CHAPTER 17
ELECTRONIC COMMERCE

CONTENTS
Teaching Approaches
Additional Teaching Suggestions
Discussion Boxes
Review Questions
Cases and Problems
Case Briefs

TEACHING APPROACHES
The attempt to understand, let alone teach, electronic commerce is reminiscent of Heisenberg’s famous Uncertainty Principle: the more precisely the subject’s position is determined, the less precisely its momentum is known. In this sense, the subject matter of this Chapter is without tradition. The regulation of electronic commerce is proceeding at a rate previously unknown by other areas of law. To take a quick example from the text, just when we began to fully understand the provisions of UNCITRAL’s Model Law on Electronic Commerce, we were forced to confront and adopt a national model law and, immediately thereafter, the enactment of nearly a dozen provincial laws, each differing in detail from the original, international model. At least a dozen more statutes will be passed in Canada during the next couple of years dealing with data protection and personal privacy. A number of other enactments will then be required to amend consumer protection legislation. A similar proliferation of regulatory frameworks is occurring in practically every country that takes business law seriously. It is not surprising, then, that we are not yet in a position to compare our teaching approach to that of other texts. Most of the other texts on business law have yet to begin approaching some of the topics in this Chapter. What your students will be reading is the third version of this Chapter. The law has changed twice already. This is truly the bleeding edge, as some entrepreneurs like to say.

The rapidity of its development is not the only thing unique to electronic commerce law. The use of digital technologies, databases and a network of networks to mediate business transactions generate a number of truly novel questions for business law. We touch on a number of these in this chapter: automated e-commerce, PKI, domain names, and intermediary liability, to name a few.

Having said all of this, it would be a mistake to conclude that electronic commerce is an entirely new area of law. It is not. Automated e-commerce and PKI are founded on contract law. The principles underlying domain names dispute resolution are modeled on trade-mark law. Intermediary liability is really just a complicated kind of tort law. In fact, you might safely predict to your students that it will not be many years before “electronic commerce” becomes, simply, “commerce.” In some sense, it already is. Still, the question: “to what extent is electronic commerce a new area of law?” provides an absolutely amazing learning opportunity for your students. We suggest that you use this question as one of the main themes in the Chapter.
As one might expect of a fledgling area of law, the topics of electronic commerce have not yet crystallized. For example, should privacy law be included under electronic commerce, or does it belong somewhere else? Are questions of information security just a subset of criminal law? Are domain name disputes really just part of intellectual property law? Are questions of internet jurisdiction simply a part of private international law?

While challenging your students to think about these big picture questions, you might inspire them to think of a few others. The internet is often described as borderless, whereas law is traditionally applied within boarders. As e-commerce law takes on a more global outlook and technologies become more and more precise, will we see a reversal of this? Is a globally coordinated regulatory scheme truly possible? Is it truly desirable? What happens when two countries disagree about a fundamental law or policy? Should one country be able to dictate its preferred laws and policies at the expense of others? And what about the features of internet communication that make it possible for people to interact with relative anonymity? Should these technologies be regulated? Anonymity provides greater freedom in the context of political speech. But it also allows child pornographers and copyright pirates to engage in illegal sales. As you can see, there are many big questions. The fact that it is not possible to address each of these in detail within the Chapter should not prevent instructors from picking and choosing some of them to sprinkle against the backdrop of the particular laws that are discussed in the Chapter. There will be plenty of occasions to do so.

Unlike many of the other Chapters in this book, the topics do not achieve unity through the application of a particular type of law. In this Chapter, it is the technologies that link the topics. This will be counter-intuitive to students who are otherwise trying to learn to categorize topics in this course by areas of law. One might explain the organization in the following way.

*Electronic commerce legislation* This section serves as an introduction to many of the legal obstacles that, if left alone, would prevent e-commerce from flourishing. You should use this section to make clear the strategy of global e-commerce: namely, the development of uniform laws that supplement traditional legal requirements with their functional equivalents. You should also use this section to introduce the concept of jurisdictionality. Although there is no express discussion of jurisdiction here, the point to be made is that each jurisdiction — in Canada that means each province or territory—has the legal authority to make its own laws. This makes the goal of harmonization difficult. If provinces vary the detail of their legislation so that it results in a different legal consequence, the harmonization process will fail. Your students might like to discuss the policy implications of this.

*Contracting online* This section brings out some of the particular issues of contract law that are peculiar to the electronic milieu. Because the original standards for contract law were set up for face-to-face interaction, students will be challenged to think about how those old rules might be applied to novel situations in the digital world, such as clickwrap
and webwrap contracts, as well as agent-mediated commerce. This section also introduces another core concern for those who wish to transact online—authentication and information security. Your students might not immediately see how security fits into a discussion about contracting. Although these topics have applications beyond e-commerce, your students must be made to see that they are essential to a fully functional commercial environment. The basic point to be made is that commerce that is not face-to-face will wither away in a world without trust. Trusted third parties will be required to authenticate transaction partners, technologies such as public key encryption will be necessary to ensure the integrity and the non-repudiation of documents. Corporate policies are also needed to ensure that information systems are not compromised by employees or the outside world.

**Online intermediaries** This section focuses on new kinds of liability for an essentially new kind of actor not previously known to traditional commerce—the online intermediary. We have limited this section to a brief introduction, mostly because the law in this area is still in the making. For starters, you can generate an excellent discussion around the distributor/publisher distinction. It will help your students grapple with the concept of the internet as a medium of communication. One additional thing that you might try to impress upon your students is that information intermediaries may be taking on additional responsibilities and duties that they did not contemplate when setting out their business plans. For example, if an online service provider collects personal information, it will owe privacy duties to its customers. In some cases, third parties will ask for that information. Sometimes it will be private sector players seeking to trade personal information. Other times it will be governments or the police trying to gather information or evidence. As there are laws being developed and implemented for the use and disclosure of such personal information, online businesses that function as intermediaries will sometimes get caught in the middle. This is something your students should know about.

**Online consumer protection** This section introduces new issues for consumers that arise in a wired world. Students will come to class with their own stories of internet scams and other questionable online business schemes. Although this will make for a fun and interesting introduction to the topic, the important thing is for your students to be able to grasp the guidelines to online consumer protection. We recommend focusing on the fact that there is some value in applying these guidelines even if they do not have the force of law. This is also a good spot to raise the question of whether a new area of law is called for, or if it is sufficient to build on existing consumer protection legislation by incorporating the online environment.

**ADDITIONAL TEACHING SUGGESTIONS**
Given the novelty of this area of the law, it is worthwhile to introduce a bit of lingo before turning to specific issues mentioned in the text. Some of your students will already know many of these as everyday words; others will be hearing these for the first time.

*Business-to-Business* (B2B) exchanges between business organizations, including purchasing and procurement, supply chain management, sales initiatives, payment
schemes, servicing, and support. Automating many of these aspects of B2B commerce can be highly beneficial to the bottom line.

*Business-to-Consumer* (B2C) exchanges between businesses and consumers, including sales, information searches, FAQs, servicing, and support. Examples of success stories in B2C include Amazon.com and Yahoo!.

*Consumer-to-Consumer* (C2C) exchanges between various consumers, including classified ads, auctions, games, and personal services. In most cases, C2C exchanges take place through an intermediary.

*Consumer-to-Business* (C2B) exchanges between a group of consumers and a business. Not unlike workers in organized labour, consumers sometimes band together to achieve greater bargaining power. Sometimes, these transactions are motivated by economics. Other times, they are motivated by social conscience.

*Government-to-Business* (G2B) exchanges between a government and a business, including licensing, sales, filings, information, tendering, and procurement. As governments continue to employ cost-cutting measures and to offload traditional services, G2B will become the norm. To the extent that businesses are set up for electronic transactions, G2B will enhance the efficiency and reduce the transaction costs of such interactions.

*Government-to-Citizens* (G2C) exchanges between a government and individual citizens, including licensing, sales, filing, information, tendering and procurement. Success in G2C requires an information infrastructure that enables access for those who lack the means to transact electronically.

Given the novelty of this area of law, it is also worthwhile to provide a brief history of its genesis for instructors less familiar with it. In fact, much of the space below devoted to additional teaching suggestions will be aimed at providing additional background for such instructors.

**Historical Developments – Electronic Data Interchange**

The history of electronic commerce dates back to the 1960s, when a group of business people from the transportation, grocery, and retail sectors decided that their costs could be substantially lowered not only by reducing the amount of paper used, but by reducing the number of human interactions involved in a commercial transaction. The aim was to standardize transaction types by devising uniform methods for consolidating purchases, developing business relationships, negotiating volume discounts, and integrating manufacturing processes. With the advent of business computers, companies were able to store and process data electronically and, as a result, needed an expedient method to communicate the data. In the early 1970s, a group known as the Accredited Standards Committee developed *standard data formats*. Standard data formats are software templates that can be used on any computer by any trading partner, over and over again without re-entering the data, in a manner that notifies the sender when the other party
receives the information. Standard data formats reduce not only transaction costs but also the number of clerical errors made in the process. The advent of this technology popularized a business process that has become known as *Electronic Data Interchange* (EDI). EDI is a means by which pre-established trading partners exchange business data electronically.

Through the use of standard data formats, companies engaged in EDI were able to translate their purchase orders, invoices, payments, shipping manifests, and delivery schedules into a globally understood business language and then transmit those documents to their trading partners. This was accomplished using secure telecommunications links provided by a private communications network known as a *value added network* (VAN). Using VANs to standardize transaction types and set out the desired terms and conditions, businesses could communicate electronically and ensure that their contracts were enforceable without having to worry about the formalities traditionally attached to paper.

Although nearly 100,000 businesses have used EDI, many have subsequently turned to the internet to achieve similar business outcomes. Besides being restricted to machine-readable messages with serious limitations in the kind of information that can be communicated, EDI is cost prohibitive for many small and medium size enterprises. Further, it is asynchronous rather than interactive and it limits commerce to other EDI-capable transaction partners. Perhaps the most serious limitation of EDI is its inability to accommodate B2C electronic commerce.

**Historical Developments – The Network of Networks**

Without question, EDI entrenched electronic commerce as a way of doing business. But it is the internet that has turned electronic commerce into a global household phenomenon. To understand the origins of the internet as a global medium, you need to be able to see the world from two very different mind-sets. These two ways of thinking are practically embedded into the very architecture of the net.

In 1969, probably right around the time that Jimi Hendrix was performing *All Along the Watchtower* at the legendary Woodstock concert, a team of engineers in Northern California were pressing a Labour Day deadline as a result of contract work owing to a US Government agency known as ARPA (Advanced Research Project Agency). While the hippies in New York danced in the mud and sang about free love, the engineers from Northern California were testing an idea known as packet-switching. It was hoped that this idea, along with an untold amount of telephone wire, would allow research institutions to share scarce computing resources. The idea was to find a way to break digitized information into little pockets and send it through various nodes in a communications network to some end point where it would be reassembled. As Vint Cerf (an early telecom pioneer) described it: “It’s like writing a message on a whole lot of postcards. You send one postcard by US mail, one by Federal Express, one by bicycle courier, and so on. If one comes back for some reason, you send it by a different route, and once all the parts of the message are collected at the recipient’s address, there’s a postcard that explains what order you read them in”*: quoted in M. Friedman *Fuzzy Logic*:
Chapter 17 – Electronic Commerce

*Dispatches From the Information Revolution* (1997) at 35. By successfully developing a means of routing and then reassembling packets of information, research scientists would be able to make the most efficient use of scarce computing resources and expensive telephone lines.

It is important to understand that the packet-switching experiment was originally based on the idea of sharing. Sharing represents the first mind-set embedded into the architecture of the internet. Eventually, what these scientists figured out was that the best way to share resources is through a decentralized medium. Recognizing that systems of control are systems of exclusion, it was determined that the best way to pass information around a network is to structure the network so that it is not subject to centralized points of control. For this reason, the packet-switching model was integrated into a redundant network. The idea was to build a web of redundant connections so that if any particular node was blocked or removed, the desired information could still travel freely through remaining nodes in the network to its ultimate destination. This idea was reinforced by others who were interested in building a network that could withstand a nuclear strike.

