merely because it knows that a user *might* use an ISP's facilities to commit infringement.

In the United States and within the European Union, specific legislation has been passed to shield Internet service providers from liability in some circumstances. Unfortunately, very few Canadian law makers have squarely addressed these issues. Canadian businesses are therefore often in the precarious position of relying on the courts to correctly interpret and apply the *SOCAN* decision. One province that has legislatively intervened is Quebec. According to section 27 of its *Act to Establish a Legal Framework for Information Technology*, service providers acting as intermediaries are not required to monitor the information communicated on their networks or in the documents stored on them, nor are they required to report communications or documents that may be used for illegal activities. Even if a service provider chooses to monitor or report, its decision to do so will not automatically result in intermediary liability if illegal content is later found on its site. Section 36 of the Act states that service

providers acting as intermediaries are not generally responsible for the illegal acts of service users. However, it also states that a service provider *may* incur liability if it *participates* in acts performed by service users.

32. In the US, the *Digital Millenium Copyright Act of 1998*, Pub L No 105-304, 112 Stat 2860 provides a safe harbour from liability where an ISP complies with a notice and take-down system. In the UK, a restricted immunity from liability is stipulated in section 1 of the *Defamation Act, 1996* (UK) 1996 c 31. Applying this provision to the online environment, a service provider who (i) is not an author, editor, or publisher, (ii) takes reasonable care, and (iii) does not know, or have reason to believe that what they did, contributed to or caused the publication of a defamatory statement, will be protected from liability for defamation. The European Union's *E-Commerce Directive 2000/31 of the European Parliament and of the Council of June 8, 2000 on certain legal aspects of information society services, in particular electronic commerce, in the Internal Market (Directive on electronic commerce),* [2000] OJL178/1 provides that intermediaries are not liable where their actions are limited to "the technical process of operating and giving access to a communication network over which information made available by third parties is transmitted or temporarily stored."

33. There is, however, a recent indication that the federal government intends act in this area. See Bill C-60, *An Act to Amend the Copyright Act*, introduced in June 2005.

34. *Act to Establish a Legal Framework for Information Technology* SQ 2001, c 32.

35. For example, liability may be imposed if the service provider (i) sends a document, (ii) selects or alters the information in a document, (iii) determines who transmits, receives, or has access to a document, or (iv) stores a document longer than is necessary for its transmission.

What about online service providers in other provinces? How can you shield your business from intermediary liability?

You should have a clear contract with each user, possibly through a click-wrap agreement. Each user should be required to clearly consent to the *terms of service* that are contained in that contract. And those terms should allow you to claim *indemnification* from a user if you are ever held liable for something that they posted.

Those *terms of service* should clearly explain, with examples, which uses are acceptable and which are unacceptable. While you should not commit yourself to monitoring content, you should reserve the right to remove content where the content is in violation of your terms of service or where you wish to remove it for other reasons in your discretion.

You should, whenever possible, set up your business so that you can demonstrate that it merely acts as a conduit or pipeline for the materials that pass through the system.

If you are sued, you should try to convince the court that while the legislation in Quebec, the US, and the European Union are not binding in other places, they are based on policies that should be adopted. The Supreme Court of Canada's decision in *SOCAN v CAIP* may also be helpful.

36. Indemnification would require the user to compensate you for any losses that you suffered (for example, by being successfully sued as an intermediary by a third party).

P2P File-Sharing

Peer-to-peer (P2P) file-sharing systems are among the most popular and controversial online applications in use today. These systems allow individuals to search for and share files of all kinds over a distributed network. Although Napster was the first widely used P2P system, newer, more sophisticated technologies are now in widespread use, including BitTorrent, Morpheus, and eDonkey. P2P technologies continue to evolve rapidly and are being used by millions of people to share an extraordinary number of files (especially music files) online.

Some copyright owners claim that P2P systems are being used to infringe their copyrights on a mass scale. Their reaction to P2P has been multi-faceted. For example, some copyright owners have launched and sanctioned music download services of their own. Some have sued P2P users and the companies that make P2P software. Ethical Perspective 19.1 describes one such example in Canada. In the United States, legislation (such as the *INDUCE Act*) that would effectively ban P2P software has been introduced in Congress.

37. US, Bill S 2560, *Inducing Infringements of Copyright Act of 2004*, 108th Cong, 2004.

Copyright issues aside, the P2P phenomenon illustrates how technology may challenge existing business models. P2P systems allow users to sample music for free and to download only those songs that they actually want. These systems threaten traditional distribution channels within the recording industry. Until recently, the music industry focused on the album format. Because it delivered songs in pre-arranged packages, the album format often forced users to buy some songs that they did not want. In those situations, the choice between album formats and P2P systems is obvious from a consumer perspective. Consequently, unless they are prepared to lose profits, and perhaps even their place in the market, traditional music companies will need to adapt and evolve alongside emerging technologies.

Ethical Perspective 19.1

BMG Canada Inc et al v John Doe (2004) 239 DLR (4th) 726 (FC TD), affd (2005) 39 CPR (4th) 97 (FC CA).

The Canadian Recording Industry Association (CRIA) brought an action in Federal Court against 29 unnamed individuals, alleging that they had illegally shared hundreds of music files on P2P systems. Though the 29 individuals could not be identified by their legal names, CRIA claimed that it was able to determine their P2P pseudonyms (such as Geekboy@KaZaA.com) and their internet protocol (IP) addresses (a unique number associated with their computers). Because CRIA was not able to determine the actual

identities of the individuals it was targeting, it asked the court to order five Internet service providers (ISPs) to reveal the legal names associated with the P2P pseudonyms using P2P to download songs. CRIA claimed that it had linked the P2P pseudonyms to IP addresses at particular times and that the ISPs would have records linking the legal names to the associated IP addresses.

