



E-commerce

business. technology. society.

Third Edition

Kenneth C. Laudon
Carol Guercio Traver



Chapter 9

Ethical, Social, and Political Issues in E-commerce

Warez Hackers End Up in the Slammer

Class Discussion

- What are “Warez” groups? What are their motivations? How to they differ from typical downloaders?
- What are the main specialties of wares groups?
- Why are members of Warez groups facing criminal charges and possible jail terms? What laws are they violating?
- How is the RIAA responding to illegal copying and distribution of music files?



Understanding Ethical, Social, and Political Issues in E-commerce

- Internet technology and its use in e-commerce disrupts existing social and business relationships and understandings
- Costs and benefits of technology must be carefully considered, especially when there are as yet no clear-cut legal or cultural guidelines

Unique Features of E-Commerce Technology and Their Potential Ethical, Social and/or Implications

Table 9.1, Page 502

TABLE 9.1	UNIQUE FEATURES OF E-COMMERCE TECHNOLOGY AND THEIR POTENTIAL ETHICAL, SOCIAL, AND/OR POLITICAL IMPLICATIONS
E-COMMERCE TECHNOLOGY DIMENSION	POTENTIAL ETHICAL, SOCIAL, AND POLITICAL SIGNIFICANCE
<p>Ubiquity—Internet/Web technology is available everywhere: at work, at home, and elsewhere via mobile devices, anytime.</p> <p>Global reach—The technology reaches across national boundaries, around the earth.</p> <p>Universal standards—There is one set of technology standards, namely Internet standards.</p> <p>Richness—Video, audio, and text messages are possible.</p> <p>Interactivity—The technology works through interaction with the user.</p> <p>Information density—The technology reduces information costs, raises quality.</p> <p>Personalization/Customization—The technology allows personalized messages to be delivered to individuals as well as groups.</p>	<p>Work and shopping can invade family life; shopping can distract workers at work, lowering productivity; use of mobile devices can lead to automobile and industrial accidents. Presents confusing issues of “nexus” to taxation authorities.</p> <p>Reduces cultural diversity in products; weakens local small firms while strengthening large global firms; moves manufacturing production to low-wage areas of the world; weakens the ability of all nations—large and small—to control their information destiny.</p> <p>Increases vulnerability to viruses and hacking attacks worldwide affecting millions of people at once. Increases the likelihood of “information” crime, crimes against systems, and deception.</p> <p>A “screen technology” that reduces use of text and potentially the ability to read by focusing instead on video and audio messages. Potentially very persuasive messages possible that may reduce reliance on multiple independent sources of information.</p> <p>The nature of interactivity at commercial sites can be shallow and meaningless. Customer e-mails are frequently not read by human beings. Customers do not really “co-produce” the product as much as they “co-produce” the sale. The amount of “customization” of products that occurs is minimal, occurring within predefined platforms and plug-in options.</p> <p>While the total amount of information available to all parties increases, so does the possibility of false and misleading information, unwanted information, and invasion of solitude. Trust, authenticity, accuracy, completeness, and other quality features of information can be degraded. The ability of individuals and organizations to make sense of out of this plethora of information is limited.</p> <p>Opens up the possibility of intensive invasion of privacy for commercial and governmental purposes that is unprecedented.</p>