Once packet-switching was perfected, it was up to the community of engineers to establish a common language — a series of protocols¹ — that would allow different parties’ commands and communications to interface with one another. Later, with the advent of the personal computer, other protocols were developed to allow people to communicate from remote locations through devices attached to their computers known as modems. What is remarkable about these protocols is not that they were developed but how. Unlike the computer software and hardware that we all use on a daily basis, the early protocols were non-proprietary. In other words, none of the engineers who created them claimed an exclusive legal right to use, copy, or market them. In fact, as one author has put it, “[t]he Net’s developers were its users, developing tools as the need arose. If the software worked, it was shared by everyone and adopted by the community as a whole. If it didn’t, it was quickly forgotten.” The mind-set represented by this open sharing of software might be described as a kind of cooperative anarchy. Because it was as free as the air, others borrowed from and contributed to these software protocols, building layer upon layer to create points of access that eventually allowed the ARPA Net to evolve into a *network of networks* with the ability to host newsgroups, list servers, email and, ultimately, web sites.

The second mind-set did not fully express itself until the original ARPA network had all but crumbled, taking the National Science Fund’s (NSF) *Acceptable Use Policy* down along with it. At the time it assumed partial funding for the internet’s backbone, NSF proclaimed that it was unacceptable to use the network for private business or other for- ²

¹ *Eg Transmission Control Protocol/Internet Protocol (TCP/IP).* “IP is responsible for moving packet of data from node to node. IP forwards each packet based on a four byte destination address (the IP number). The Internet authorities assign ranges of numbers to different organizations. The organizations assign groups of their numbers to departments. IP operates on gateway machines that move data from department to organization to region and then around the world. TCP is responsible for verifying the correct delivery of data from client to server. Data can be lost in the intermediate network. TCP adds support to detect errors or lost data and to trigger retransmission until the data is correctly and completely received.” See <http://www.yale.edu/pclt/COMM/TCP/IP.HTM>.
profit activities. But once the NSF ceased to fund the network, it became a kind of free-for-all. The internet was finally open for business.

Enterprise, however, required a different kind of architecture — one that looks flashy, is user-friendly, and has proprietary sensibilities. Recognizing that commerce does not bide well in a cooperative anarchy, some commercial software developers took a very different tack than the one taken while the hippies were frolicking in the mud at Woodstock. Rather than developing architectures of freedom, companies like America Online and Microsoft started to develop architectures of control. We are no longer free to roam the web world-wide. There are now many roadblocks on the information superhighway. Many sights are password-protected; others require VISA numbers or the disclosure of personal information through cookies. These proprietary architectures will become more and more prevalent as commerce becomes more deeply entrenched online. They represent the second mind-set embedded into the architecture of the net. And it should come as no surprise that there are two mind-sets; recall Stewart Brand’s jingle set out in the previous chapter: “Information wants to be free. It also wants to be expensive.”

Although not without resistance from the open source software movement, the internet has more recently shifted from the early architectures of freedom to architectures of control. Without some element of control, electronic commerce would not be possible. The source of such control, however, does not rest solely in the hardware and software that form the infrastructure of the internet. It also comes from law. Recognizing that electronic commerce cannot flourish unless those interacting in the marketplace are subject to the rule of law, many jurisdictions have begun to enact electronic commerce legislation. Such legislation aims not only to provide certainty, it aims to provide a measure of control. It is now time to investigate the means by which legislative control is achieved.

Privacy
Because the provincial legislation is still in the making, we decided not to dedicate space to a separate section on privacy in the Chapter. Our brief introduction to privacy is limited to Ethical Perspectives 17.1. No doubt, the next edition of the book will have a substantial amount of space dedicated to this topic. But we do recognize that some instructors will want to discuss privacy with their students now. For those who do, here is some material, written in language similar to the text.

The Federal Personal Information Protection and Electronic Documents Act
Although the provinces generally govern the regulation of commerce, there is one piece of federal legislation that plays a critical role in the regulation of electronic commerce:

[2] “Cookies are pieces of information generated by a Web server and stored in the user's computer, ready for future access. Cookies are embedded in the HTML information flowing back and forth between the user's computer and the servers. Essentially, cookies make use of user-specific information transmitted by the Web server onto the user's computer so that the information might be available for later access by itself or other servers. In most cases, not only does the storage of personal information into a cookie go unnoticed, so does access to it. Web servers automatically gain access to relevant cookies whenever the user establishes a connection to them, usually in the form of Web requests.” See <http://www.cookiecentral.com>.
the Personal Information Protection and Electronic Documents Act (PIPEDA). This Act serves three broad ends. First, it protects privacy rights by regulating the manner in which personal information can be collected, used or disclosed in certain circumstances. Second, it facilitates electronic commerce by providing for the use of electronic means to communicate or record information or transactions. Third, it makes several important amendments to the Canada Evidence Act, the Statutory Instruments Act, and the Statute Revision Act.

PIPEDA must be understood as Parliament’s attempt to protect the informational privacy interests of all citizens through a balancing of three different interest groups: (i) consumers; (ii) businesses; and (iii) the international community. PIPEDA extends to all federal works and undertakings and, as of 2004, it extends to all commercial activity in every province, with the exception of those provinces who choose to enact their own similar legislation. PIPEDA defines “personal information” as information about an identifiable individual, but does not include the name, title, or business address or telephone number of an employee in an organization. The Act protects personal information by adopting the 10 principles developed by the Canadian Standards Association (CSA) in its International Model Privacy Code. These principles are summarized below in the Figure below.

<table>
<thead>
<tr>
<th>CSA Privacy Principles Adopted in PIPEDA*</th>
</tr>
</thead>
<tbody>
<tr>
<td>Accountability</td>
</tr>
<tr>
<td>Identifying Purposes</td>
</tr>
</tbody>
</table>

---

3 SC 2000, c 5.
4 RSC 1985, c C-5.
5 RSC 1985, c S-22.
6 RSC 1985, c S-20.
7 For example, the European Union has issued a privacy directive that will preclude European businesses from doing business with foreign companies that do not meet certain minimum privacy standards. EC, Parliament and Council Directive 95/46 of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, [1995] OJ L 281/31 Art 25(6).
| **Consent** | Except where inappropriate, the knowledge and consent of the information subject is required. Information collected for one purpose cannot generally be transferred or used for another purpose without knowledge and consent. Implied consent may be appropriate for insensitive information. Exceptions exist where: (i) a crime is being investigated; (ii) for journalistic, artistic or literary purposes; or (iii) the information is publicly available. |
| **Limiting Collection** | Collection of information must be limited to whatever is necessary to achieve the identified purpose of collection and must be collected by fair and lawful means. |
| **Limiting Use, Disclosure, and Retention** | Personal information shall not be used or disclosed for purposes other than which it was collected. A number of exceptions exist including disclosure for research purposes, criminal investigation, and emergency situations. Guidelines and procedures regarding the retention of personal information should be developed, including a procedure for destroying personal information, the retention of which is no longer necessary for the fulfilment of its original purpose. |
| **Accuracy** | Personal information collected must be accurate, complete and up-to-date. Organizations may only update information in order to achieve the original purpose for which it was collected. |
| **Safeguards** | Organizations that collect personal information must implement security safeguards (appropriate to the sensitivity of the information) that protect against: (i) loss or theft; and (ii) unauthorized access, disclosure, copying, use, or modification. Protective safeguards include: (i) physical measures (locks); (ii) organizational measures (security clearance policies); and (iii) technological measures (firewalls, passwords, encryption). |
| **Openness** | Organizations collecting personal information must make its policies and procedures available to all members of the organization. Notification of the existence of policies is insufficient. The policy must include: (i) the name and address of the person accountable for the policies; (ii) a description of the type of information held and a list of those entitled to access that information. |
| **Individual Access** | Unless it interferes with the privacy rights of others, law enforcement, or client-solicitor confidentiality, individuals have the right: (i) to obtain access to personal information that has been collected about them; and (ii) to find out how that information has been used; and (iii) to find out to whom such information has been disclosed. Where an individual finds errors in personal information, the organization must correct the error. |
Challenging Compliance

Where he or she believes that personal information is being collected, used, disclosed or retained in a manner contrary to the privacy requirements, any individual (whether an information subject or not) can institute a challenge against the person named accountable for an organization’s collection of personal information.

* Extracted from Schedule 1 of Personal Information Protection and Electronic Documents Act, 2000, c 5.

**PIPEDA** sets out a number of remedies that are available when the rules protecting personal information are breached. Enforcement of these rules, and the request for remedies, can be triggered by individual complaints, or as a consequence of an audit by the Office of the Privacy Commissioner. In its investigation, the Privacy Commissioner’s office may compel evidence, administer oaths, and search business premises. Upon completion of the investigation, the Privacy Commissioner’s office must prepare a report, unless it is satisfied that the complainant should exhaust internal grievance procedures first, or if too much time has lapsed. The Privacy Commissioner has no actual powers to enforce any recommendations or orders in the report. Therefore, either the complainant or the Commissioner must apply within 45 days to the Federal Court (Trial Division) for a remedy. The Court may order an organization to: (i) change its practices, (ii) publish a notice of action taken, or (iii) award damages (including damages for humiliation). Finally, **PIPEDA** affords protection to *whistleblowers*. A whistleblower is someone who reveals something covertly or who informs against another. An employer may not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee by reason that he or she reported a violation of the Act or refused to violate the Act. If the organization does so, or if the organization destroys documents after an individual has launched a complaint, it may be fined up to $100,000.

The next exercise allows students to investigate the ethical implications of **PIPEDA**.

**Ethical Perspectives**

**Whistleblowing**

Evelyn became the supervisor of the HCSC mailroom, reporting to her manager Don. On Friday, October 23, three mailroom employees found a large box of three-month old retired railroad-worker beneficiary claims that had not been forwarded to Travelers Insurance Company as required. Evelyn immediately contacted Don, informed him of the discovery of the claims, and requested his direction in handling the situation. That afternoon, Don contacted Evelyn and directed her to bring the box of

---

9 Though the Commission may not search dwelling homes, leaving uncertain the approach for home-based businesses.

claims to his office. When she reached Don’s office, she noticed that a paper shredder was sitting over a wastebasket. Don informed Evelyn that the two of them were going to shred the claims. Evelyn emphatically stated she would not assist him in shredding the claims and that it was wrong. She suggested they contact HCSC officials for instructions on how to proceed. Don refused and instructed Evelyn that she was never to tell anyone about the claims shredding. He stated that if she did, he would assert that she was the one who had actually shredded the claims, and that everyone would believe him rather than her. When she attempted to leave Don’s office, he told her to consider herself fired once she left. After shredding the last claim, Don placed the scraps in ten to twelve large, green garbage bags which he discarded in a dumpster located at the back of the building. When Evelyn reported for work the following Monday, October 26, she went to Don to discuss her concerns about the claim shredding. She told Don that destroying the claims was improper and illegal and would prevent the beneficiaries from receiving their Medicare benefits. In response, Don again threatened that if Evelyn ever reported his actions he would tell everyone that she had been the one who did the shredding, and he personally would ensure that she went to prison. Evelyn ultimately went directly to HCSC’s Vice-President and former Director of Operations, to report the destruction of the claims. However, he participated in the cover-up of the shredding and declined to take any action against Don for his actions. He instructed Evelyn that she should cease worrying about the claims.

Questions For Discussion
1. Does Evelyn have a moral duty to blow the whistle?
2. Does she have a legal duty to file a complaint with the Privacy Commissioner? Why or why not?
3. What other means might Evelyn use to address the problem?
4. If you were a Federal Court judge and the evidence before you confirmed the Privacy Commissioner’s report that these events actually transpired, what remedies would you award and to whom?