Citing concerns about online privacy, doubts about whether P2P file-sharing even amounted to copyright infringement under Canadian law, and weaknesses in CRIA's evidence, the court refused to order the ISPs to reveal the names of their subscribers to CRIA. For example, the court stated that "[t]here is no evidence explaining how the pseudonym 'Geekboy@KaZaA' was linked to IP address 24.84.179.98 in the first place. Without any evidence at all as to how IP address 24.84.179.98 has been traced to Geekboy@KaZaA, and without being satisfied that such evidence is reliable, it would be irresponsible for the Court to order the disclosure of the name of the account holder of IP address 24.84.179.98 and expose this individual to a lawsuit by the plaintiffs."

Questions for Discussion

1. Do you agree with the decision of the Federal Court refusing to order ISPs to reveal the names of their customers? Why or why not? Under what circumstances should ISPs be required to disclose the names of their subscribers?

2. Assuming that sharing copyrighted music on P2P networks is illegal, why do you think that so many people are using P2P for that purpose? Has the law fallen out of step with socially acceptable behaviour when it comes to P2P?

3. What do you think of the morality of CRIA's strategy of suing individual users? If you were a decision maker at CRIA, would you take the same approach to perceived problems regarding P2P networks? What other options might you consider?

38. K Damsell "Uploaders not 'pirates,' court told" *Globeandmail.com* (15 March 2004).

Online Privacy

The growth in e-commerce has caused increased concern about privacy. Many online businesses have technology that allows them to record, store, and process personal information about their customers. Consumers very often give up those details without consent and, indeed, without even knowing it. The law has therefore begun to provide additional protection. Businesses need to carefully consider their obligations under those laws. By limiting the types of information that it collects from its customers, a company may be able to minimize its exposure to liability and reduce compliance costs.

The *Personal Information Protection and Electronic Documents Act* (*PIPEDA*) is Canada's legislative attempt at regulating the collection, use, and disclosure of "personal information" in the private sector. *PIPEDA* defines "personal information" as information about an identifiable individual, but does not include the name, title, business address, or telephone number of an employee in an organization. In the online context, information collected through the use of "cookies" on a website can constitute personal information.

39. Privacy Commissioner of Canada *PIPEDA* Case Summary #162, *Customer complains about airline's use of "cookies" on its Web site* (2003). The Privacy Commissioner of Canada defines "cookies" as "small text files that are placed on your computer's hard drive when you visit websites. Cookies collect and store information about you based on your browsing patterns and information you provide." See <http://www.privcom.gc.ca/cf-dc/2003/cf-dc_030416_7_e.asp>.

PIPEDA generally applies when (i) an organization collects, uses, or discloses personal information in the course of commercial activity, and (ii) an organization collects, uses, or discloses personal information about an employee in connection with some activity of the federal government. The Act does not apply, however, in those provinces that have enacted similar legislation. To date, only British Columbia, Alberta, and Quebec have done so.

40. *Personal Information Protection Act*, 2003 SBC c 63; *Personal Information Protection Act*, SA 2003, c P-6.5; *Act Respecting the Protection of Personal Information in the Private Sector*; RSQ, c P-39.1. The fact that businesses are subject to either the

federal *PIPEDA* or a provincial equivalent may raise a question of constitutional authority. We discussed the division of powers between the two levels of government in Chapter 1.

In one form or another, *PIPEDA* and the provincial equivalent privacy laws require organizations to comply with 10 legal obligations:

1. *Accountability:* An organization is responsible for personal information under its control. It must name a person who can be held accountable for the organization's compliance with the obligations in this list.

2. *Identifying purposes:* Before collecting personal information, an organization must state its reason for doing so.

3. *Consent:* An organization should generally obtain informed consent from a person collecting taking personal information. That requirement does not apply, however, where it would be inappropriate.

4. *Limiting collection:* An organization must act fairly and lawfully when collecting personal information, and it must not collect more information that it needs for its stated purpose.

5. *Limiting use, disclosure, and retention:* Unless it either has the person's consent or is under a legal obligation to act differently, an organization can use personal information only for its stated purpose. An organization should not retain personal information any longer than necessary.

6. *Accuracy:* Personal information must be protected by safeguards that are appropriate to the circumstances.

7. *Safeguards:* Personal information must be protected by safeguards that are appropriate to the circumstances.

8. *Openness:* An organization must be prepared to provide individuals with details about its personal information policies and practices.

9. *Individual access:* Upon request, an organization must provide each individual with access to information that has been collected about him or her. The individual has the right to challenge the accuracy and completeness of that information, and the right to have errors or omissions rectified.

10. *Challenging compliance:* An individual has the right to direct complaints and concerns arising under these rules to the person who the organization has made accountable.

As a result of interpreting the legislation, judges have begun to provide businesses with guidance on how to meet their obligations under *PIPEDA*. When presented with a potential problem, an organization should ask itself the following questions.

Is the collection, use or disclosure of personal information necessary to meet a specific organizational need?

Is the collection, use or disclosure of personal information likely to be effective in meeting that need?

Is the loss of privacy proportional to the benefit gained?

Is there a less privacy-invasive way of achieving the same end?

