5.1 Legal and Ethical Issues

The acceptance of the Internet by the business community in the mid 1990s has resulted in a period of extraordinary growth in global electronic communications. However, to ensure the longer-term success of e-Business there have been calls for an adequate enabling framework to be put in place, particularly of a legislative nature. Stakeholders are demanding a more stable environment in which to conduct routine business and consumer transactions.

In past, technical issues (e.g. inter-connection, inter-working, inter-operability) were the main concerns of the e-Business companies. In present, many companies aim at creating the necessary commercial environment (e.g. competitiveness, framework and market access) to stimulate the emergence of a global marketplace. The situation has changed yet again with the growth of the Internet, more specifically the Web. It is now common practice for companies to use the Web to advertize and promote their products and services, often including copies of product brochures, other promotional materials, and contact details. In near future, e-Businesses will involve greater concerns for legislative actions (e.g. liability, jurisdiction, taxation, copyright, data protection, encryption, authentication, consumer rights) to safeguard the interests of all stakeholders with a sound technology base and commercial infrastructure. (Figure 5.1)

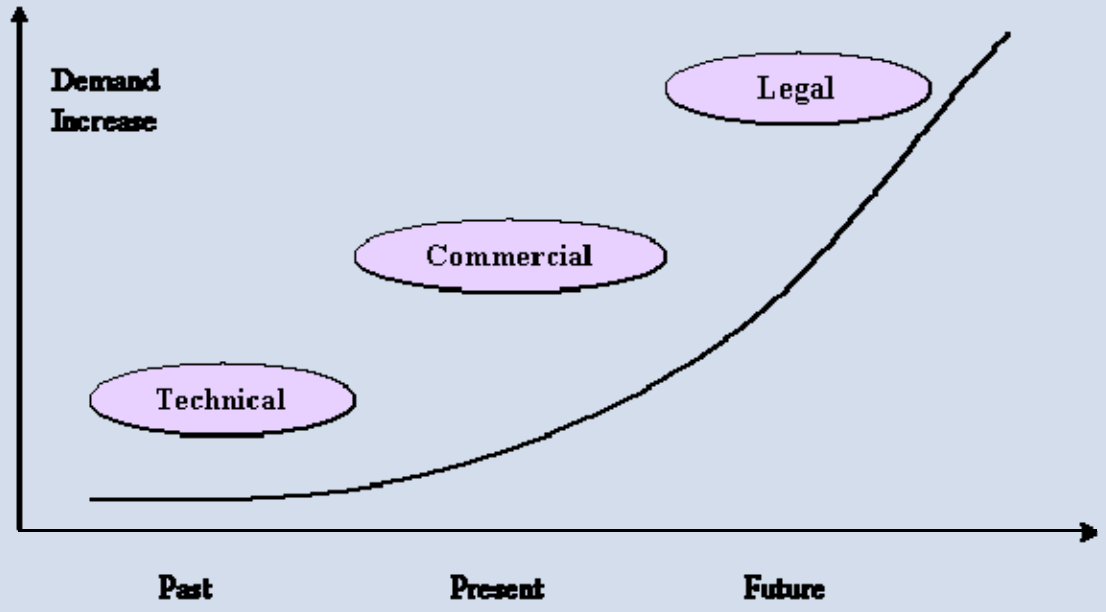


Figure 5.1 The change of demand by time in the e-Business global marketplace

The Internet has posed significant challenges to the legal structure. Copyright infringement has come up against file-sharing technology, and privacy continues to be challenged by personalization mechanisms. There are differences between the *physical environment* consisting of chronological and geographic boundaries, and *cyberspace,* the kingdom of digital transmission not limited by geography. The legal issues are of far more concern for those engaged in online commercial

transactions over the Web than the more traditional business. This is because in the case of traditional business interactions usually some previous negotiations have established a relationship between the trading parties, whereas online customers appear as spontaneous users usually with no such prior relationship having been established between buyer and seller [3].

Common Legal Disagreements on the Internet: Disagreements on the Internet in an online shopping scenario occur often because of one of the following reasons:

- The customer pays, but the merchant does not deliver.
- The customer pays, but the merchant delivers the wrong goods or in less quantity or broken.
- The customer pays, but the money does not arrive at the seller.
- The merchant delivers, but the customer refuses to pay.
- The merchant delivers, but the customer has not ordered anything.

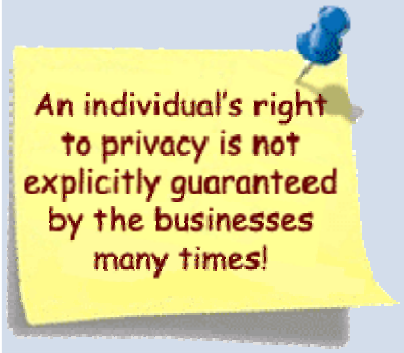
These are the most common issues between buyer and seller. In order to resolve them, laws are in place to support one or the other. The problem that arises with the Internet is that other than in a local shop the buyer and the seller may be in two different countries, whereby the web server could be in a third country. The important thing for the courts to decide is where the business transaction has taken place. Depending on the Country where the transaction has taken place the laws are enforced [2].