Answers
1. Evelyn does have a moral duty to report the shredding of the documents. Although she had no idea that Don would take the documents and shred them and although she did not have the power to prevent the illegal act, by giving the files to Don, she enabled the act. Further, because she was the only person other than Don who knew about the victims’ entitlement, a failure to report what happened would prevent the victims from being able to make claims that they were entitled to make. Silence in this case would be a kind of omission and can only be seen as morally impermissible. This is especially true in light of the fact that Evelyn’s job is protected by PIPEDA. Although it would not make her popular amongst those in the company willing to cover up the situation, disclosing the
cover-up is the right thing to do. It is unclear why or whether she would want to continue working there in any event.

2. The legislation must require companies to designate a person who will be accountable for legislative compliance and implementing internal policies that: (i) protect personal information, (ii) establish a complaints procedure, and (iii) provide staff with adequate training. It is not clear from the facts whether Evelyn was the person accountable under the Act. If she was, then she did have a legal duty to file a complaint. If she is not the accountable person, the legislation does not expressly require her to report, though one might try to infer such a duty, based on the stipulation that employers may not dismiss, suspend, demote, discipline, harass or otherwise disadvantage an employee by reason that he or she reported a violation of the Act or refused to violate the Act. Although inferring such a duty is something of a stretch, it remains the case that Evelyn is morally bound to tell even if she is not legally bound. This is especially true when one considers that she knew those who were in fact legally obliged to report the incident had knowingly and in bad faith decided not to do so.

3. Although Evelyn was powerless to address the problem from the perspective of her position in the company, she could have considered leveraging external political power. One way that she could have achieved this is through cooperation with the media. The press can sometimes operate as a kind of ombudsperson, given individuals who otherwise lack power the opportunity to be heard by broadcasting the issue to the greater public. By placing the issue within the public eye, Evelyn might have been easier able to convince the powers that be to “do the right thing.

4. If I were a Federal Court judge and the evidence before me confirmed that these events actually transpired, I would order the company to refrain from destroying an such claims in the future, and draft a new policy accordingly. I would also award damages to Evelyn for humiliation. Finally, I would fine the company in the nature of $100 000 for their egregious conduct.

Part 2 of PIPEDA provides for the use of electronic alternatives where federal law contemplates the use of paper to record or communicate information or transactions. Although there is a level of detail that differentiates the federal approach from that of various provinces, those differences will not be discussed here. Businesses engaging in federal works and undertakings, or private sector companies carrying on business in a province or territory that has not enacted electronic commerce legislation, should make themselves aware of the details of these provisions. The remainder of the federal legislation deals primarily with detailed amendments to the Canada Evidence Act, the Statutory Instruments Act, and the Statute Revision Act. None of these amendments will be discussed here.

**Public Key Infrastructure**
You may wish to have some additional background information about public key infrastructures. Here is some, presented in the style used in the text.
The invention of public key cryptography is generally credited to Diffie and Hellman in the mid 1970s. A PKI usually consists of: (i) a certification authority (who issues the digital certificate), (ii) a registration authority (who authenticates the identity or other attributes of the certificate holder), (iii) one or more directories where the certificates are held, and (iv) a certificate management system. The primary documents of a PKI are its Certification Practice Statement, governing its operations; the Subscriber Agreement, which governs the legal relationship between the certification authority and the end user; and the Certificate Policy, which governs the use of digital certificates.

As it is suggested in the Chapter, if you want to send me an encrypted message using public key cryptography, you simply need to get hold of my public key and use it to encrypt and send the message, thereby turning plaintext into ciphertext. Once your ciphertext arrives in my inbox, I then use my private key to decrypt the message so that I can read it. Only I can decrypt it, since I alone control my private key (I will not share my private key, both for obvious security reasons and also because doing so would be a breach of the typical Subscriber Agreement that everyone using PKI is required to sign). You should point out to your students that the public key is irrelevant to the decryption process. Viewed the other way round, if I want to send you a message, I can obtain your public key from a public directory hosted by your certification authority and encrypt a message, for your eyes only. Once that message arrives, you then decrypt it with your private key. By making it computationally unfeasible for anyone without a matching private key to decipher our message, we can use PKI to enhance the security of our transactions.

But what justification do I have for the assumption that the public key that I used to decrypt the message was your public key? Key pairs can be created using sophisticated techniques devised by Rivest, Shamir and Adelman (RSA), but are very easy to produce given the necessary software which is freely available. Therefore, there is little to prevent a rogue from creating a key pair and sending that public key directly to me or to a public directory claiming that it is your private key. The rogue could then sign and send a message to me, using the public key that he created, claiming that it was signed by you, when in fact it was not. Unaware of the scam, I might verify the message using the public key that I think belongs to you, and be fooled into verifying the signature and message as belonging to you.

This is why a trusted third party is necessary. Here, the role of the certification authority is crucial. After you create your key pairs, you send your public key to a certification authority, that assures itself that the corresponding private key is in your custody and will be used only by you. It adds your name, an expiry date, a serial number and whatever other information it wants to the public key and signs that document with its private key. The resulting document is the digital certificate. It then makes your digital certificate, containing your public key, available on its public directory.

Now, if you send me your digital certificate in conjunction with a message, I can use the certification authority’s own digital certificate to validate your certificate. In other words,
since the certificate is just an electronic document, I will decrypt the certification authority’s signature on your certificate and compare it to your certificate contents and also determine whether the certificate has expired or been revoked. In that way, I can verify that the certificate and enclosed public key, in fact, belongs to you and is still valid.

Here is a chart that summarizes the PKI processes discussed in the text and in the instructors’ manual.

<table>
<thead>
<tr>
<th>Public Key Cryptography</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Action Desired</strong></td>
</tr>
<tr>
<td>Send an encrypted message</td>
</tr>
<tr>
<td>Send an encrypted signature</td>
</tr>
<tr>
<td>Decrypt an encrypted message</td>
</tr>
<tr>
<td>Decrypt an encrypted signature (authenticate the sender)</td>
</tr>
</tbody>
</table>

Space constraints in the text did not allow us to elaborate fully on some of the key uses of PKI in electronic commerce. Here is a further elaboration that some instructors might like to bring into the classroom.

**Electronic Cash**

Perhaps the most difficult challenge facing the traditional clearing and settlement system is direct payment using electronic cash. One well-known example of electronic cash is Chaum’s digicash: D Chaum “Achieving Electronic Privacy.”[^11] Thus far, the digicash concept has not been successfully adopted.

Before explaining a simplified version of the digicash system, it is useful to recall how traditional cash works. Pick up a $5 bill and have a good look at it. At first glance, the bill in your hands seems like little more than a very durable and colourful piece of paper created by the Royal Canadian Mint. If you look closely at the $5 bill, however, you will see that it has a very intricate pattern and a unique serial number. These features make it extremely difficult to forge. In part, the difficulty is a function of the pattern on the paper. As a tangible commodity, it is not easily replicated in part because of the complicated numerical sequences on the bill. These make the bill unique. Electronic notes are quite the opposite — they are easy to replicate and quite difficult to render unique. The challenge for digicash, then, is to find a way to make electronic bills act like paper cash.

On the simplest model of digicash, for example, Alicia would create a bank account. She would then create an electronic note that says, “this is $5e,” and electronically sign the note to ensure against forgery. In addition to an electronic signature, it is necessary to make each electronic note unique, by attaching a serial number. The unique serial number ensures that the note is not spent more than once. Fortunately, this process is now technically possible using public key cryptography. Still, there remains a problem. If Alicia is simply left to create as many notes as she wishes, there is no way to ensure that the total number of notes that she might create is backed by sufficient funds in her account. What is needed is a system that enables her bank to debit corresponding funds from her account. Another feature that is needed in order to replicate the function of paper cash, is a means by which to make the digital cash untraceable. After all, no one would use digital cash as cash if it were possible for someone to create a record of absolutely everything that they bought. They can already do that without a need for digital signatures through the credit card system.

Alicia, therefore, must be able to blind the serial number. Blinding ensures that a bank will not be able to trace the note back to a particular purchase. Only slightly modifying Caesar’s original encryption technique, this is accomplished by digitally signing the note in a way that hides the serial number so that the bank can’t see it. Once all of this has been accomplished, and the bank is able to verify Alicia’s note and debit her account, it can send the note back with its own digital signature so that Alicia can finally go online and spend it. Let’s say that Alicia decides to pay for a good purchased from Bassinio. Alicia simply sends the electronic note to Bassinio, via the internet or otherwise. To deposit the money represented by the note, Bassinio submits his note to the bank. The bank verifies the signature on the note as its own and checks to see if a note bearing that serial number has been spent. If it has not already been spent and the signature is valid, Bassinio’s account is credited.

So, to recap, Alicia creates $5e with a unique serial number, digitally signs the note, blinds its serial number and sends it to her bank. The bank authenticates her signature and then strips it from the note, signs the note with its own signature, debits her account, and sends it back to her. She may then take the note and send it to an online merchant in exchange for goods or services. Once received, the merchant sends the note to the bank and its account is credited.

Secure Credit Payments
Given the complexity of digital cash systems, none have yet become popular. Electronic payments sent over the internet are predominantly facilitated using credit services such as Mastercard, VISA and American Express. Although most people are comfortable with the use of a credit card, they are often less comfortable handing out their credit card numbers on open networks. To facilitate the growth of electronic commerce, it is necessary to create infrastructures that ensure secure credit payments. This has been accomplished by sending payment messages over the internet between a server and the customer computer using Secure Sockets Layer (SSL). Secure Sockets Layer (SSL) is an implementation of public key cryptography for transferring information via hypertext transfer protocol (http), the protocol used by web browsers for transferring information.
Such payment services are secure, thus ensuring confidentiality of the payment messages and non-disclosure of credit card numbers. Notice that SSL encrypts information in the transmission but with only one-sided authentication: only the server, and not the customer, authenticates itself. Unlike digicash, secure credit payments do not require a full implementation of PKI and are therefore much less cumbersome.

**Alternative Payment Intermediaries**
So far, we have seen two different kinds of electronic payment schemes. The first kind, Digicash, requires the cooperation of traditional payment intermediaries such as banks, trust companies, and credit unions. It is premised on a debit system that withdraws money from an already existing account. The second kind, secured credit payment systems, requires the cooperation of credit card institutions. It is premised on a credit system that does not withdraw money but instead exacts an undertaking for future payment. With the advent of electronic commerce, a number of entrepreneurs have invented alternative payment intermediaries. Rather than using debits or credits themselves, these institutions layer their services on top of a traditional payment infrastructure by demanding cash-in-advance and, then, holding that money in trust.

*Hyperwallet* is an interesting example of an alternative settlement intermediary: <http://www.hyperwallet.com>. *Hyperwallet* allows a person to pay for goods and services using Canadian dollars. But, unlike the credit card system, *Hyperwallet* has the advantage of allowing a purchaser’s identity to remain anonymous. In order to make this system work, *Hyperwallet* has registered itself with a number of financial institutions in Canada. If you wish to use their services, you fill-up your own hyperwallet with cash by causing your bank to debit the cash from your bank account and transfer it to Hyperwallet's trust account at a Canadian Chartered Bank. *Hyperwallet* will hold onto and keep records of all transferred amounts, acting as a kind of trustee on your behalf. Whenever you want to use cash from your hyperwallet to pay merchants for goods or services purchased online, *Hyperwallet* will record the respective changes in your account and the merchant’s beneficial interest in the trust funds as a result of the payment. With *Hyperwallet* acting as a trusted intermediary, the merchant does not need to know who you are or authenticate your identity. Thus you can spend electronic money as though it were cash. As the trusted holder and record-keeper of your electronic cash, *Hyperwallet* can facilitate payments without ever becoming a deposit-taking institution.

**The Canadian Payments System**
The Canadian Payments System is a network of complementary and competing services facilitating the exchange of some means of payment, usually in return for goods, services, or assets. While most payments are made directly by tendering bills of exchange or coins, the Canadian Payments System is primarily concerned with enabling indirect transfers of value, such as cheques, using financial institutions as payment intermediaries. Pursuant to the *Canadian Payments Association Act*, the Canadian Payments Association (CPA) has been given two mandates: (i) to set up and run the national clearing and settlement system; and (ii) to plan the evolution of the payments system: *Canadian Payments Association Act* RSC 1985 c C-21.
Given its decentralized, open-ended architecture and anarchic underpinnings, the internet presents a number of serious challenges to traditional payment systems which were designed to operate on private networks subject to strict control by the CPA. Given the relative inexperience of the CPA in dealing with an open network, business managers and employees in the finance sector must carefully observe the proposed amendments to the *Canadian Payments Association Act*, which would provide the CPA with the authority to implement a PKI for the payments system.