The Federal Court applied that framework in *Eastmond v Canadian Pacific Railway*. CPR installed video surveillance equipment in an effort to deter theft and vandalism on its property. The court received a complaint that, in doing so, CPR had violated *PIPEDA*. The court disagreed. It said that (i) CPR had a specific need to investigate and deter trespassers and vandalism, (ii) the video surveillance was likely to meet that need, (iii) because the area in question was outdoors, where people have a reduced expectation of privacy, the loss of privacy was minimal and proportional to the benefits of surveillance, and (iv) because other strategies for dealing with theft and vandalism

were considerably more expensive, there was no other *effective* solution that involved less invasion of privacy.41. (2004) 16 Admin LR (4th) 275 (FC). See also *Englander v Telus Communications* (2004) 247 DLR (4th) 275 (FC CA).

Concept Summary 19.3

Strategies for Minimizing Privacy Compliance Risks and Costs

- Gain a clear understanding of how your business and your technology might collect, use or disclose personal information. Talk to your information technology staff and involve them in your privacy compliance plans.
- Appoint a person or team of people to be responsible for privacy issues. Ensure that all of your employees receive adequate training in privacy.
- Consider strategies for limiting, as much as possible, the collection of personal information—especially information of a sensitive nature.
- Before dealing with personal information, always ask how a reasonable person would view the situation.
- Ask the following questions before dealing with personal information:

    (i) Is it necessary to meet a specific need?

    (ii) Is it likely to be effective in meeting that need?

    (iii) Is the loss of privacy proportional to the benefit gained?

    (iv) Is there a less privacy-invasive way of achieving the same end?

- Whenever possible, obtain consent before dealing in personal information. And, of course, always comply with the consent requirements under *PIPEDA* and similar statutes.

Online Consumer Protection

We end this chapter with a brief look at consumer protection principles in the e-commerce environment. Consumer protection principles are important to individuals as consumers, but they are also important to businesses. By adopting them, along with the privacy practices described above, a business can enhance its reputation, strengthen consumer confidence, and ultimately increase sales. This is particularly important in electronic commerce, where consumer confidence remains relatively low.

Although some provinces have amended existing consumer protection legislation in light of electronic commerce, full-scale law reform has not yet occurred. Industry Canada (a branch of the federal government) has promoted a code of practice in its *Canadian Code of Practice for Consumer Protection in Electronic Commerce*. Although the Code is not law, its provisions reflect a number of the legal obligations described throughout this chapter. The Code contains suggestions for ethical and effective business practices that are intended to supplement the laws that already protect consumers. Compliance with the Code will likely minimize legal risks in a number of areas. In 2004, the Code was endorsed by federal, provincial, and territorial ministers responsible for consumer affairs. The Code is now open for endorsement by private sector organizations and consumer organizations. We summarize here the provisions of the Code.

42. Industry Canada *Canadian Code of Practice for Consumer Protection in Electronic Commerce* (2004). This document is itself based on the OECD Council *Recommendation of the OECD Council Concerning Guidelines for Consumer Protection in the Context of Electronic Commerce* (1999). It is excerpted from CSA Standard *Model Code for the Protection of Personal Information* (1999).

1. Information provision.

Consumers should be provided with clear and sufficient information to make an informed choice about whether and how to make a purchase. Online businesses should avoid jargon and use plain language whenever possible. They should clearly distinguish marketing and promotional material from the terms and conditions of sale. They should disclose the legal identity of their business, their business address, and any geographic limitations on where a product or service is for sale. They should fairly and accurately describe their goods. They should set out a complaints procedure and provide consumers with their own record of the transaction.

2. Language.

When an online business offers products or services in a language, it shall use that language to provide all of its material information about the product or service, the vendor, the vendor's relevant policies, and the terms and conditions of the transaction and all other material information. When information or support is not available in that language, this shall be stated by the vendor in the language in which the transaction was conducted.

3. Contract formation and fulfillment.

Vendors should take reasonable steps to ensure that the consumer's agreement to contract is fully informed and intentional. Consumers shall be provided with a opportunity to correct or cancel the order before it is accepted and filled. Vendors who cannot deliver a product within the time frame originally specified shall promptly notify consumers and give them the option of cancelling their order at no charge, except where unreasonable.

4. Online privacy.

An online business should set up its data collection and information systems with a view to respecting and protecting its customers' privacy in compliance with the CSA *International Model Code*.

5. Security of payment and personal information.

Vendors and intermediaries should take reasonable steps to ensure that transactions in which they are involved are secure. An online business should use the technology and procedures discussed in this chapter and consistent with industry standards in order to safeguard payment and personal information that is exchanged or stored as a result of a transaction.

6. Complaint handling and dispute resolution.

Consumers should have access to fair, timely, effective, and affordable means for resolving problems with any transaction. An online business should have resources for handling consumer complaints efficiently and effectively. Vendors shall offer an internal complaints-handling process that is easily accessible, available to consumers free of charge, easy to use, acknowledges complaints within seven business days, endeavours to resolve or address complaints within 45 days, and records and monitors complaints.

7. Unsolicited e-mail.

Vendors shall not send unsolicited e-mail to consumers without consent. If a vendor has more than a passing existing relationship with a consumer, consent may not be required. In any marketing e-mail, vendors shall provide a return address and a simple way for consumers to indicate that they do not wish to receive such messages. Online businesses should avoid spamming, sending unsolicited e-mails to a large number of people. Not only is it bad Internet etiquette, or "netiquette," but also spam exposes a business to the risk of being associated with products that are worthless, deceptive, and at least partly fraudulent. Many of the online scams that we discussed above are perpetrated through unsolicited mass e-mail. Why risk the reputation of your business when there are more sophisticated and successful means of advertising?