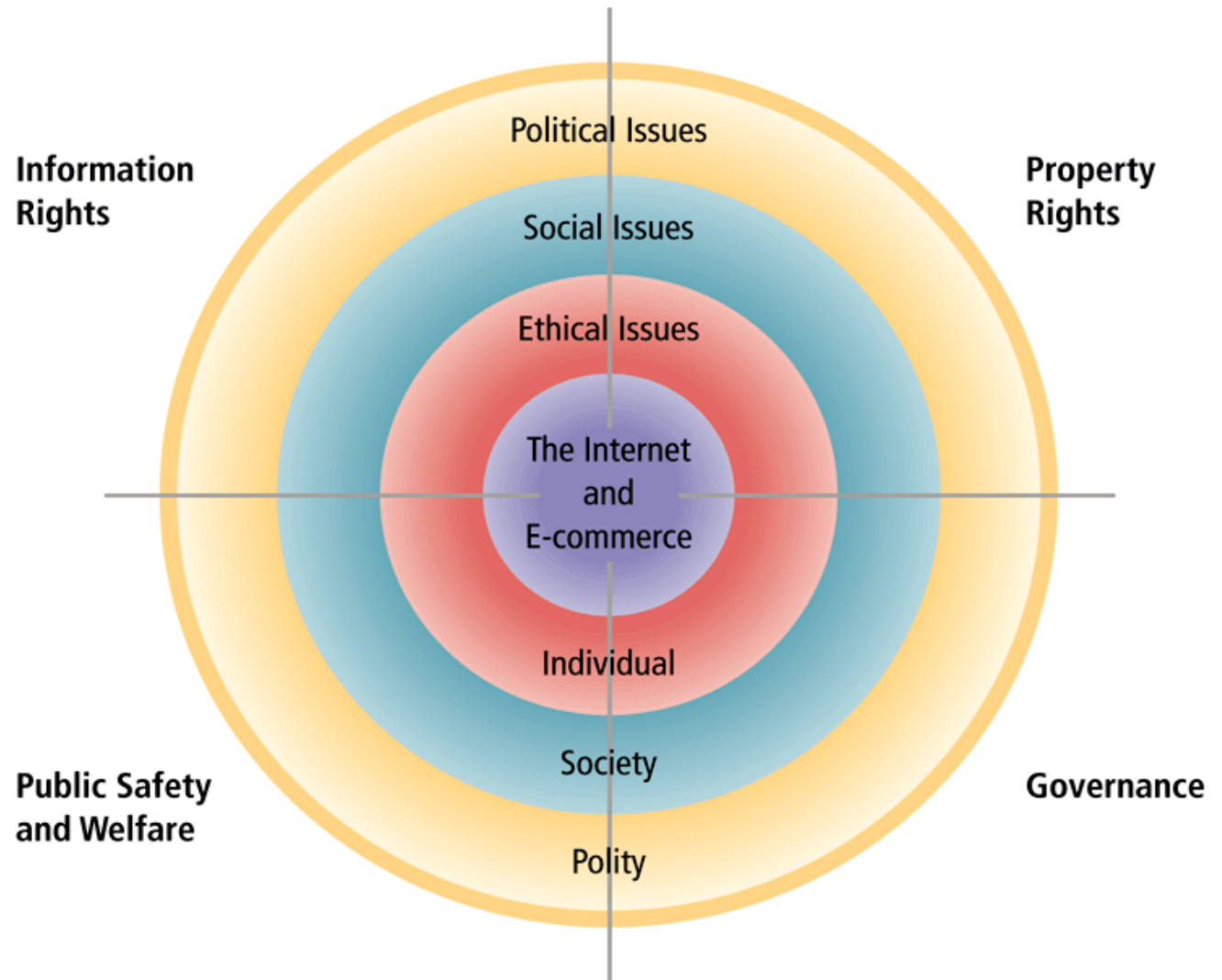


A Model for Organizing the Issues

- Issues raised by Internet and e-commerce can be viewed at individual, social, and political levels
- Four major categories of issues
 - Information rights
 - Property rights
 - Governance
 - Public safety and welfare

The Moral Dimensions of an Internet Society

Figure 9.1, Page 503



Basic Ethical Concepts

- **Ethics:** Study of principles that individuals and organizations can use to determine right and wrong courses of action
- **Responsibility:** As free moral agents, individuals, organizations, and societies are responsible for the actions they take
- **Accountability:** Individuals, organizations, and societies should be held accountable to others for the consequences of their actions
- **Liability:** Extends the concepts of responsibility and accountability to area of law
- **Due process:** Refers to process by which laws are known and understood, with ability to appeal to higher authorities to ensure that laws have been correctly applied

Analyzing Ethical Dilemmas

- Process for analyzing ethical dilemmas:
 1. Identify and clearly describe the facts.
 2. Define the conflict or dilemma and identify the higher-order values involved.
 3. Identify the stakeholders.
 4. Identify the options that you can reasonably take.
 5. Identify the potential consequences of your options.

Candidate Ethical Principles

- One or more of the following well-established ethical principles can be used to help you determine your actions when confronted with an ethical dilemma:
 - Golden Rule
 - Universalism
 - Slippery Slope
 - Collective Utilitarian Principle
 - Risk Aversion
 - No Free Lunch
 - The *New York Times* Test (Perfect Information Rule)
 - The Social Contract Rule



The Concept of Privacy

- Privacy: The moral right of individuals to be left alone, free from surveillance or interference from other individuals or organizations
- Information privacy: Includes both the claim that certain information should not be collected at all, as well as the claim of individuals to control the use of whatever information is collected about them