**Information Security**

You might find that the following chart provides further useful background for a number of the concepts discussed in the Chapter under the heading of Information Security.

<table>
<thead>
<tr>
<th>Service</th>
<th>What does the service do?</th>
<th>Example for secure electronic mail</th>
</tr>
</thead>
<tbody>
<tr>
<td>Authentication Service</td>
<td>Assures identity of the entity and the information</td>
<td>Alicia verifies Bassinio’s signature and validates Bassinio’s digital certificate. Bassinio trusts the certification authority.</td>
</tr>
<tr>
<td>Access Control Service</td>
<td>Assures that no unauthorized access takes place</td>
<td>Alicia requests access by digitally signing a message and sending it to service. Service verifies the signature and checks a list to see if Alicia is authorized to access information system.</td>
</tr>
<tr>
<td>Confidentiality Service</td>
<td>Assures that information is not disclosed to unauthorized persons</td>
<td>Alicia encrypts her message to Bassinio with Bassinio’s public key. Only Bassinio can decrypt the message with his private key.</td>
</tr>
<tr>
<td>Data Integrity Service</td>
<td>Protects against tampering with information</td>
<td>Alicia electronically signs her message. Bassinio verifies her signature by decrypting Alicia’s signature and comparing it to a “hash” of Alicia’s message.</td>
</tr>
<tr>
<td>Non-repudiation Service</td>
<td>Assures that a party to a transaction cannot later deny that the transaction did not occur</td>
<td>Bassinio has authenticated the message and the sender and Alicia has signed a contract that any use of the private key is her use of it.</td>
</tr>
</tbody>
</table>

**Domain Names**

There is no doubt that many of your students will want to know more about the infrastructure that governs the domain name system on the internet. Here are a couple of Figures that you might find useful.
### Summary of gTLDs and ccTLDs

<table>
<thead>
<tr>
<th>Universal TLDs</th>
<th>Country-Code TLDs</th>
</tr>
</thead>
<tbody>
<tr>
<td>.aero</td>
<td>.au</td>
</tr>
<tr>
<td>.biz</td>
<td>.ca</td>
</tr>
<tr>
<td>.coop</td>
<td>.cn</td>
</tr>
<tr>
<td>.com</td>
<td>.ge</td>
</tr>
<tr>
<td>.edu</td>
<td>.fr</td>
</tr>
<tr>
<td>.gov</td>
<td>.il</td>
</tr>
<tr>
<td>.info</td>
<td>.in</td>
</tr>
<tr>
<td>.int</td>
<td>.it</td>
</tr>
<tr>
<td>.mil</td>
<td>.jp</td>
</tr>
<tr>
<td>.museum</td>
<td>.kr</td>
</tr>
<tr>
<td>.name</td>
<td>.mx</td>
</tr>
<tr>
<td>.net</td>
<td>.ru</td>
</tr>
<tr>
<td>.org</td>
<td>.pr</td>
</tr>
<tr>
<td>.pro</td>
<td>.uk</td>
</tr>
<tr>
<td>.ws</td>
<td>.us</td>
</tr>
</tbody>
</table>

#### ICANN Uniform Domain Name Dispute Resolution Policy (UDRP)*

UDRP sets out the terms and conditions for the resolution of a dispute concerning the registration and use of an ICANN-governed gTLD.

Any person or entity may initiate an administrative proceeding by submitting a complaint in accordance with the UDRP to any dispute resolution provider approved by ICANN.

Owners of ICANN-issued domain names are required to submit to a mandatory administrative proceeding with respect to the following complaints:

(i) the domain name is identical or confusingly similar to a trademark or service mark in which the complainant has rights; and

(ii) the registered owner has no rights or legitimate interests in respect of the domain name; and

(iii) the domain name has been registered and is being used in bad faith.

NB: The complainant must prove the presence of each of these three elements.
Evidence of registration and use in bad faith shall be gathered from the presence of the following circumstances:

(i) the registered owner has acquired the domain name primarily for the purpose of selling, renting, or otherwise transferring the domain name registration to the complainant who is the owner of the trademark or service mark or to a competitor of that complainant, for valuable consideration in excess of its documented out-of-pocket costs directly related to the domain name; or

(ii) the owner has registered the domain name in order to prevent the owner of the trademark or service mark from reflecting the mark in a corresponding domain name, provided that the owner has engaged in a pattern of such conduct; or

(iii) the owner has registered the domain name primarily for the purpose of disrupting the business of a competitor; or

(iv) by using the domain name, the owner has intentionally attempted to attract, for commercial gain, Internet users to its website by creating a likelihood of confusion with the complainant’s mark as to the source, sponsorship, affiliation, or endorsement of its website or of a product or service on its website.

As a registered owner, you may demonstrate your rights and legitimate interests in the domain name by proving that:

(i) you made preparations to use the domain name or a name corresponding to the domain name in connection with a bona fide offering of goods or services; or

(ii) you (as an individual, business, or other organization) have been commonly known by the domain name, even if you have not acquired a trademark or service mark rights; or

(iii) you are making a legitimate non-commercial or fair use of the domain name, without intent for commercial gain to misleadingly divert consumers or to tarnish the trademark or service mark at issue.

The remedies available to a complainant include the cancellation of the defendant’s registered ownership of the domain name or the transfer of ownership and registration of the domain name to the complainant.

* ICANN <http://www.icann.org/udrp/udrp-policy-24oct99.htm/>

CIRA Draft Dispute Resolution Policy*

The draft DRP sets out the terms and conditions for the resolution of a dispute concerning the registration and use of a dot ca domain name.

The party initiating the complaint must satisfy the Canadian Presence Requirements for registration in respect of the domain name that is the subject of the complaint.

Following receipt of CIRA’s notice of a complaint, the domain name that is the subject of the complaint is prohibited from being cancelled or transferred to another person.

Owners of CIRA-issued domain names are required to submit to a mandatory administrative proceeding with respect to the following complaints:

(i) the domain name is confusing with respect to a mark in which the complainant had rights prior to the date of registration and continues to have such rights; and

(ii) the registered owner has no legitimate interests in the domain name; and

(iii) the domain name has been registered in bad faith.

NB: The complainant must prove the presence of each of these three elements
A registrant will be considered to have registered a domain name in bad faith if and only if:

(i) the registrant has acquired the domain name for the purposes of selling, renting, licensing or otherwise transferring the registration to the complainant, or the complainant’s licensor or licensee of the mark, or to a competitor of the complainant or the licensor or licensor for valuable consideration in excess of the its actual costs;

(ii) the registrant has acquired the domain name in order to prevent the complainant, or the complainant’s licensor or licensee of the mark, from registering the mark as a domain name, provided that the registrant has engaged in a pattern of obstructing owners of rights in marks from registering them as domain names; or

(iii) the registrant has acquired the domain name for the purpose of disrupting the business of the complainant, or the complainant’s licensor or licensee of the mark, who is a competitor of the registrant.

The registered owner may establish a legitimate interest in the domain name in dispute if, and only if, it can demonstrate that prior to the time of complaint that:

(i) it used the domain name in Canada in good faith as a mark and had rights in the mark;

(ii) it used the name in Canada in good faith in association with any wares, services or business and the domain name was clearly descriptive in Canada in the English or French language of (a) the character or quality of the wares, services or business; (b) the conditions or of the persons employed in the production of the wares, performance of the service or operation of the business; or (c) the place of origin;

(iii) it used the domain name in Canada in good faith in association with any wares, services, business or non-commercial activity and the domain name was understood in Canada to be the generic name thereof in any language;

(iv) it used the domain name in good faith in Canada in association with a non-commercial activity including, without limitation, criticism, review or news reporting;

(v) the domain name comprised the legal name of the registrant or was a name, surname or other reference by which the registrant was commonly identified; or

(vi) the domain name was the geographical name of the location of the registrant’s non-commercial activity or place of business.

- The remedies available to a complainant include the cancellation of the defendant’s registered ownership of the domain name or the transfer of ownership and registration of the domain name to the complainant.

- If the registrant is successful in proving that the complaint was filed for the purpose of attempting, unfairly and without colour of right, to cancel or obtain a transfer of domain name in dispute, the complainant may be ordered to pay five thousand dollars to the resolution provider in trust for the registrant in order to defray costs reasonably incurred.


DISCUSSION BOXES
Ethical Perspectives 17.1
Online Privacy
1. Dale and Bruce have willingly undertaken to disseminate people’s phone conversations over the internet. Assuming that some people exchange personal information when they talk on the phone, there is the possibility of violating PIPEDA by disclosing personal information
without knowledge or consent. However, Dale and Bruce may find refuge under PIPEDA’s exception for information that is publicly available or, though it is something of a stretch, perhaps the exception for artistic purposes. It will be difficult to succeed in proving that what they are doing is artistic. Though they will argue that they had created reality-based entertainment programming, there is little artistry in this unless they did something in addition to re-transmitting the broadcast signals. If they are not able to show some artistic merit or that the information was not publicly available, they will very likely have transgressed PIPEDA.

2. This argument helps to illustrate the greater issue of the appropriate legal response to rapid technological change. Information technologies such as the internet and email have had a tremendous effect on the security of personal information in electronic form. However, provided that use of a tool for a specific purpose has not been prohibited, people are entitled to innovate at will. Dale and Bruce make a good point by establishing that the scanner used to pick up the conversation was obtained legally with no restrictions in its terms of use. In light of these circumstances, perhaps the PIPEDA requirement should also explicitly prohibit the broadcasting of personal information.

3. When discussing this question, students should be encouraged to note:
   • Canadian citizens have a right to be protected from the unauthorized disclosure of their personal information.
   • The need to protect the rights of Canadian as data-subjects becomes even more pressing and substantial as our culture is transformed into a surveillance society.
   • Dale and Bruce should consider the Kantian idea that people should act only upon those maxims that they would choose to make universal. If everyone where to transgress the private sphere by doing what Dale and Bruce are doing, that very meaningful space in our lives would quickly fade away.
   • The disclosure of personal information may have all sorts of unintended harmful consequences as the information collected can be later used for different purposes.

Business Law in Action 17.1

Parody Web Sites
1. Students should be able to recognize that while some critical expression is legal, the law prohibits expression that actually injures its target. For example, conveying a true though gruesome fact about someone is defensible, even if that fact causes injury to another’s reputation. Businesses that lose profits as a result of unfavourable yet accurate publicity have no recourse under law. However, the dissemination of an unsubstantiated rumour, especially if the rumour injures a person’s or a business’ reputation, is a reprehensible practice that is not generally protected by freedom of expression. Consumers who unjustifiably lash out at corporate entities or otherwise wilfully manipulate their business affairs could and should face legal sanctions.

2. Arbitration may have been avoided by:
   • Seeking to work with Ken in developing a bona fide consumer complaint site for Wal-Mart Canada.
• Offering to buy the domain name from Ken at a price equal to, or less than, the cost of arbitration.
• Commencing an action for defamation against Ken in the court system.

**You Be The Judge 17.1**

**UEIJ et LICRA v Yahoo! Inc et Yahoo! France**

1. In discussing this question, students should have recognized that the issue to be addressed is whether the French Court was correct in finding that it had jurisdiction. Students should apply the three jurisdictional tests introduced in the text: (i) real and substantial connection, (ii) passive versus active, and (iii) effects-based. Given the evolving case law in this area, the best in-class approach is to assume that no single approach rules the day. Students should therefore justify their positions through the application of all of the tests.

Under the real and substantial connection test, it is likely demonstrable that the plaintiff’s cause of action, and the effects of Yahoo!, are sufficiently linked to France based on the fact that its French users were able to access prohibited materials on Yahoo!’s main site. However, it is also plausible for Yahoo! to argue that the US and French Yahoo! sites are distinct entities and, as such, any sale of prohibited materials to citizens of France was strictly beyond the scope of the Yahoo!France terms of service. Nevertheless, the mere availability of the prohibited materials may be sufficient to establish French jurisdiction under this test.