8. Communications with children.

Vendors have a social responsibility to determine whether they are communicating with a child in any given transaction. Vendors should not exploit the lack of experience or

sense of loyalty of children and must not exert pressure on children to urge their parents to purchase products or services. Vendors shall take reasonable steps to avoid monetary transactions with children and shall not collect the personal information of children except where express parental consent has been obtained.

Chapter Summary

Electronic commerce refers to technology-mediated business transactions. Although e-commerce has facilitated the development of the knowledge-based economy, its success will ultimately depend on eliminating various legal uncertainties and impediments.

Electronic commerce legislation tries to facilitate online transactions by removing commercial uncertainty and other impediments. The co-ordination of model laws at both the international and national level has facilitated the global implementation of uniform laws at the provincial level. Canada's model law, the *Uniform Electronic Commerce Act,* sets out a framework for inferring consent to participate in electronic transactions, the functional equivalents of paper-based requirements, the proper treatment of government documents, and a clarification of the rules of contract formation in the online setting (including the timing requirements for sending and receiving electronic documents). Although the adoption of electronic commerce in various Canadian jurisdictions differs in detail, many provinces and territories have maintained fidelity to much of the approach taken in *UECA*.

Online contracts, such as click-wrap and web-wrap agreements, have been recognized as enforceable provided the basic requirements of contract formation are adequately met. To ensure that an agreement is enforceable, managers charged with Web development should design online transactions with the requirements of electronic commerce legislation in mind. They should also ensure that the design of those transactions provides reasonable notice of the terms and conditions, and, if necessary and desirable, reserves the right to make modifications to contractual terms and to post them to a website. Automated electronic commerce promises to dispense with the need for human supervision in the contract-formation process. Although most provincial

legislation contemplates a method for rectifying keystroke errors, managers should incorporate safety mechanisms into their electronic contracts to protect their businesses against liability for computer-generated errors.

Electronic signatures and related technologies promise to fortify the flimsy foundation of trust resulting from global online interaction. Information systems such as these can be used to authenticate transactions, ensure their integrity, and enhance online security. Technological measures are not, however, the sole means of ensuring information security. Business managers must also consider legal measures, including the adoption and enforcement of terms of service agreements and other strictly enforced corporate policies. A careful approach to information security will ultimately prove fundamental to the success of electronic commerce.

Although one key benefit of electronic commerce is that geography becomes less important, location is still relevant online. Domain names provide the virtual storefronts necessary for electronic commerce. Mimicking traditional real estate speculation, some individuals and companies are in the business of cybersquatting. Domain name registration authorities have developed uniform dispute resolution procedures to help resolve complaints brought by those claiming a proprietary interest in a particular domain name. For a fee, dispute resolution professionals will mediate and, if necessary, arbitrate disputes through various electronic media, thus decreasing the time and expense associated with traditional litigation.

The global reach of electronic commerce means that compliance with local laws is no longer sufficient insulation from legal risk. Website owners and operators must consider the possibility that they may be dragged into a court battle in some remote jurisdiction. In resolving these disputes, Canadian courts consider whether there is a real and substantial connection between the cause of action, its effects, and the location in which the action has been commenced. Other considerations include the passivity or interactivity of the website and the actual effects of the alleged transgression in the location where jurisdiction has been sought. Targeting strategies, including the use of technological measures, will reduce the risk of being sued successfully in a foreign

jurisdiction. The question of liability for online intermediaries is not perfectly settled. Early decisions have held that service providers who exercise no editorial control over their sites are immune from liability, whereas service providers who exercise even a low level of control might be held liable. Concerned that this approach provides a clear disincentive for service providers to read and remove illegal content from their websites, some jurisdictions have enacted legislation that provides a more balanced approach, extending further protection to online intermediaries under certain circumstances. The prospect of enhanced liability has led many Internet access and online service providers to insist on exclusion clauses in their terms of service. Prudent online intermediaries have also sought to implement practices to shield themselves from liability by demonstrating that they operate as mere conduits of electronic communication.

P2P file-sharing continues to be one of the most hotly contested areas of online activity with ramifications and lessons to learn for the way that law and business react to new technologies.

Privacy has taken on a great significance in electronic commerce. Technology increasingly enables the collection, use, and disclosure of vast amounts of personal information. *PIPEDA*, as well as the enactment of privacy laws in certain provinces, will require some businesses to ensure that adequate steps have been taken in order to minimize their risks and costs of compliance associated with the collection, use, and disclosure of personal information about identifiable individuals.

Full-scale law reform in the consumer protection area has not yet occurred. The most substantial development is a Code promoted by Industry Canada. Since the Code is not law, any action taken by the Competition Bureau is merely educational in nature. Still, these guidelines offer insight to businesses and consumers about the shortcomings of conducting business online in a manner that does not ensure the development of trusting relationships with customers and clients.

Review Questions

1. In what sense is the law a source of uncertainty in the electronic commerce marketplace?

2. What are four potential benefits that electronic commerce offers to businesses willing to implement the use of information technologies?

3. What is the role and purpose of Canada's *Uniform Electronic Commerce Act*?

4. How is Canada's UECA enforced in each province and territory?

5. What are the relevant rules about sending and receiving electronic documents? As a risk manager, what steps can you take to avoid related disputes?

6. Given that electronic commerce legislation is provincially enacted, discuss several issues that a business manager should consider when engaged in interprovincial commerce.