5.2 Legal Issues

The application of traditional law to the Internet is not always straightforward. The following four items are about privacy on the Internet, the others relate to the other areas of concern.

Privacy Rights

An individual's right to privacy is not explicitly guaranteed by the businesses many times, but protection from government intrusion should be implicitly guaranteed. With widely usage of the Internet , the right to individual privacy moved beyond private property. The Internet is currently a *self regulated* medium. The Internet industry essentially governs itself. This condition enables the Internet to grow without the constraints of legislation, but it also creates problems because there are few specific guidelines to follow.



Many Internet companies collect users' personal information as the users navigate through a site. P rivacy advocates argue that these efforts violate individuals' privacy rights . On the other hand, online marketers and advertisers suggest that, by recording the likes and dislikes of online consumers, online companies can better serve their users. For example, if one purchases a ticket from Istanbul to Ankara , the travel site might record this transaction. In the future, when a ticket goes on sale for the same flight, the Web site can inform the person. It is true that there are advantages of collecting users' personal information as a marketing tactic and the methods used for collection. Nevertheless, there are thoughtful consequences as well. Consider a different scenario. For instance, in near future,

Web sites providing health information to consumers could potentially share this information with third parties. If one visits a Web site and download information on cancer, AIDS and other life-threatening diseases, this information could be distributed without your knowledge or permission. In this case, you could be left without a job.

In fact, most privacy protection legislation protects consumers against advertisers, but it does not mention content providers. Many Web sites studied collected personal information; a few of those sites gave any indication to the consumer that information was being collected. Some Web sites contain third-party tracking devices (e.g. log-file analysis, data mining, customer registration and cookies) that collect consumer data. Cookies, perhaps the most common of tracking devices, are concerning to consumers.

According to consumers, online security is a major concern. Many users are uncertain to use their credit-card numbers for online transactions in the event that records are kept of what they purchased and from where it was purchased. Businesses must provide consumers with the ability to actively choose not to have their information shared with third parties, for online privacy.

Many e-businesses are creating specific positions to manage consumer privacy. Chief Privacy Officers (CPOs) are responsible for maintaining the integrity of a Web site's privacy policy. This involves creating policies and serving as an intermediary to government officials regarding privacy issues. American Express and Microsoft are among organizations that employ a CPO.

Employee Privacy Rights: Many businesses monitor employee activities on company and communications equipment. One of the newest observation technologies are keystroke cops, generating tension between employers and employees. Keystroke software provides an inexpensive, easy-to-use method of monitoring productivity and the mistreatment of company equipment. For example, Raytown Corporation LLC offers a variety of surveillance software that is available at a fee for download from the site [6].

The observation software is loaded onto the hard drive of an employee's computer, or it can be sent to an unsuspecting employee as an e-mail attachment. Once activated, the software registers each keystroke before it appears on the screen. Many products also have scanning capabilities that enable them to search through documents for keywords such as “boss” and “union”, etc.

When implementing a surveillance mechanism, make it known. This way, surveillance takes on a protective role, saving both parties time and energy. For example, letting your employees knows what is expected of them will, in many cases, cut back on the amount of time wasted surfing the Internet and sending e-mail to family and friends. Proponents of notification argue that prevention would reduce the number of questionable transactions made over the Internet. However, opponents suggest that notification could result in lawsuits, as the recipients of the questionable e-mail or other communications could argue that the company

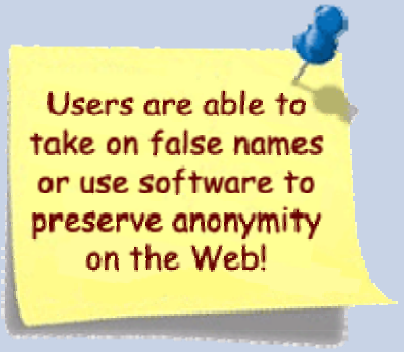
knowingly allowed these transactions to be made [1].

In order to determine the outcome of court cases on these issues, the courts propose the determination of two criteria: (1) did the employee have a reasonable expectation of priv acy and (2) does the business have legal business interests that would reasonably justify the intrusion of an employee's privacy.

5.3 Privacy Protection

Users' Privacy Protection

Web users are able to take on falsified identities or use software to maintain secrecy on the Web. For example, PrivacyX.com a free Internet service, allows users to surf the Web unidentified. To do this, PrivacyX.com creates a digital certificate for new users when they register. The Web site service allows that anonymity can be maintained even in the digital certificate, which holds no personal information the user does not wish to include. PrivacyX.com then uses the digital certificate to return the requested information to the user, encrypted.