Under the passive versus active test, the interactivity resulting from the availability of prohibited materials, and the commercial nature of the offering, help to establish the active nature of the US-based Yahoo! web site and, consequently, justifies French jurisdiction over the case at hand. Alternatively, Yahoo! may argue that the US-based web site at issue is merely passive, so much so that Yahoo!France users have to take their own initiative in order to locate and access the racist materials on its US-based web site. On this argument, the French court will not be said to have jurisdiction.

Both Yahoo! and Yahoo!France will have a much more difficult time defending themselves under the effects-based approach. Because the actual impact of the Yahoo! sale of prohibited materials was experienced in France, French courts would be justified in assuming jurisdiction. However, the plaintiffs seeking French jurisdiction would have the burden of evidencing that the availability of the prohibited materials has actually impacted citizens of France.

2. The global ramifications of the French court’s decision can be separated into two distinct issues:

*Foreign jurisdiction* Businesses must protect themselves against the possibility that their online business practices may result in legal action in jurisdictions other than those specifically contemplated. The consequences of a broad application of several of the jurisdictional tests could frustrate a business’ ability to shield itself from foreign liability.
Targeting technologies

The French court’s ruling requiring Yahoo! to employ targeting technologies in order to prevent access to the Nazi auctions being hosted on Yahoo!’s US-based site presents a serious financial burden on both Yahoo!, and other companies, who must restrict access to customers residing in jurisdictions where those companies are not prepared to assume liability. When can businesses be expected to use targeting technologies? There has been no clear pronouncement on this subject by North American courts. Given the novelty of such technologies, their cost, and the fact that they have not been perfected, it is unclear when they should be implemented. For example, should a business be expected to implement targeting technologies, regardless of the cost, provided that they have a certain level of effectiveness? Alternatively, should a cost-benefit analysis be used, similar to that of tort law?

3. One strategy is to employ targeting technologies to prevent non-local users from accessing and participating in the online discussion. A more cost-effective approach may be to require all users to identify their respective geographic locations and route users through the website accordingly. For example, foreign users may be required to agree to a different terms of use than local residents. Such a webwrap or clickwrap agreement could include an indemnity should the company be found liable in the users’ home jurisdiction. It may also include a provision that foreign users refrain from using the website entirely.

Business Decision 17.1
Respecting Consumer Protection

1. Students may argue that because the guidelines are not required by law, the senior managers should do what is best for business. If research has proven that the corporate advantages of ignoring the guidelines outweigh the benefits of adoption, then that is what should be done until the law demands otherwise. Other students will be tempted to self-serving thinking. Those who are might say that part of being a good risk manager requires ensuring the continuance of your own employment with the company. On this basis, they will support the proposed policy for no reason other than the fact that it has been dictated by senior management. These students should be reminded that effective managers will sometimes buck against the saddle when there is good reason to do so. Students who adopt this position will choose to take the high moral ground and refuse to support the proposed corporate policy on the basis that it does not have due respect for the importance of consumer protection in the online marketplace.

2. Students should note that the adoption of the Industry Canada guidelines might result in greater corporate advantages, such as enhanced business reputation, greater consumer confidence and increased sales. As well, students may have the insight that further investigation is required into the issue of consumer protection to ensure that the company is up-to-date with consumer protection requirements and, thus, protected from potential liability. Such an investigation may conclude that the guidelines should be adopted. Furthermore, the adoption of the suggested guidelines in advance of their possible legal enactment helps to offset associated costs by spreading them over a longer time period.
REVIEW QUESTIONS

1. There are several sources of legal uncertainty in the electronic commerce marketplace. One such source is the fact that contract law was founded on the paradigm of face-to-face interaction and the traditional medium of paper-based exchanges. An application of these standards is often difficult in the electronic milieu. When an application of traditional rules to a new technology is required, sometimes there is no applicable law. Perhaps the greatest challenge, however, stems from the fact that global e-commerce is multi-jurisdictional. The absence of consistent laws across jurisdictions ultimately frustrates certainty in electronic commerce transactions where the parties do not possess the resources to acquaint themselves with the relevant governing laws in each and every jurisdiction.

2. Four potential benefits that electronic commerce offers to businesses willing to implement the use of information technologies are:

   Easier transactions  Businesses can use information technologies to make transactions easier. This is accomplished through the use of help functions embedded in web pages and other informational offerings. Electronic communications such as email facilitate interaction between a business and its customers.

   More affordable transactions  Streamlining and automation of transactions significantly reduces business costs once initial implementation investments have been recouped.

   Reach larger – international audiences  Internet technologies allow for businesses to communicate with potential customers across the globe without the expense of long-distance communication charges.

   Reduce expenses  Besides the obvious savings in implementing cost-efficient technologies, businesses can reduce expenses associated with marketing products both locally and internationally, as they will not require satellite offices and their associated costs. Furthermore, electronic contracting helps to dispense with unnecessary costs stemming from the need for human intermediaries in the contracting process.

3. The purpose of Canada’s Uniform Electronic Commerce Act is to facilitate uniform legislation with respect to electronic commerce in order to remove barriers resulting from rapid technological innovation in the marketplace. In seeking to do so, its role is to provide a model for the creation of a consistent set of laws across the provinces. This is necessary because our constitutional structure allows each province to govern commerce within its jurisdiction. Though each province is free to accept or reject the model law, the drafting of a model law serves to provide an easily adoptable, and adaptable, general framework for provincial legislation.

4. Canada’s Uniform Electronic Commerce Act is not enforceable in each of its provinces and territories. This is because the Act is simply a model and has no legal force in and of itself. The provisions contained within this model law are only enforceable to
the extent that they are adopted and implemented by a particular province or territory. Once enacted, the legislation has the same force or effect as any other provincial legislation.

5. The relevant rules with regard to sending and receiving electronic documents are governed by Canada’s *Uniform Electronic Commerce Act*, as adopted by each respective province and territory. Messages are deemed to be sent and received at each party’s respective place of business. A message is deemed to be sent when it leaves the sender’s control. A message is deemed to have been received when it reaches an information system in the control of the party to whom it was sent. This is true even if the message is never actually opened or read, provided that technological difficulties did not prevent the message from being downloaded to the recipient’s information system. Messages communicating contractual acceptance remain under common law jurisdiction.

Prudent risk managers can seek to avoid disputes related to the sending and receiving of electronic documents through the requirement of transmission acknowledgements or, alternatively, by way of the implementation of automated message confirmation systems. Sometimes, it is a good idea to use multiple channels of delivery.

6. When engaging in interprovincial commerce, business managers should be mindful of the fact that the legislation governing such activity varies from province to province. While many of the provinces have adopted Canada’s *Uniform Electronic Commerce Act* entirely, or with only minor variations, there are some differences in the manner in which certain provinces have sought to address these issues. Thus, the relevant legislation in every province in which the company intends to do business must be examined in order to ensure that differences in the law are attended to and built into the transactions.

7. The major difficulty associated with the formation of contracts online is ensuring that both parties understand and consent to their terms and conditions. When a business chooses to employ a clickwrap or webwrap contract, it must take steps to make certain that customers will be bound to the terms set forth. As illustrated in the case of *Rudder v Microsoft*, the online contract must take steps to draw their customers’ attention to particularly onerous clauses or clauses that could potentially be considered “fine print.” Businesses should repeat the key terms in the clickwrap, indicating that the customer is accepting those terms (whether or not they have actually been read). As well, the method of conveying acceptance of the offer must also be clearly understood as such.

8. The advantage of ensuring that advertised information about products or services are considered an invitation to treat is that customer orders are received as offers, which the business is then free to accept or reject as desired. This gives a business the last word on whether a binding agreement will be generated and allows the business to control the transaction, which is useful in such as cases where products or services may be in low supply. A web designer can try to ensure that the placing of an order is merely the making of an offer by including language that makes it clear that the business is not bound to fill orders, but can accept or reject them at its discretion. By clearly specifying
Chapter 17 – Electronic Commerce

that an order is of the nature of an invitation to treat, and that it is not binding, the web designer will afford the business leeway to better control the transaction.

9. Automated electronic commerce makes it more difficult to identify the existence of a meeting of the minds (consensus ad idem). The absence of human interaction presents challenges when seeking to apply the traditional notions of contract. Furthermore, fully automated transaction systems are vulnerable to keystroke errors, which occur when a person mistakenly hits a wrong button or key while conducting a transaction. This is due to the inability to correct the mistake with a subsequent communication because of the fact that the system is automated and therefore cannot recognize or process such additional communications. Most electronic commerce statutes contain provisions that allow well-intentioned consumers to escape liability resulting from a keystroke error by rendering the contract unenforceable. Businesses conducting electronic commerce can avoid the consequences of keystroke errors by incorporating error prevention/correction mechanisms into their ordering process. The simplest and most effective strategy is to require the purchaser to confirm the details of the order, or else confirm important information such as the number of items ordered by physically re-entering it into the information system.

10. PKI stands for Public Key Infrastructure and is used to refer to a set of policies and procedures crafted to provide a high level of security for parties exchanging information online. Security is obtained through the technology of encryption and through the employment of a trusted third party. Encryption makes it prohibitive for others to be able to read or understand private communications between parties. A trusted third party plays a role by authenticating the identity (or other attributes such as a person’s level of security clearance, age or whether that person holds a particular license, etc) of persons by way of the issuance of a unique digital certificate. In this way, a trusted third party can facilitate trust among otherwise unidentifiable persons. Such a service is crucial to electronic commerce, given the need to know that businesses are interacting with, and offering goods and services to, appropriate parties. Through the use of digital certificates, vendors and purchasers can be assured that they are not entering into fraudulent transactions that may result in financial loss.

11. Cryptography is the encryption and decryption of information to protect against inadvertent disclosure to unauthorized parties. Encryption is the coding of plaintext into an unreadable form called ciphertext that cannot be understood by those who do not have the relevant code. Decryption is the process of converting ciphertext back into its original form so that it can be understood. Historically, this has been accomplished through the use of a private key, which is used to both encrypt and decrypt the information. Should that private key ever be disclosed to unauthorized parties, however, they will not only be able to read the encrypted information, but they will also be able to send encrypted messages which will be presumed to have come from an authorized person.

In order to protect against this, public key cryptography is preferable. In public key cryptography, two keys are created, one is public, and the other is private (one to encrypt; the other to decrypt). Your public key is made freely available for the encryption of
messages being sent to you. You can then decrypt them with your private key. By avoiding the possibility of your private key falling into unauthorized hands, the integrity of your messages is maintained. This method has gained popularity with internet users due to its ease of use and effectiveness. Sending a private key to someone over the internet is a dangerous and ill-advised practice. Public key cryptography makes this risk unnecessary.

12. In seeking to enhance information security within the workplace, businesses can use the law as a deterrent in two ways:
   - Informing users of workplace information systems that they will be disciplined or even dismissed if they engage in illegal activities. Publication of relevant laws such as those contained within the Criminal Code of Canada also help to encourage compliance.
   - Contract law can be utilized in the form of confidentiality agreements and internet use policies which can be enforced against employees, as necessary. Contracts can also be employed to allow for the monitoring of employee communications in order to facilitate compliance.

13. Communication security refers to the technological protection of information while it is being transmitted from one information system to another. An example of communication security is protection against the interception of transmissions through the use of cryptographic technologies. Computer security is the protection of information within a computer system. An example of computer security is the use of firewalls to protect against unauthorized entry and possible contamination of a computer system.

14. Cybersquatting is the practice of purchasing a potentially valuable domain name with the intention of later selling it to the highest bidder. Though associated with the practice of the registration of domain names in which the squatter has no commercial rights, the act of cybersquatting is not always a reprehensible behaviour. For example, some cybersquatters purchase generic words that cannot be registered as trade-marks. If no one claims a prior right to a particular domain name, the first person to register it becomes the owner and thereby has the right to resell it to an interested purchaser.