7. Explain the difficulties associated with the formation of contracts online. What lesson can business managers learn from the case of *Rudder v Microsoft*?

8. Does *Kanitz v Rogers Cable* suggest a different lesson from *Rudder v Microsoft*?

9. How can information about products or services be designed to ensure that it is considered an invitation to treat? Why should a Web designer seek to do so?

10. Explain the complexities associated with automated electronic commerce. How can a business safeguard against the undesirable consequences of keystroke errors?

11. Why are the services of trusted third parties crucial to electronic commerce?

12. Distinguish between *communications* security and *computer* security, and provide an example of each.

13. What steps can a business take to avoid targeting a particular jurisdiction?

14. Name and discuss the variables that a court may consider in deciding if a specific online interaction falls under its jurisdiction.

15. What is cybersquatting? Is it ever legally permissible?

16. Describe three typical disputes arising from the domain name registration system, and provide an example of each. How can business managers avoid domain name disputes?

17. Distinguish between Internet access providers and online service providers, and give an example of each. In which role is an online intermediary most likely to attract potential liability? Why?

18. As an online service provider in the province of Newfoundland and Labrador, describe how you can shield yourself from possible liability as an online intermediary.

19. Name one way that an online business can minimize its privacy compliance risks and costs.

20. Describe how a business can incorporate consumer protection principles into its online contracting practices.

Cases and Problems

1. You are the general manager of a company that does business exclusively in Saskatchewan. With the aim of increasing efficiency and cutting costs, you are contemplating a change in corporate software that would enable filing all necessary government documents in electronic form. However, you are uncertain whether the provincial government will be obligated to accept documents in that form. Before paying a lawyer, you have decided to review the relevant legislation yourself to see if there is a clear answer. Using the legislation set out below, decide whether your company should switch to an electronic format. Can your provincial government force you to file solely by electronic means?

The *Uniform Electronic Commerce Act* contains these clauses concerning the filing of electronic forms with the government:

6. (1) Nothing in this Act requires a person to use or accept information in electronic form, but a person's consent to do so may be inferred from the person's conduct.

(2) Despite subsection (1), the consent of the Government to accept information in electronic form may not be inferred by its conduct but must be expressed by communication accessible to the public or to those likely to communicate with it for particular purposes.

9. A requirement under [enacting jurisdiction] law for a person to provide information to another person in a specified non-electronic form is satisfied by the provision of the information in an electronic document,

(a) if the information is provided in the same or substantially the same form and the electronic document is accessible by the other person and capable of being retained by the other person so as to be usable for subsequent reference, and

(b) where the information is to be provided to the Government, if

(i) the Government or the part of Government to which the information is to be provided has consented to accept electronic documents in satisfaction of the requirement; and

(ii) the electronic document meets the information technology standards and acknowledgment rules, if any, established by the Government or part of Government, as the case may be.

Saskatchewan's *Electronic Information and Document Act* does not contain sections corresponding to 6(2) or 9(b) as do many of the other provinces. Instead it amends the following clause:

28. (1) A person may file a document or information in an electronic format with the appropriate department pursuant to a designated Act, but only if:

(a) the document or information is of a class that is prescribed in the regulations made pursuant to the designated Act as a document or information that may be filed electronically;

(b) the electronic format used is a format that is prescribed in the regulations made pursuant to the designated Act;

(c) the document or information is recorded on a system of electronic data storage that, in the option of the person responsible for the maintenance of the document or information to be filed, can be read by the computer or other equipment used in the information filing system; and

(d) the person filing the document or information is, or is a member of a class of persons that is, authorized to file the document or information in an electronic format by:

(i) a person who has the power to grant that authorization pursuant to the designated Act; or

(ii) if there is no person who has the power to grant that authorization pursuant to the designated Act, the member of the Executive Council to whom for the time being the administration of the designated Act is assigned.

2. You are the information manager of an electronic mailing service BadNews.ca. Your primary customers are collections agencies. BadNews.ca assists these agencies by locating debtors and delivering legal notices to them before the repossession of their assets. You were taking the position that simply sending an e-mail message would fulfill the written notice requirements set out in the provincial legislation that regulates the collection of debts. Recently, however, you discovered that the law requires such notices to not merely be sent but to actually be received. You have been asked to determine the effect that the *UECA* will have on your company's business practices. Prepare a brief memo explaining the rules governing the sending and receiving of

electronic messages. Make sure that your memo provides some advice indicating the best way to avoid disputes with intended recipients.

3. Unlike most of your friends in business, you are quite familiar with encryption technologies and have been using them for a few years. Recently, you have done further research on the use of trusted third parties in electronic commerce. In so doing, it has come to your attention that it is possible for a hacker to forge a pair of encryption keys, using them to deceive you into thinking that you have authenticated the sender's identity when in fact you have not. Recognizing this possibility, you have decided to write a memo to the senior vice-president of your company explaining what a certification authority is and why your company should consider using one. Draft the memo.

4. Your company is drawing up an employee terms of service agreement. One paragraph states:

> The computer network and connected devices are the property of the employer. The employer retains ownership and associated rights of all files, documents, and communications received, created, or stored by employees. The computer system is to be used for business purposes only. The e-mail system must not be used to transmit, view, or store obscene, defamatory, discriminatory, pornographic, threatening, sexually explicit, harassing, or any other offensive material. The e-mail system must not be used to duplicate or transmit copyright-protected material without the appropriate permission. At no time should confidential or trade secrets be transmitted over the Internet. The employer reserves the right to monitor e-mail communication and Internet browsing, and to make use of keystroke technologies at any time without notice. The employer retains the right to disclose an employee's personal information, e-mail communication, and Internet browsing history upon request and without notice. Violation of this policy will result in employee discipline. By using the employer's communication facilities, the employee acknowledges and consents to the above terms and conditions of usage.