The World Wide Web Consortium is introducing the *Platform for Privacy Preferences Project (P3P) .* Microsoft and IBM, already employ the P3P protocol. The P3P privacy policies are XML-based applications. This system allows the preferences of users to be matched precisely to the site's standardized privacy protocols. It does not enforce Web sites to abide by their own policies, at the same time as it will prompt users if the privacy policy of a particular Web site does not match the users' given preferences. Opponents warn that this method will instead present Internet users with a false sense of security that their privacy is being protected. To find more information on privacy issues, you can visit www.epic.org and www.privacyrights.org .

Businesses Privacy Protection

It is vital to include a privacy policy on your Web site, respect the stated policy and treat your visitors' information with care. This includes conducting regular audits to recognize exactly what information is being collected through Web site of the business. There are several services available over the Web that can generate a privacy policy according to a business needs. For instance, PrivacyBot .com features a survey concerning interests of the business in collecting consumer information and tries to specify how the business plans to use the collected information.

The Federal Trade Commission (FTC) has established five *Core Fair Information Practices* regarding online marketing tactics that involve gathering and using consumer information [7]:

1. Consumers should be made aware that personal information will be

collected.
2. The consumer should have a say in how this information will be used.
3. The consumer should have the ability to verify the information collected to ensure that it is complete and correct.
4. The information collected should be secured.
5. The Web site should be responsible for considering that these practices are followed.

Not all sites carrying the mark of a security company make the effort to follow their privacy guidelines. It is still up to the organization to honor its stated privacy policies.

Network Advertising Initiative

In an effort to support self-regulation, The Federal Trade Commission (FTC) approved the Network Advertising Initiative (NAI) in July 1999. The NAI is a cooperative of online marketing, analytics, advertising and email companies who are committed to addressing important privacy and consumer protection issues in emerging media [4]. The group was established to determine the proper protocols for managing a Web user's personal information on the Internet. While the Initiative prohibits the collection of consumer data from medical and financial sites, it allows the combi nation of Web-collected data and personal information.

It has also taken steps to dictate how this information should be collected, including issues of user notification and allowing users access to their own records. You can look at the Appendix I for information on DoubleClick, a Web advertiser.

The opponents to the NAI argue that what may appear to be good self-regulation to one group may he a violation of privacy to another. The FTC plans to continue pursuing a method of regulating privacy on the Internet, except has agreed to offer the *NAI* a *safe harbor* provision provided that the Initiative acts according to FTC protocols. [5]

Defamation

Defamation is the act of injuring another's reputation, honor or good name through false written or oral communication. In law, defamation is the communication of a statement that makes a false claim, expressly stated or implied to be factual, that may harm the reputation of an individual, business, product, group, government or nation. Most jurisdictions provide legal actions, civil and/or criminal, to punish various kinds of defamation [8]. Defamation contains two parts:

- *Slander :* This is a spoken defamation.
- *Libel:* These statements are written or are spoken in a context in which

they have permanence and commonness that exceed slander. For instance, broadcasting is considered libelous although it is spoken.

To verify defamation, an applicant's case must meet following requirements:

- The statement must, in fact, be defamatory.
- The statement must have been published, spoken or broadcast.
- There must be identification of the individual(s) through name or reasonable connection.
- There must be evidence of injury or definite loss .

The responsibility of defamatory statements is addressed in Appendix II.

5.4 Electronic Cash (E-Cash)

Similar to regular cash, e-cash enables transactions between customers without the need for banks or other third parties. When used, e-cash is transferred directly and immediately to the participating merchants and vending machines. Electronic cash is a secure and convenient alternative to bills and coins. This payment system complements credit, debit, and charge cards and adds additional convenience and control to everyday customer cash transactions. E-cash usually operates on a smart card, which includes an embedded microprocessor chip. The microprocessor chip stores cash value and the security features that make electronic transactions secure. Mondex, a subsidiary of MasterCard (Mondex Canada Association) is a good example of e-cash.

E-cash is transferred directly from the customer's desktop to the merchant's site. Therefore, e-cash transactions usually require no remote authorization or personal identification number (PIN) codes at the point of sale. E-cash can be transferred over a telephone line or over the Web. The microprocessor chip embedded onto the card keeps track of the e-cash transactions. Using e-cash the customer has two options: a stand-alone card containing e-cash or a combination card that incorporates both e-cash and debit .