15. Three typical disputes arising from the domain name registration system are:
   - A person may innocently, or with some justification, register a domain name that is later disputed. For example, the registration of a person’s family name may conflict with a business operating under the same name.
   - A person may register a domain name that resembles a trademark to which both parties claim a commercial right. For example, registered trademarks from different jurisdictions may conflict. This would be the case where both a US and Canadian business held a valid registration in the mark “Super Glue”, and the corresponding domain name was purchased by one of the parties.
   - A person may register a domain name in which it has no commercial rights. For example, a cybersquatter may register the domain name www.superglue.ca in order to hold it for ransom from the Super Glue Company of Ottawa, Ontario.
Prudent business managers can avoid domain name disputes by being proactive in their registration of the company’s *bona fide* trademarks and business names. An ounce of prevention is worth a pound of cure when seeking to avoid costly and drawn-out disputes. Managers should also try to determine whether registering the domain name will likely result in a complaint from someone who is a bona fide owner of a similar mark in another jurisdiction. Again, it is useful in such situations to be proactive. It is better to strike a deal at the outset than to become embroiled in a legal battle down the road.

16. When deciding whether to participate in electronic commerce on a global level, prudent business managers are advised to consider the possibility of litigation stemming from the alleged contravention of foreign law. In doing so, they must investigate the compliance issues and types of liability that may result from their particular online business practices. These risks can be managed by paying particular attention to the tests which are used to determine whether or not such practices will likely fall under a foreign jurisdiction, and crafting their business practices accordingly. Moreover, businesses should avoid targeting particular jurisdictions through the employment of forum-selection clauses in its standard form contracts, and the use of technologies that restrict the geographic area in which it is possible to interact with the business’ web site.

17. There are three different tests that a court may apply when considering the matter of whether or not a particular online interaction falls under its jurisdiction.

- **Real and substantial connection test** This test is used by Canadian courts to date. When applying it, the court will ask whether plaintiff’s cause of action and the effects of the defendant’s conduct are *sufficiently linked* to the place in which the plaintiff has brought an action.

- **Passive versus active test** Under this test, courts will examine the online interaction in order to determine: (i) the *level of interactivity* between the parties, and (ii) the *commercial nature* of the exchange of information that occurs on the web site. The more interactive and commercial-oriented a web site is with respect to a particular country, the more likely that a court in that country has jurisdiction to hear a case concerning it.

- **Effects-based test** A more recently applied, and more open-ended, test which focuses on the *actual impact* that a web site has in the place where jurisdiction is being sought. The court will look at *where* the alleged harm is done, rather than *how* it was allegedly done.

18. The two main types of online intermediaries are:

- **Online access provider** A person or business that provides others with access to the Internet. A good example would be Bell Sympatico, which provides both dial-up and high-speed internet access for a fixed monthly fee. Most communication and cable companies are also providers of internet access.

- **Online service provider** A person or business that offers goods and services in exchange for something of value. Such goods and services extend beyond mere internet access and typically fall under the heading of electronic commerce. Appropriate examples would be email suppliers, bulletin board operators, auction
hosts, anonymous remailers, and commercial web sites. A specific example is Chapters.ca, a well-known online retailer of books and videos.

Online access providers are generally immune from liability on the basis that they neither monitor nor control information passing through their networks. Moreover, potential liabilities can be safeguarded against through exclusion and indemnity clauses in their standard form agreements with their users. An online service provider is much more likely to attract potential liability as an intermediary. This is due to the fact that although an online service provider may seek to protect itself through a liability exclusion clause in its standard form agreement with its users, it cannot protect against potential liability to a third party.

19. An online service provider may protect itself against liability as an online intermediary by taking steps to ensure that it is not seen as a publisher of information disseminated through its system. One way to achieve this is to refrain from exercising editorial control over the content carried by the system. By structuring its business arrangements so that it is seen to act as a mere distributor, it is in a better position to argue that it is not liable. The online service provider should further protect itself through the use of a standard form agreement. Such an agreement can be implemented through a clickwrap or webwrap format. In either case, users of the service should be required to manifest informed consent to a terms-of-service agreement containing both an exclusion and indemnification provision. The use of examples in the agreement is encouraged for the purposes of ensuring understanding and thus achieving the requisite consensus ad idem. Should the Newfoundland company be sued, it would be well-advised to put forth a policy argument that legislation in other jurisdictions, such as Quebec’s Act to Establish a Legal Framework for Information Technology, should be adopted in order to shield it from liability.

20. Prudent businesses may seek to incorporate consumer protection principles into their online contracting practices by adopting and implementing Industry Canada’s guidelines, titled, Principles of Consumer Protection in Electronic Commerce. This can be achieved in the following manner:

- Make use of plain language whenever possible.
- Disclose all relevant details with respect to both product and service offerings.
- Provide consumers with a record of their transactions.
- Implement a complaints procedure.
- Ensure that their customers’ contractual agreements are fully informed and intentional.
- Respect and protect customers’ privacy through appropriate data collection and storage.
- Conduct payment and personal information transactions through secure servers and networks.
- Handle customer complaints efficiently and effectively.
- Do not charge for unauthorized transactions. Provide refunds where fraud is alleged and the goods or services have already been delivered. Allow for order
cancellations within a reasonable time period where there has been a mistake or inadequate information was provided.

- Avoid the transmission of commercial email without the consent of consumers, unless there is a pre-existing relationship where consent may be implied.
- Engage in consumer education initiatives with respect to the risks associated with electronic commerce and how they can be minimized or avoided.

**CASES AND PROBLEMS**

1. The *Uniform Electronic Commerce Act* is not law – it does not create rights, powers, obligations or immunities. Commerce, whether electronic or otherwise, is exclusively governed by provincial legislation, in this case, Saskatchewan’s *Electronic Information and Document Act*. With respect to the ability to file electronically, subsection 28(1) clearly states that a person may file in an electronic format provided that the person filing is a member of a class of persons in possession of the appropriate authorization. This point needs to be further researched in order to confirm that such pre-authorization exists. Without pre-authorization, the Saskatchewan company must apply for permission to file electronically. Furthermore, in order to be accepted by the Saskatchewan government the document must be (i) of a class of documents which may be filed electronically, (ii) in the prescribed format, and (iii) recorded on a system of electronic data storage that is machine-readable. Further details are available in the accompanying regulations to the Act. As a manager required to decide whether to expend funds on new corporate software, a further investigation needs to be carried out in order to ascertain whether and how the company can comply with aforementioned requirements when creating their electronic format. The available cost-savings hinge on the cost of compliance and, as such, the decision of whether to switch to an electronic format cannot be made at this time. However, the opportunity to comply does exist.

The second issue to address is whether the Saskatchewan government can force a business to file solely by electronic means. In examining section 28 of the Act, it would seem that there is no provision giving the Saskatchewan government the power to force a business or person to file documents only in electronic format. Moreover, there is no mention that should a party choose to file electronically, it will be implied that they must continue to do so. Such provisions would go against the spirit of e-commerce legislation, which aims to make transactions technology neutral. Forcing a company to file electronically places digital technologies above others. [based on the *Uniform Electronic Commerce Act; Electronic Information and Document Act*, SS 2000, c. E-7.22]

2. There are four ways in which an appropriate web design can protect against erroneous customer orders.

- *Prevent keystroke errors* Given that the web site will automatically process customer orders, it is important to prevent the processing of orders containing keystroke errors. Since most relevant provincial statutes state that transactions are unenforceable when purchasers contracting with an automated payment system make a keystroke error, the onus is on the vendor to prevent them. This is accomplished by proving that the automated system provided an opportunity to prevent or correct the error, allowed for communication of a correction, and
allowed for customer returns provided that they have not received material benefit from the product or service ordered. The easiest way to meet these requirements is to require the purchaser to confirm their order by repeating the critical ordering steps or otherwise requiring confirmation of the order prior to processing. Likely, a simple order confirmation screen and the clicking of a “Confirm” button will be sufficient.

- **Successful contract formation** The website should be designed so that customers must assent to a terms of service agreement which includes a provision for the exclusion of liability and the indemnification of the company in the case of erroneous customer orders. These terms of service must be clearly brought to the customer’s attention. This is best accomplished through the use of a clickwrap or webwrap contract when the customer first enters the website. In either event, the terms and conditions should be plain language and conspicuously placed on the site.

- **Invitation to treat** Another method to ensure against the acceptance of erroneous customer orders is to design the website so that it extends an invitation to treat, as opposed to an offer. In this way, the company is merely demonstrating a willingness to receive offers from customers and is not bound to its customers’ orders. This makes it possible for the review and confirmation of customer orders where errors are suspected. This can be done through human review of all orders. If an automated system is being used, orders that surpass a certain threshold (e.g., monetary or quantity of items ordered) can be automatically diverted for human review.

- **Authentication** The company can require the customers to provide digital identification, such as electronic signatures, in order to prevent against fraudulent orders.

   [based on *Uniform Electronic Commerce Act*, ss 5, 7-9]

3. The *Uniform Electronic Commerce Act* allows for the use of electronic functional equivalents where, historically, paper-based mediums were employed. Depending on the relevant provincial legislation, BadNews.ca would be free to substitute electronic mail messages for paper legal notices of repossession. According to the *UECA*, a message is deemed to be sent from the sender’s place of business and received at the recipient’s place of business. Because the main concern is the receipt of an electronic message, explanations concerning the sending of such messages will not be discussed in this memo. A message is deemed received when it reaches an information system in the control of the person to whom it is sent. Thus, once a person decides to make use of an electronic mail system, the onus is on them to check their messages frequently. However, the recipient may rebut the presumption of receipt by evidencing that they were unable to access their electronic mail system during the dates in dispute. Prudent business practice would therefore require the sending party to either require acknowledgement of receipt, or to implement a system capable of automatic confirmation of receipt. Simple reliance on presumed receipt is ill-advised. A further means of avoiding disputes about notice is to find a back-up method of ensuring receipt. Although this is time consuming, a back-up method can help avoid costly litigation where debtors claim not to have received notice.
4. The central legal issue in this case is whether Scroll can rely on its price variation clause and its statement that “acceptance of the order is expressly conditioned on the buyer’s assent.” Whether these clauses will be incorporated into the clickwrap depends on whether sufficient notice was given. In the actual case upon which this case was based, *Corinthian Pharmaceutical Systems Inc v Lederle Laboratories Inc* 724 F Supp 605 (SD Ind 1989), Scroll would not be required to fill the remainder of the order as the terms and conditions were held to govern the transaction. Moreover, Scroll’s delivery of 50 XV11 routers at the initial market price does not require them to fill the remainder of the order at that price but, rather, was seen simply as an friendly accommodation of no subsequent effect. Would the preceding analysis, based on US precedent, likely be followed in Canada? The likely answer is yes. This is due to the fact that simple contract law varies very little between these neighbouring jurisdictions. The terms and conditions were clearly laid out and easily understood. However, this conclusion is premised on the fact that they were indeed adequately brought to ICanSolve’s attention within the format of the clickwrap contract.

Scroll can avoid similar future situations by designing its web site so that its online product listings are even more clearly intended as mere invitations to treat rather than offers which may be accepted without further interaction. Customer orders should not be automatically processed by automated systems but instead should be reviewed at some point prior to acceptance and shipping. [based on *Corinthian Pharmaceutical Systems Inc v Lederle Laboratories Inc* 724 F Supp 605 (SD Ind 1989) – which is discussed below in Case Briefs]

5. The reality of identity spoofing is not to be taken lightly. Fraudulent transactions such as these can be a direct threat to a business’ profit margins. Some hackers, and others with technological savvy, are able to forge encryption keys, thereby preventing the ability of one party to correctly identify the other party to a transaction. Fortunately, such practices can be thwarted through the employment of a certification authority.