Review this agreement. As a manager who is concerned about information security and intermediary liability, what is your opinion on its merits and shortcomings? What changes might be made to improve it?

5. Marcus is an employee of Scroll Networks. Alone at the office late one night with a pounding headache, deep concerns about meeting a deadline, and the knowledge that he was nowhere near finishing the assigned corporate memo, Marcus happened upon an idea. He decided that he would simulate a lightning strike on his company-issued laptop by stripping the Ethernet wire and inserting it into the 100 volt AC electrical wall outlet. Much to his surprise, he destroyed not only his laptop but also a cluster of workstations in the office. Although he stuck to his game plan, claiming that the office was struck by lightning, the hidden surveillance camera revealed otherwise. You are in charge of information security at Scroll Networks. What possible courses of action does the company have against Marcus? Assuming that you want to use the law as a means to educate employees at Scroll Networks and deter future information security breaches, which course of action will you choose, and why?

6. You are the owner of a small digital content provider based in Brandon, Manitoba. Your content is marketed under your Canadian registered trademark dFOX. As well, you are the registered owner of the dFOX.com and dFOX.ca domain names. It has come to your attention that a US software company is advertising its newest voice-mailbot under the name dFOX on its website, codeworks.com. Code Works does not have a registered trademark for the dFOX product in the US or anywhere else. The Code Works site is targeted to Americans and explicitly warns that its voice-mailbot software may only work with US telecommunications hardware. The site has a US-only 1-888 number, but allows transactions to be completed online from anywhere in the world. The terms and conditions say that the warranty for the product is valid only for sales in the US. You decide to write a demand letter to Code Works, insisting that they cease using your trademark immediately. In the letter, you indicate that, for the past several weeks, customers confused by Code Work’s use of your mark have flooded your Web server, causing e-mail transmission problems and irreparable damage to some of your corporate hardware. Code Works ignores your demand and continues to

market dFOX voice-mailbots on its website. You decide to go to a Manitoba court to seek a remedy for trademark infringement and economic loss. Outline the jurisdictional issues and tests you will be facing. What will your argument be? What can you expect Code Works to argue? As a risk manager, how can you seek to avoid legal liabilities in foreign jurisdictions?

7. As the information manager of the XACTO Standard Weights and Measurements Corp, you have received an e-mail from a party identified as koko_k@pobox.com. The e-mail asks whether you are interested in purchasing the rights to the domain name www.xacto.ca. After entering the URL into your Web browser, you determine that the site is not currently in use. You then consult CIRA's website and ascertain that the domain name was registered to a party named Koko Kerasic of Edmonton, Alberta only one week ago. Somewhat curious, you decide to respond to the koko_k e-mail, inquiring about the price. A reply to your e-mail comes only moments later demanding $75 000. As the person charged with overseeing your firm's intellectual property enforcement, you are deeply concerned about securing that domain name.

You seek preliminary advice from your lawyer, Erik, who asks whether your company owns the Canadian trademark for XACTO. Your answer is "yes." Erik then does a business search in Alberta to determine whether Koko has registered a business operating under the name XACTO. No such business name is registered. Upon further investigation, it turns out that Koko is an industrious 19-year-old high-school student who heard about cybersquatting in an ICQ chat room. Erik indicates that this matter must be resolved in accordance with the CIRA dispute resolution policy and quotes his fee for representing you in the matter. Given that your company is a financially-strapped start-up, you decide to handle the matter without representation. You point your Internet browser to www.cira.ca and review the CIRA *Domain Name Dispute Resolution Policy.* What position will you take when making XACTO's submissions to the CIRA dispute resolution provider? What argument can you expect from Koko or her parents? How is the matter likely to be resolved?

8. You work for a video game development company, CuddleTech, that has just started selling a major new game—an extreme mountain bike game called CuddleBike. Having a Web presence is a key component of the launch and the ongoing promotion and sale of the product. Although sales of the game will be international, your main market for the game is in Canada and the United Kingdom.

You are responsible for the launch of the new game, particularly in relation to the Web presence. You have arranged for CuddleBike trademark applications to be filed and your lawyer has advised you that there are no similar trademarks or business names registered in Canada. However, when you begin to looking into registering domain names, you discover that a person named Eddy had registered the domain name www.cuddlebike.com just a few days earlier. You write to Eddy by e-mail and ask him to contact you regarding the domain name. The next day, Eddy contacts you by telephone. During your conversation, he tells you that he knows a girl named Nicolle who works at CuddleTech. Eddy tells you that Nicolle mentioned the CuddleBike game to him at a party before the launch of the game. He tells you that he planned to use the domain name to develop a fan site for the game after it was released. When you ask whether he would be willing to sell the domain to CuddleTech, he says he would sell it for $200 000. He then tells you that if CuddleTech doesn’t want to buy it, he will sell it to a competitor of CuddleTech. In light of these statements, you question Eddy about his true motives in registering the domain name. He says that he will deny ever offering to sell the domain for $200 000 or to a competitor. You do not have a recording of the call.

Briefly indicate what domains you might register for CuddleTech's new game. With respect to the www.cuddlebike.com domain name, do you think that online arbitration could be an appropriate option for CuddleTech to resolve the dispute with Eddy? Assuming that arbitration could be appropriate, do you think CuddleTech should pursue litigation or arbitration? Support your answer by describing the factors that you would consider in making your decision.