E-commerce and Privacy

- Major ethical issue related to e-commerce and privacy: Under what conditions should we invade privacy of others
- Major social issue: Development of “expectations of privacy” and privacy norms
- Major political issue: Development of statutes that govern relations between recordkeepers and individuals



Information Collected at E-commerce Sites

- Personally identifiable information (PII): Data that can be used to identify, locate, or contact an individual
- Anonymous information: Demographic and behavioral information that does not include any personal identifiers
- Almost all e-commerce companies collect PII and use cookies to track clickstream behavior



Profiling and Behavioral Targeting

- Profiling: Creation of digital images that characterize online individual and group behavior
- Anonymous profiles: Identify people as belonging to highly specific and targeted groups
- Personal profiles: Add personal identifiers
- Advertising networks can:
 - Track both consumer behavior and browsing behavior on the Web
 - Dynamically adjust what the user sees on screen
 - Build and refresh high-resolution data images or behavior profiles of consumers



Legal Protections for Privacy

- May be explicitly granted or derived from constitutions (U.S., Canada, Germany)
- May also be found in common law (U.S, England)
- In U.S, also found in federal and state laws and regulations



Informed Consent

- Consent given with knowledge of all the material facts needed to make a rational decision
- Two models:
 - Opt-in
 - Opt-out
- Many U.S. e-commerce firms merely publish information practices as part of privacy policy without providing for any form of informed consent



Statutory and Regulatory Protections of Online Privacy

- In U.S., Federal Trade Commission has taken lead in conducting research and recommending legislation to Congress
- FTC Fair Information Practice Principles (1998):
 - Notice/Awareness (Core)
 - Choice/Consent (Core)
 - Access/Participation
 - Security
 - Enforcement

FTC's Fair Information Practice Principles

Table 9.7, Page 519

TABLE 9.7	FEDERAL TRADE COMMISSION'S FAIR INFORMATION PRACTICE PRINCIPLES
Notice/Awareness (Core principle)	Sites must disclose their information practices before collecting data. Includes identification of collector, uses of data, other recipients of data, nature of collection (active/inactive), voluntary or required, consequences of refusal, and steps taken to protect confidentiality, integrity, and quality of the data
Choice/Consent (Core principle)	There must be a choice regime in place allowing consumers to choose how their information will be used for secondary purposes other than supporting the transaction, including internal use and transfer to third parties. Opt-in/Opt-out must be available.
Access/Participation	Consumers should be able to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.
Security	Data collectors must take reasonable steps to assure that consumer information is accurate and secure from unauthorized use.
Enforcement	There must be in place a mechanism to enforce FIP principles. This can involve self-regulation, legislation giving consumers legal remedies for violations, or federal statutes and regulation.

SOURCE: Federal Trade Commission, 1998; 2000a.

FTC Recommendations Regarding Online Profiling

Table 9.8, Page 520

TABLE 9.8	FTC RECOMMENDATIONS REGARDING ONLINE PROFILING
PRINCIPLE	DESCRIPTION OF RECOMMENDATION
Notice	Complete transparency to user by providing disclosure and choice options on the host Web site. "Robust" notice for PII (time/place of collection; before collection begins). Clear and conspicuous notice for non-PII.
Choice	Opt-in for PII, opt-out for non-PII. No conversion of non-PII to PII without consent. Opt-out from any or all network advertisers from a single page provided by the host Web site.
Access	Reasonable provisions to allow inspection and correction.
Security	Reasonable efforts to secure information from loss, misuse, or improper access.
Enforcement	Done by independent third parties, such as seal programs and accounting firms.
Restricted collection	Advertising networks will not collect information about sensitive financial or medical topics, sexual behavior or sexual orientation, or use social security numbers for profiling.



The European Directive on Data Protection

- Privacy protection much stronger in Europe than in United States
- European approach: Comprehensive and regulatory in nature
- European Commission's Directive on Data Protection: Standardizes and broadens privacy protection in European Union countries
- Department of Commerce safe harbor program for U.S. firms that wish to comply with Directive



Private Industry Self-Regulation

- Safe harbor: Private, self-regulating policy and enforcement mechanism that meets objectives of government regulations and legislation, but does not involve government regulation or enforcement
 - Example: Privacy seal programs such as TRUSTe Internet privacy protection program
- Industry associations include:
 - Online Privacy Alliance
 - Network Advertising Initiative



Insight on Business: Chief Privacy Officers

Class Discussion

- What does a Chief Privacy Officers do?
- Why do corporations need a CPO?
- What is a “privacy audit?”
- Why did ChoicePoint hire a CPO?
- How do federal laws like Graham-Leach Bliley and HIPPA influence corporate privacy practices?
- What is a “legalistic” approach to privacy as opposed to a “pro-consumer” approach?