A certification authority (CA) is a trusted company in the business of validating the identity of the parties to a transaction (the CA is a third party to the transaction and therefore has no interest in the particulars of the deal). The validation process is accomplished through the issuance of digital certificates to parties using its services. The digital certificate contains an electronic signature encrypted by the party holding its private key. By decrypting the signature with the corresponding public key, recipients can be sure that the attached message or document was sent by the particular signing party – so long as the key pairs can be authenticated by the certificate authority. In this respect, a certification authority is commonly referred to as a trusted third party. Given that our company transacts with individuals from around the world whose identities and credit ratings are unknown, it is important to take proactive steps to make sure that our online transactions can be validated in much the same way that traditional face-to-face interactions are. Certificate authorities make this possible on a practicable cost basis.
6. Overall, the Employee Terms of Service agreement is well-drafted. It does a good job of setting out most of the relevant issues and prohibiting behaviours that may attract liability. Moreover, the provision that the employer may monitor the employee’s activities and discipline those parties in contravention of the agreement serves as an effective deterrent. However, it is deficient in some areas and overly severe in others, as follows. (Students are unlikely to glean all of these points from the Chapter; some of them stem from first principles in contract and employment law as discussed in other Chapters.)

- **Intermediary liability** The issue of intermediary liability is appropriately dealt with by directing the employees to refrain from activities that may attract liability for the employer. However, since the computer network and connected devices are the property of the employer, the potential for liability remains. Consequently, it would be a good idea to include a provision detailing that the employee agrees to indemnify the employer should liability indeed result as a consequence of the employee breaching the terms of use.

- **Personal information** The employer should refrain from the disclosure of personal information without notice and upon simple request. Although the employer is justified in disclosing information when required to do so in order to comply with court orders and other legal obligations, the employee should be given notice that this has been done. Any non-law enforcement requests should not be fulfilled until the employee has received notice and an appropriate time period in which to dispute the request. The protection of employees’ personal information is a statutory duty [some students will recall this from Ethical Perspective 17.1] and should not be taken lightly at risk of attracting employer liability.

- **Discipline** The disciplinary steps for contravention of the agreement should be clearly laid out. Not only does this protect the employer from later actions for constructive dismissal and the like, it also serves as a meaningful deterrent to employees.

- **Contract formation** Regardless of how well the agreement is drafted, it is of no effect if a meeting of the minds (consensus ad idem) cannot be established. Therefore, the agreement should be included as part of the initial employment contract offered to prospective employees prior to their commencement of work. The agreement should be brought to the employees’ attention and clear signification of the employee’s consent should be obtained. This is especially important if use of the workplace computer network is an essential part of the employee’s work duties.

7. Given the possibility that there are others like Marcus within the ranks of the company, it is of the utmost importance to have an adequate information security plan in place. The prevention of further mishaps is best accomplished through the use of law as a deterrent. For starters, the corporate policy should publish the relevant sections of the Criminal Code of Canada – namely, sections 342.1, 430(1.1), 183 and 184. Furthermore, Scroll Networks should implement a contractual agreement aimed at protecting both information contained within a computer system, as well as the system itself. Such an
agreement would outline prohibited behaviours and set out the respective penalties. The agreement should also require employees to indemnify the company for damages resulting from their contravention of the agreements terms. An external security provider or consultant may be warranted, if cost-effective. As well, an information security oriented insurer may be contracted to offset potential monetary losses.

With respect to Marcus, Scroll should commence a proper investigation to see whether there is sufficient evidence to press charges. If so, Scroll Networks can pursue a criminal charge under section 430(1) of the Criminal Code (computer mischief resulting in the destruction, alteration, and obstruction of the data contained within the scorched computer network). By gathering sufficient proof, there will also be grounds for dismissing Marcus. Not only would such a course of action provide a meaningful deterrent to other employees, it would remove Marcus (and any influence that he might have over other employees) from harm’s way. [Employment law; Contract law; and Section 430(1) Criminal Code if Canada]

8. We may expect the arguments to be as follows:
   - **XACTO’s argument** Koko’s registration of the domain name xacto.ca is (i) confusingly similar to the Canadian trademark XACTO currently registered to the XACTO Standard Weights and Measurements Corp.; (ii) Koko has no legitimate interests in the domain name; and (iii) the domain name has been registered in bad faith. Evidence of bad faith can be discerned from Koko’s email. Clearly, she has acquired the domain name for the purposes of selling, renting, licensing or otherwise transferring the registration to the XACTO Corp. for valuable consideration in excess of its actual costs.
   - **Koko’s argument** Koko will claim that she has a legitimate interest in the domain name in dispute as it is understood to be a generic name in Canada. She may also argue that she planned to use the domain in association with a non-commercial activity such as criticism, review and/or news reporting. Lastly, she may argue that the domain name is a reference, or nickname, by which she is commonly identified.

We may expect that Koko will be unable to provide adequate evidence to support any of her arguments on a balance of probabilities. Thus, the likely resolution of the matter will be the cancellation of Koko’s registration in the domain name at issue and an order to transfer it to the XACTO Corp. [based on iTravel2000.com Inc v Fagan [2001] OJ No 943 (Ont Sup Ct) – which is discussed below in Case Briefs]

9. This question is best divided into the following three issues. (If your students have not covered the topics of economic loss and trademarks, they are likely to limit their responses to the jurisdictional issues.)

   **Jurisdiction** The first issue to be resolved is whether a Manitoba court can assert jurisdiction over the US-based software company. Based on the real and substantial connection test (as adopted in Alteen v Informix Corp (1998) 164 Nfld & PEIR 301 (Nfld SC TD)) it is likely that jurisdiction will be asserted. This conclusion is premised on the
extremely low connection threshold required under this case, *ie*, the mere posting of information accessible to Canadian citizens. This case is binding in Canada.

Alternatively, dFOX may argue for the application of the *effects-based approach* currently being advocated by academics and courts. Under this approach, the actual impact of Code Works’ behaviour on the Canadian plaintiff will be examined. dFOX will be required to evidence the harm alleged. Given Code Work’s awareness of the damage being caused to dFOX by the marketing of its voicemailbot, it is also likely that grounds for the assertion of jurisdiction will be found under this test.

Code Works, however, may counter the argument on appeal by contending that the correct test to be applied is the *passive versus active test* as adopted in both *Zippe Manufacturing Co v Zippo Dot Com Inc* 952 F Supp 1119 (WD Pa 1997) and *Braintech Inc v Kostiuk* (1999) 171 DLR (4th) 46 (Ont CA). Under this test, the appropriate determination is to examine the level of interactivity between the parties and the commercial nature of the exchange of information that occurs on the web site. Code Works can be expected to argue that their web site specifically targets Americans through its US 1-888 telephone number, not to mention the fact that it disowns compliance with foreign hardware and excludes all warranties for foreign customers. Nevertheless, because the web site still allows for online foreign-based orders, these elements merely amount to a disincentive rather than a prohibition. Thus, it is possible, if not likely, that jurisdiction may be found under each of the three preceding tests.

Code Works would have been well-served to avoid targeting foreign jurisdictions. This could have been accomplished through the employment of a jurisdictional clause in its standard form contract, requiring that disputes be heard in a specific jurisdiction. Additionally, targeting technologies may be used to restrict the geographic area in which business is conducted. However, because the dispute at hand does not result from a transaction between Code Works and a Canadian-based customer, such targeting approaches would have been ineffectual. Instead, Code Works could prevent similar legal liabilities in foreign jurisdictions by responding promptly and appropriately to such complaints, thereby mitigating potential legal liability.

*Economic loss* Should jurisdiction be found, based on *Pro-C Ltd v Computer City Inc* [2000] OJ No 2823 (Ont Sup Ct), Code Works will likely be held responsible for the economic loss resulting from the damage caused by their customers’ attempts to access the dFOX web site. In that case, the defendant similarly made use of the plaintiff’s registered trade-mark and refused to desist when notified of the negative effect it was having on the plaintiff’s business (namely, server overload, communication interruption and irreparable hardware damage). In the case upon which this question was based, the plaintiff was awarded both general and punitive damages for the economic loss stemming from the defendant’s wilful continuance in their business practices despite awareness of their harmful impact. However, both awards were based on a finding of trade-mark infringement.
Trade-mark infringement  Again, based on Pro-C Ltd v Computer City Inc [2000] OJ No 2823 (Ont Sup Ct), Code Works will likely be held responsible for trade-mark infringement. Code Works was demonstrably aware of the Canadian registered trade-mark “dFOX,” yet continued marketing to Canadian citizens nonetheless. Code Works holds no competing mark in either Canada or the US. This conclusion is, however, premised on the finding of jurisdiction. [based on Pro-C Ltd v Computer City Inc [2000] OJ No 2823 (Ont Sup Ct) – which discussed below in Case Briefs]

10. Based on the US case of Stratton Oakmont v Prodigy 1995 WL 323710 (NY Sup Ct 1995), it is certainly possible that the company may succeed against us in their defamation action. Similar to the facts at hand, Prodigy, an online intermediary, deliberately chose to exercise editorial control over its content. Unfortunately, this means that the benefits of maintaining community standards and keeping the peace online are offset against a corresponding increase in the potential for liability. The more active role an intermediary plays (as opposed to being a passive conduit), the greater the liability it attracts by virtue of the possibility that it will be understood to operate as a publisher. There are two possible arguments that we might attempt in order to avoid liability in spite of our actions. First, we might try to characterize ourselves as a distributor in spite of the facts. To an extent, this is what was accomplished in the case of Cubby Inc v CompuServe Inc 776 F Supp 135 (SDNY 1991). Should we succeed with this argument, we would only be held liable if there was actual knowledge of the defamatory content. Since we did not actually know about it, we would stand a decent chance of defending ourselves against liability. Another approach would be to try to defeat the policy underlying intermediary liability. A policy that removes all incentive for improving online community standards, we would argue, is a bad policy. Where a service provider gets involved with the bona fide objective of improving the community, it should not be held liable just because some remarks went unnoticed. To invoke such a policy is to risk a very slippery slope.

Liability to third parties is a serious business risk—one that must be dealt with strategically and appropriately. This case raises an opportunity to restructure our business practices. We would be better off avoiding the exercise of any control over the postings on our bulletin board unless instructed otherwise by law, at least until the law provides some sort of safe harbour. We might even consider technological measures that would prevent the removal of customer postings. Until such time as the law provides a defence for service providers who remove content in good faith, we must do our best to ensure that we will not be seen as a publisher. [based on Pro-C Ltd v Computer City Inc [2000] OJ No 2823 (Ont Sup Ct)]

11. Although it would be comforting to think that all friends from days gone by can be trusted, history has repeatedly proven otherwise. With this in mind, it is quite plausible that your old high-school friend is the perpetrator of a dot con. The distribution scheme at hand sounds suspiciously similar to the multi-level marketing system traditionally used to defraud consumers in the offline world. Under this approach, greater emphasis is put upon the recruitment of distributors than on the selling of an actual product. Newly recruited distributors pay an initiation fee to their recruiter for the product samples and
promotional materials. They also pay a percentage of their overall sales up the ladder. Thereby, high-ranked founding members can receive large amounts of monies for doing little work other than the initial recruitment of the layer under them. For this reason, such a business formula is commonly referred to as a pyramid scheme. Given the likelihood of duplicity surrounding your friend’s claim and his enthusiasm for you becoming a recruiter below him, you are best to politely decline. [based on Stratton Oakmont v Prodigy 1995 WL 323710 (NY Sup Ct 1995)]

12. It is possible that the adoption of such a principle would not always provide more protection to consumers; nevertheless, its adoption could not hurt. For one thing, its adoption might spur the use of more sophisticated and successful means of advertising. Still, Canadian corporations are not required to adopt the principle, as it is merely a suggestion propagated by Industry Canada and aimed at supplementing existing consumer protection laws. Such guidelines are based on extensive research and drafted with an eye towards benefitting both consumers and businesses. Existing laws, however, could be amended and the likelihood of future law reform is yet another reason to adopt such a principle. Companies should also consider the cost ramifications of retrofitting such policies should they become law. Moreover, by showcasing the adoption of this and other consumer protection principles, businesses can enhance their reputation, strengthen consumer confidence, and thereby increase overall sales. Conversely, ignoring the Industry Canada guidelines will likely result in the loss of consumer trust, and thus reduced business, especially where competitors choose to leverage showcasing opportunities such as these.