9. Using the facts in the previous case problem, describe how the matter might be resolved if it were resolved under the Uniform Domain Name Dispute Resolution Policy (UDRP). The UDRP can be accessed at www.icann.org/udrp/udrp-policy-24oct99.htm.

10. You have decided to go into business as an online intermediary. Among other things, you maintain an online discussion board dedicated to financial issues and publicly-traded companies. At times—especially when stock prices drop—conversation on the discussion boards heats up, and people start to point fingers. Sometimes inflammatory and demeaning remarks are made. To maintain community standards and keep the peace online, you have on occasion directed your Web master to remove certain remarks that you believe to be defamatory. Sometimes, the decision to remove such remarks results from your own random monitoring of the discussions. Other times, the decision results from requests or demands made by discussion board participants.

Today, you received a statement of claim alleging that you are liable for defamatory statements posted on your discussion board. The claim, filed by a large corporation and its CEO, is seeking millions of dollars in damages. This is the first that you have heard of any disparaging remarks made about that company. Although you have a policy to remove postings when asked, neither the corporation nor its CEO made any such request, and no one on your staff had noticed the remarks. Needless to say you are very concerned. You immediately check the discussion group and, sure enough, six false, disparaging remarks had been posted. After checking various financial records, you see that the complaining company's stock prices plunged substantially the day after the remarks were made and have not since recovered. Is there any chance that the company might actually succeed against you? Explain why. How might a different approach to website management have reduced exposure to liability?

11. Marie-Sophie is the owner of *Tixe*—one of Canada's most exclusive online luxury stores for women. Paul is the Vice-President in charge of Online Security and you have been retained to provide legal advice. In the past six months, *Tixe* has been attacked by hackers on two occasions. There had never been attacks before. While the hacking attacks diverted some staff and technology resources for a short time, the *Tixe* online

operations were not affected and no business was lost. However, Marie-Sophie is very concerned about the attacks and has instructed Paul to ensure that the situation does not reoccur.

You know that there are vulnerabilities in *Tixe's* online ordering system which likely contributed to the fact that the attacks were not stopped at an earlier stage. You also know that although those vulnerabilities could be fixed and would stop the hackers, it would be expensive to do so and it might slow down overall system performance. But Paul thinks he has a better solution; he wants to catch the hackers in the act. To do so, he wants to install a key-logging program on the computer of every user who visits the *Tixe* website. This program would be invisible to all but the most sophisticated computer users and it would keep track of every key a user types on their computer. That information would be relayed back to *Tixe* where Paul could monitor it for suspicious patterns or activities. Paul thinks this is a real win–win solution because the hackers would be caught and *Tixe* could also use the information it gathers from marketing or other purposes. Your job is to advise Paul about whether his proposed solution is acceptable for the company from a legal perspective in light of *Tixe's* obligations under *PIPEDA*. If you do think that there are problems with his system from a privacy perspective, how might those problems be addressed?

12. The proliferation of electronic commerce has left consumer protection legislation slow to catch up. This has spurred Industry Canada to announce a policy that includes updated consumer protection principles tailored to the online environment. One of those principles is that "[v]endors should not transmit commercial e-mail without the consent of consumers, or unless a vendor has an existing relationship with a consumer." If followed, would this principle always provide more protection to consumers? As a Canadian corporation, is your business required to adopt this policy? What are the likely business consequences of adopting it and the other principles announced by Industry Canada? What are the likely business consequences of ignoring them? Develop an appropriate e-mail business practice policy statement for your company.

WWWeblinks

Intellectual Capital—Industry Canada

strategis.ic.gc.ca/SSG/pi00004e.html

This website provides information on current developments and intellectual capital through links to journal articles, research papers, and interviews.

Electronic Commerce

http://canada.justice.gc.ca/en/ps/ec

The Department of Justice site addresses proposed statutes on electronic commerce and provides links to news releases, consultation papers and reports, and other resources.

Electronic Commerce Task Force

http://e-com.ic.gc.ca/english/strat/641.html

This Industry Canada site offers information for companies involved in electronic commerce on marketplace rules—legal and commercial frameworks, financial issues and taxation, and intellectual property protection.

Privacy Commissioner of Canada

www.privcom.gc.ca/legislation/index_e.asp

This site provides links to Canadian privacy legislation, privacy guides, reference materials, and other privacy-related sites.

The Validity and Enforceability of Web-Wrap Agreements

www.law.ualberta.ca/alri/ulc/current/ewebwrap.htm

This article examines the enforceability of online contracts with respect to traditional standard form contracts and fundamental contractual requirements.

UNCITRAL Model Law on Electronic Signatures

www.uncitral.org/english/workinggroups/wg_ec/wp-88e.pdf

This document contains a draft guide to the UNCITRAL Model Law on Electronic Signatures and provides insight into the principles of electronic signatures.

Canadian Internet Registration Authority

www.cira.ca

Operating as the authority for the registration of .ca domain names, this site also provides access to its official dispute resolution policy and rules.

Internet Corporation for Assigned Names and Numbers

www.icann.org

An internationally organized non-profit organization responsible for managing the generic and country code domain name systems. Its dispute resolution policy—the UDRP—and cases decided under that policy can be viewed on its site.