How a typical e-cash system works: A customer or merchant signs up with one of the participating banks or financial institutions. The customer receives specific software to install on his or her computer. The software allows the customer to download “electronic coins” to his or her desktop. The software manages the electronic coins. The initial purchase of coins is charged against the customer's bank account or against a credit card. When buying goods or services from a web site that accepts e-cash, the customer simply clicks the “Pay with e-cash” button. The merchant's software generates a payment request, describing the item(s) purchased, price, and the time and date. The customer can then accept or reject this request. When the customer accepts the payment request, the software residing on the customer's desktop subtracts the payment amount from the balance and creates a payment that is sent to the bank or the financial institution of the merchant, and then is deposited to the merchant's account. The attractive feature of the entire process is its turnaround time which is a few seconds. The merchant is notified and in turn ships the goods.

5.5 Electronic Checks (E-Check)

E-check is the result of cooperation among several banks, government entities, technology companies, and e-commerce organizations. An e-check uses the same legal and business protocols associated with traditional paper checks. It is a new payment instrument that combines high-security, speed, convenience, and processing efficiencies for online transactions. It shares the speed and processing efficiencies of all-electronic payments. An e-check can be used by large and small organizations, even where other electronic payment solutions are too risky or not appropriate. The key advantages of e-checks are as follows:

- Secure and quick settlement of financial obligations
- Fast check processing
- Very low transaction cost

E-check is being considered for many online transactions. Appendix II shows an e-check transaction.

Appendix I

Doubleclick - *Marketing with Personal Information* [1]

While privacy advocate groups argue that the Web will not survive without some login of regulation advertising organizations disagree. DoubleClick, an Internet advertising firm suggests that advertising must be effective to minimize Internet-related costs. Regulation of the Internet could limit a company's efforts to buy and sell advertising. As with television and radio advertising, the money generated by Internet advertising can allow people of all economic means to use the medium.

Web sites use a variety of tracking methods to record where visitors come from, where they go and what catches their interest along the way. This information is tied to your computer's IP address (i.e., the numerical address of your computer on the Internet), Web browser and operating system; it is used by marketers to target relevant advertisements at specific computers. DoubleClick has an advertising network of more than l,500 sites where banner advertisements for 11,000 of its clients appear. This network enables DoubleCliek to combine data from many sites to target advertisements for particular computers.

However, targeting a specific IP address, browser and operating system is less effective than targeting a specific consumer. In 1999, DoubleCliek acquired Abacus Direct Corporation, a direct-marketing organization. Abacus stores names, addresses, telephone numbers, age, gender, income levels and a history of purchases at retail, catalog and online stores. This acquisition enabled DoubleClick to attach personal information to the activities of what were once “nameless” personal computers.

One concern with this method of collecting and using data is termed *digital redlining.* Digital redlining suggests that a company could skew an individual's knowledge of available products by basing the advertisements the user sees on past behavior. This practice could allow advertisers to influence consumers' habits by limiting the information they see to what the advertisers determine the consumers want to see.

Direct marketing in the traditional sense affords a certain time lapse between an individual's purchases, the processing of that information and the use of that information to target the particular customer. However, users can be targeted instantly as they browse the Internet.

Perhaps of greater concern is the recording of personal activities. The Internet is appreciated as a medium in which users can search for information and express opinions anonymously. Privacy advocates are concerned that such data could be used against individuals attempting to obtain housing, get a loan, and apply for insurance coverage. For example, a user visiting a Web site to learn more about an illness might not want that information to be made available to insurance companies. DoubleCliek promises to uphold its privacy policy, which assures users that the company will not collect financial, sexually oriented or medical information. In response to concerns about privacy, DoubleCliek has joined the Network Advertising Initiative.

Appendix II

Cubby v. CompuServe & Stratton Oakmont v. Prodigy [1]

Cubby v. CompuServe

In the case *Cubby v. CompuServe* , an anonymous individual used a news service hosted by CompuServe to post an allegedly defamatory statement. As the provider of the bulletin board, CompuServe claimed that it could not be held legally responsible for the defamatory statements, because CompuServe was not the publisher of the statement.

The deciding factor in this case rested on the distinction between *distributor* and *publisher* . In the court's opinion, a distributor cannot be held legally responsible for a defamatory statement unless the distributor has knowledge of the content. As a result, CompuServe and other providers cannot be held responsible far their users' statements.

Stratton Oakmont v. Prodigy

On the other hand, there was a fine line between claiming responsibility as a publisher of users' content and maintaining the “distance” of a distributor. This can be discovered when addressing the case *Stratton Oakmont v. Prodigy* .

Prodigy differed from CompuServe in that it, as an ISP, claimed responsibility to remove potentially defamatory or otherwise questionable material when the material has been brought to its attention. Prodigy further claimed that it had an automatic scanning device that screens bulletin board postings before they are posted.

As a result, Prodigy assumed the role of a publisher by claiming control over specific statements made by its users. As a publisher, Prodigy was held legally responsible for the posted statements.