Email Business Practice Policy Statement [Example]:
The Kerasic Group undertakes to protect its customers against unwanted disclosure of their personal information, including their email address. The Kerasic Group, however, maintains affiliations with parties in order to transmit commercial email messages to Kerasic customers. Such messages are provided on an opt-in basis. No other personal information besides your email address is provided to third parties unless you specifically agree to their provision. You will not receive commercial messages from or through Kerasic unless you have consented to do so at the time of your first purchase. Once you have consented to their receipt, you will continue to receive similar messages from time to time until you elect otherwise. Electing otherwise can be accomplished by filling out, and submitting, the “opt-out” form available through the Kerasic web site. Any further questions can be directed towards Kerasic customer service. [based on Principles of Consumer Protection in Electronic Commerce: A Canadian Framework (1999)]

CASE BRIEFS
Rudder v Microsoft (1999) 47 CCLT (2d) 168 (Ont Sup Ct) – note 12
The basic facts are provided in Case Brief 17.1.

Mafiaboy online QL (National General News, September 12, 2001) – note 19
The basic facts are provided in Case Brief 17.2.
This case explores the issue of whether a domain name including the suffix “suck” is confusingly similar to the domain name upon which the word “sucks” has been appended. Additionally, the issue of whether a criticism or parody privilege extends to the use of the suffix “sucks” is considered. The complainant, Wal-Mart Stores, Inc. is the registered owner of the trademark Wal-Mart, which is used in conjunction with retail store services. The respondent is Kenneth J Harvey, a resident of Newfoundland.

The complainant alleged that the domain name in question was registered in bad faith, ie, it was registered with the intent of offering it for sale to the complainant at a price far exceeding its cost. Such behaviour is commonly referred to as cybersquatting. The respondent claims that the domain name in dispute was used for the legitimate purpose of operating a freedom of expression web site, aimed at protesting the business practices of the complainant. The respondent has been found to have cybersquatted several other domain names with respect to Wal-Mart in the past. In the case at hand, however, the respondent was not found to have registered the domain name in bad faith as defined by the ICANN UDRP. The domain name in dispute was not found to be identical or confusingly similar to the trademark in which the complainant holds rights. Furthermore, the respondent was deemed to have a legitimate interest with respect to the domain name, wallmartcanadasucks.com. A violation of the ICANN policy was not found. The respondent was allowed to continue operating the domain name.

This case was referred to as authority for the proposition that courts will sometimes adopt a “real and substantial connection test” for jurisdiction. On the facts, the plaintiff was a child injured in a motor vehicle accident. The child was a resident of British Columbia, but the accident occurred in Saskatchewan while his father was driving. The defendant was a resident of Saskatchewan. The car carrying the plaintiff and the defendant’s car were registered to their respective home provinces. The action was brought in British Columbia. The matter at issue is whether the applicable law is “that of the place where the tort arises”. The British Columbia Court of Appeal found that the law of the forum in which the action is brought should apply. The Supreme Court of Canada allowed the appeal, holding that “the applicable law in cases of actions within Canada in respect of wrongs committed in Canada was the law of the place of the wrong.” In its reasoning, the Court cited the real and substantial connection test.

This case was primarily concerned with the reciprocal enforcement of foreign judgments. Lenders on a mortgage of properties in Alberta obtained judgments against a resident of British Columbia (who was previously an Alberta resident at the time of his mortgage) for foreclosure and deficiencies on sales on Alberta mortgages. The judgments and accompanying court order were obtained in an Alberta court. The respondents then sought to have the Alberta deficiency judgments enforced in a British Columbia court. The judgments were obtained and later upheld on appeal. Upon further appeal, the Supreme Court of Canada held that the appeal should be dismissed. This case stands for
the adoption of a more flexible approach to the recognition of foreign judgments. It is, however, often cited for its holding that the approach of permitting suit where there is a real and substantial connection with the action provides a reasonable balance between the rights of the parties. According to the court, this approach affords some protection against being pursued in jurisdictions having little or no connection with the transaction or the parties.

**Inset Systems Inc v Instruction Set** [937 F Supp 161 (D Conn 1996)]
This case has become famous for its characterization of an internet web site as akin to a continuous advertisement. In this case, the plaintiff, Inset Systems, brought a trade-mark infringement action against the defendant, Instruction Set, for using its trade-mark in their domain name. The plaintiff operated out of the state of Connecticut, while the defendant was based in Massachusetts. The defendant moved to dismiss the action, citing an absence of personal jurisdiction. The district court found that the defendant’s internet advertising was sufficient to establish the requisite minimum contacts with the state of Connecticut. The motion was denied. Accordingly, Connecticut’s *long-arm* statute was applicable and the defendant was deemed to reside in Connecticut for the purposes of the infringement action.

**Alteen v Informix Corp** (1998) 164 Nfld & PEIR 301 (Nfld SC TD)
The basic facts are provided in the Jurisdiction section of the text.

The basic facts are provided in Case Brief 17.3.

**Zippo Manufacturing Co v Zippo Dot Com Inc** [952 F Supp 1119 (WD Pa 1997)]
This case is illustrative of a court decision adopting the active versus passive test for jurisdiction. Zippo Manufacturing, the manufacturer of Zippo brand lighters, brought an action for trade-mark infringement against the defendant, a computer news service operating under the domain names: zippo.com, zippo.net and zipponews.com. The plaintiff does business in the state of Pennsylvania and brought the action there. The defendant argued that it does not maintain offices or agents within Pennsylvania and on that basis sought to file a motion to dismiss or transfer the action to its principal place of business, California. The Pennsylvania District Court held that the defendant had purposefully conducted business in the Pennsylvania by making its services available to residents of the state of Pennsylvania and was, therefore, subject to personal jurisdiction within that state. The basis of the claim was that, unlike the earlier cases where the sites were merely passive in nature, (akin to continuous advertising), the use of the disputed domain names was active in nature. Given that the sites were found to be active within Pennsylvania, the defendant’s motion was denied.

**Braintech Inc v Kostiuk** (1999) 171 DLR (4th) 46 (Ont CA)
This case is a leading case in Canada applying the active versus passive approach adopted in the Zippo case. On the facts, the plaintiff was a technology company incorporated in Nevada, operating in British Columbia, and conducting business in several US states. The
plaintiff commenced an action in Texas against Kostiuk, a British Columbia resident, alleging that the defendant had published defamatory information about the corporation on an Internet bulletin board in 1996. The defendant has no connection with Texas. The plaintiff obtained a default judgment in Texas and attempted to have it enforced in British Columbia under the principle of comity. A judgment for reciprocal enforcement was obtained at summary trial. The defendant appealed. Applying the active versus passive test established in Zippo, the British Columbia Court of Appeal held that there was no connection between the defendant’s actions and the tort alleged to have been committed in Texas. Moreover, comity did not require the recognition of the default judgment obtained in Texas. The appeal was therefore allowed.

**UEJF et LICRA v Yahoo! Inc et Yahoo! France** Tribunal De Grande Instance De Paris (NRG 00/05308, 22 May 2000) – note 32
The basic facts are provided in You Be The Judge 17.1.

**Cubby Inc v CompuServe Inc** 776 F Supp 135 (SDNY 1991) – note 34
The defendant, CompuServe, was a corporation in the business of providing its subscribers with access to its computer network and several forums containing informational resources. It was alleged by the plaintiff that the defendant had published a defamatory statement in one of the electronic newsletters available in their Journalism Forum. A separate entity had been contracted to provide the content contained within the newsletter in question. In this case, the Court found that because CompuServe had no opportunity to review the contents of the newsletter prior to being uploaded to the Journalism Forum, and because CompuServe did not interfere with the publication once it became generally available, it did not exercise the editorial control necessary to attach publisher liability. Rather, CompuServe was a mere distributor. Consequently it was not presumed to know about the defamatory statements and ultimately found not to be liable.

**Stratton Oakmont v Prodigy Services Co** 1995 WL 323710 (NY Sup CT 1995) – note 34
This case also concerned a defamatory remark posted on an online bulletin board system called “Money Talk,” hosted by an online service provider called Prodigy. As did CompuServe in the previous case, Prodigy contracted-out the management of the forum. In this case, board leaders would participate in, and monitor, the discussions taking place on the different bulletin boards. The defamatory statement was not removed by the board leader subsequent to its discovery. At issue was whether Prodigy exercised the degree of editorial control necessary to attach liability. The court found that the board leader was an agent for Prodigy. Moreover, Prodigy had sought to attract customers by advertising its control of content on its board and the resulting absence of offensiveness or “bad taste.” Because Prodigy has deliberately chosen to “gain the benefits of editorial control” it was subject to an increased level of liability for the content it disseminated. On this basis, the court found that Prodigy had acted in the role of a publisher, as opposed to a distributor. Accordingly, the court found Prodigy liable for the defamatory statement.

**Corinthian Pharmaceutical Systems Inc v Lederle Laboratories Inc** 724 F Supp 605 (SD Ind 1989) – this case was the basis for Cases and Problems 4.
Chapter 17 – Electronic Commerce

The plaintiff, Corinthian, placed an order for 1000 vials of a vaccine manufactured by defendant, Lederle, when it received inside information that the price per vial was set to increase substantially one day before the prices were to go into effect. The information was obtained from an internal document circulated by Lederle to its sales staff. Corinthian immediately placed its order via an electronic ordering system. Lederle delivered the first 50 vials at the initial market price but refused to fill the order for the subsequent 950 vials, citing the standard terms and conditions on its invoices which read: “Acceptance of the order is expressly conditioned on buyer's assent to seller's terms and conditions... [p]rices are subject to change without notice at any time prior to shipment, and that Lederle would not be liable for failure to perform the contract if the materials reasonably available to the seller were less than the needs of the buyer.” Lederle later agreed to provide 50 vials at the initial market price and informed Corinthian that although the remaining 950 vials would be shipped at the new price, it could cancel its order for said remainder. Corinthian brought an action seeking specific performance for the remaining 950 vials. Lederle filed for summary judgment. The court held that the shipment of the 50 vials in response to Corinthian’s order was not an acceptance of Corinthian’s offer at the initial market price, but was, rather, an accommodation. Lederle could rely on the invoice’s terms and conditions. Accordingly, Corinthian’s action for specific performance was denied.

iTravel2000.com Inc v Fagan [2001] OJ No 943 (Ont Sup Ct) – this case was the basis for Cases and Problems 8
This case concerns an internet domain name dispute. The plaintiff, Itravel2000.com filed an interlocutory injunction to restrain Fagan from removing himself as registrant of the domain name itravel.ca, citing irreparable harm. Furthermore, the plaintiff sought to have ownership of the domain name transferred to it. Itravel2000 had been operating in Canada under the business name “itravel” which had been registered with the Business Names Act since October 1998. Fagan was not in the travel business. Fagan had owned the domain name for a lesser time period. Both parties had pending trade-mark registration applications for the mark “itravel.” Fagan purported to own said trade-mark and offered to sell the domain name in dispute to Itravel for $75,000. Given Itravel’s longer use of the name, the balance of convenience favoured the granting of the injunction sought. The determination of the correct owner of the domain name was not made.

Pro-C Ltd v Computer City Inc [2000] OJ No 2823 (Ont Sup Ct) – this case was the basis for Cases and Problems 9
In this case, the plaintiff, Pro-C brought an action against the defendant for trade-mark infringement. Pro-C is the registered Canadian owner of the trade-mark WINGEN. It sold software under this mark and maintained a corresponding web site at wingen.com. Computer City planned to sell computers under the name WINGEN over a website available to Canadian citizens. Computer City was aware of the plaintiff’s mark but continued nonetheless. Potential customers searching for information on the defendant’s products overloaded the plaintiff’s computers. The defendant did not desist when notified. The Court found that advertisement of the mark on the defendant’s web site constituted use in Canada. Accordingly, the court held that Computer City had infringed
the plaintiff’s trade-mark. Damages were assessed at $450,000. In addition, punitive damages of $750,000 were awarded for the defendant’s continued use despite awareness of harm caused to the plaintiff.