Additional Resources for Chapter 19 on the Companion Website (www.pearsoned.ca/mcinnes)

In addition to self-test multiple-choice, true-false, and short essay questions (all with immediate feedback), three additional Cases and Problems (with suggested answers), and links to useful Web destinations, the Companion Website provides the following resources for Chapter 19:

Business Decision 19W—Respecting Consumer Protection

Xxxxxxx xxxxx xxxxxxx xxxxxx xxxxx
Xxxxxxx xxxxx xxxxxxx xxxxxx xxxxx
Xxxxxxx xxxxx xxxxxxx xxxxxx xxxxx

Xxxxxxx xxxxx xxxxxxx xxxxxx xxxxx
Xxxxxxx xxxxx xxxxxxx xxxxxx xxxxx
Xxxxxxx xxxxx xxxxxxx xxxxxx xxxxx
Xxxxxxx xxxxx xxxxxxx xxxxxx xxxxx
Xxxxxxx xxxxx xxxxxxx xxxxxx xxxxx

Canadian Case Study for Part 4
Art in Motion: Counterfeiting from Canada to China

Art in Motion is a Canadian success story. Twenty years ago, Garry Peters operated a small business out of his home in Coquitlam, British Columbia. He worked together with a few local artists to design, produce, and frame fine art. He continues do much the same thing today—but on a much larger scale. While he still works with local artists, he also commissions art from more than one hundred artists around the world. And instead of packaging the pieces himself, he employs more than five hundred employees and operates out of a 12 000 square metre facility in Coquitlam. From humble origins, Art in Motion now sells millions of dollars worth of fine art to purchasers in over 70 countries.

Art in Motion's future success is not, however, a sure thing. In fact, the company's very existence is threatened by every artist's worst nightmare: counterfeiters. While on a business trip to China, Garry Peters discovered that many of his company's products were being peddled on the black market. But it was only after digging deeper that he began to appreciate the enormity of the problem. Dozens of Chinese companies have sold several hundred thousand counterfeit pictures worth more than a billion dollars. Garry Peters calls that "out and out theft."

The success of the counterfeit operations is easy to understand. Art in Motion devotes a large part of its budget to the commission, design, and creation of art work. The artists are the heart of the company and they are paid accordingly. In contrast, counterfeiters

require nothing more than high quality copying machines. And because they face far lower production costs, they are able to sell their pieces at much lower prices.

Although he has been able to shut down a few of the counterfeit operations, Garry Peters realizes that the situation is getting worse. If the counterfeiters earned one billion dollars last year, they may earn twice that much next year. Peters also knows that every dollar gained by the black market is a dollar lost to legitimate operations like his own. Consequently, there is a danger that, unless the problem is solved, Art in Motion will be driven out of business. If that happens, a lot of people will suffer. Garry Peters will lose his company. Hundreds of employees will lose their jobs. Artists will lose an important source of income. And ultimately, consumers will lose access to high quality art. After all, artists will not be willing to create new works unless they have some assurance that the profits will go to themselves, rather than to counterfeiters.

Garry Peters doubts that those problems can be entirely solved simply through the enforcement of international copyright laws. The real solution, he believes, lies closer to home. Chinese counterfeiters are successful only because purchasers—especially those in North America, who form the biggest part of the world market—are willing to buy rip-off reproductions. Consumers must therefore be made to recognize the consequences of their actions. They must realize that the money that they save by buying black market art comes straight out of the pockets of the people who created the images in the first place.

Questions to Consider

Some of the difficulties facing Garry Peters arise from the fact that the counterfeiters were operating in China. To a large extent, however, the laws protecting artists are much the same all over the world. The following questions can therefore be answered on the basis of Canadian law.

1. Use the concepts of *natural scarcity* and *artificial scarcity* to explain the basic problem facing Art in Motion.

2. Art in Motion is unhappy because counterfeiters are making reproductions of *new* images. Would the situation be any different if Art in Motion were dealing with *very old* pieces of art, like Leonardo da Vinci's *Mona Lisa*, which was created 500 years ago?
3. Art in Motion sells reproductions of images that it receives from artists. In terms of copyright, does it matter whether those artists are classified as *employees* of the company, as opposed to *independent contractors*?
4. To what extent is the protection of artists' rights a matter of *morality*, rather than *law*? How effective is the law at preventing copyright violations? Have you ever broken the copyright laws?

Video Resource: "Chinese Counterfeiters: Art, Lies and Videotape" *Venture* # 906 (21 December 2003).

Additional Resources

Art in Motion

www.artinmotion.com/

This is the website for Art in Motion, the Canadian company at the heart of the story.

Art Copyright Coalition

www.artcc.org/board.html

This website belongs to the Art Copyright Coalition. Garry Peters, the founder of Art in Motion, is also the ACC's board of directors. The purpose of the organization is to protect copyright holders and to educate the public about the nature and effects of copyright in fine art.

Copyright Act

http://laws.justice.gc.ca/en/C-42/

This website contains a complete copy of Canada's *Copyright Act*, which determines the rights and obligations that arise when an artist creates a painting.

www.studiolo.org/Mona/MONA39Th.htm
This website provides several examples of how the *Mona Lisa* has been reproduced in popular culture.

Mona Lisa Images for the Modern World
http://desktoppub.about.com/gi/dynamic/offsite.htm?site=http://www.studiolo.org/Mona/MONALIST.htm
This website contains provides an entertaining demonstration of the various ways in which Leonardo da Vinci's *Mona Lisa* has been exploited in popular culture and commerce.

Tim's Journal: Public Domain
http://torque.oncloud8.com/archives/cat_public_domain.html
This website provides a brief explanation of the extent to which old images may be within the public domain and therefore open to exploitation.