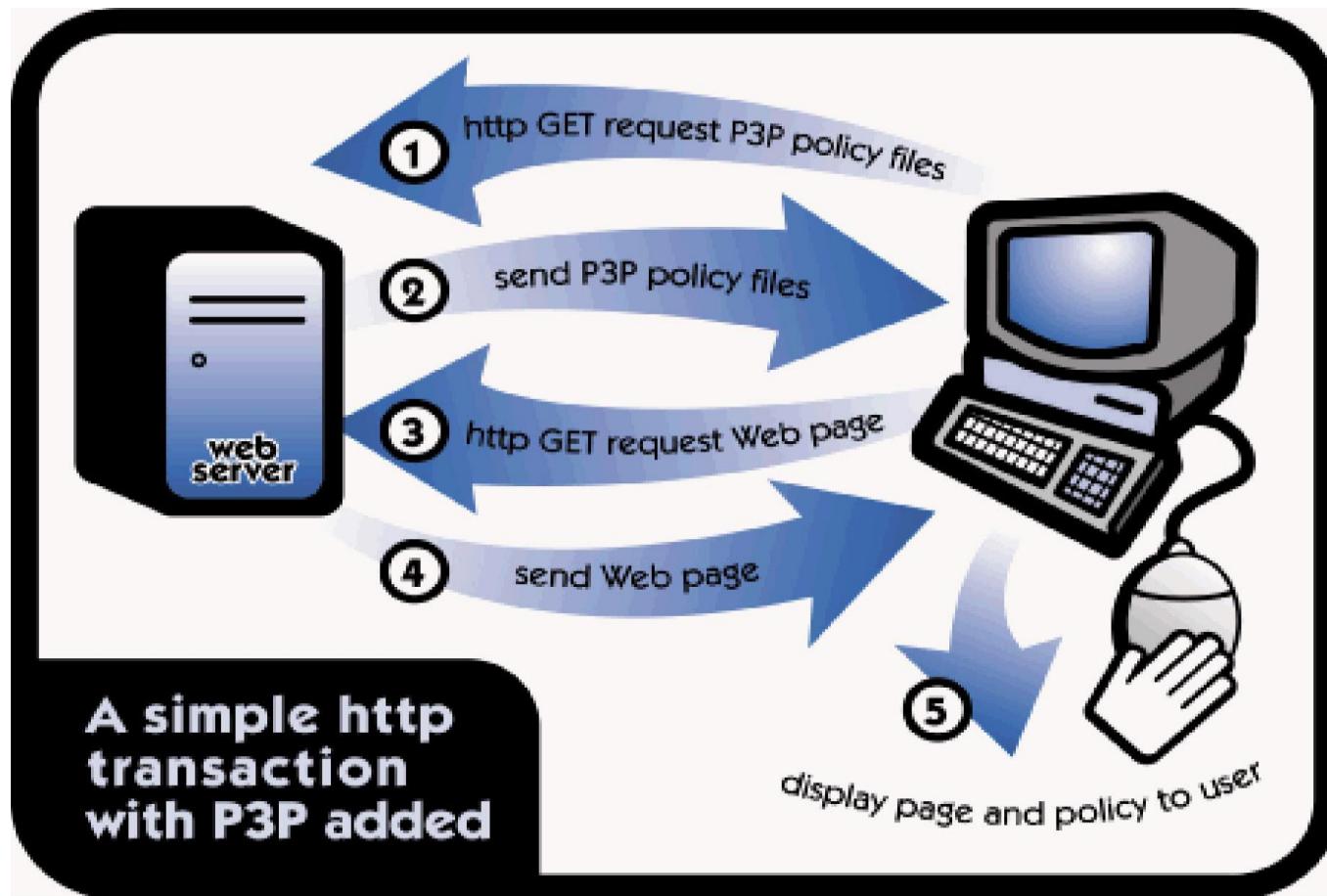


Technological Solutions to Privacy Invasion on the Web

- Many privacy-enhancing technologies being developed emphasize security
- Platform for Privacy Preferences (P3P):
Comprehensive technological privacy protection effort sponsored by W3C
 - Is a standard designed to communicate to Internet users a Web site's privacy policy, and to compare that policy against user's preferences or to other standards such as FTC's FIP guidelines or EU's Data Protection Directive

How P3P Works

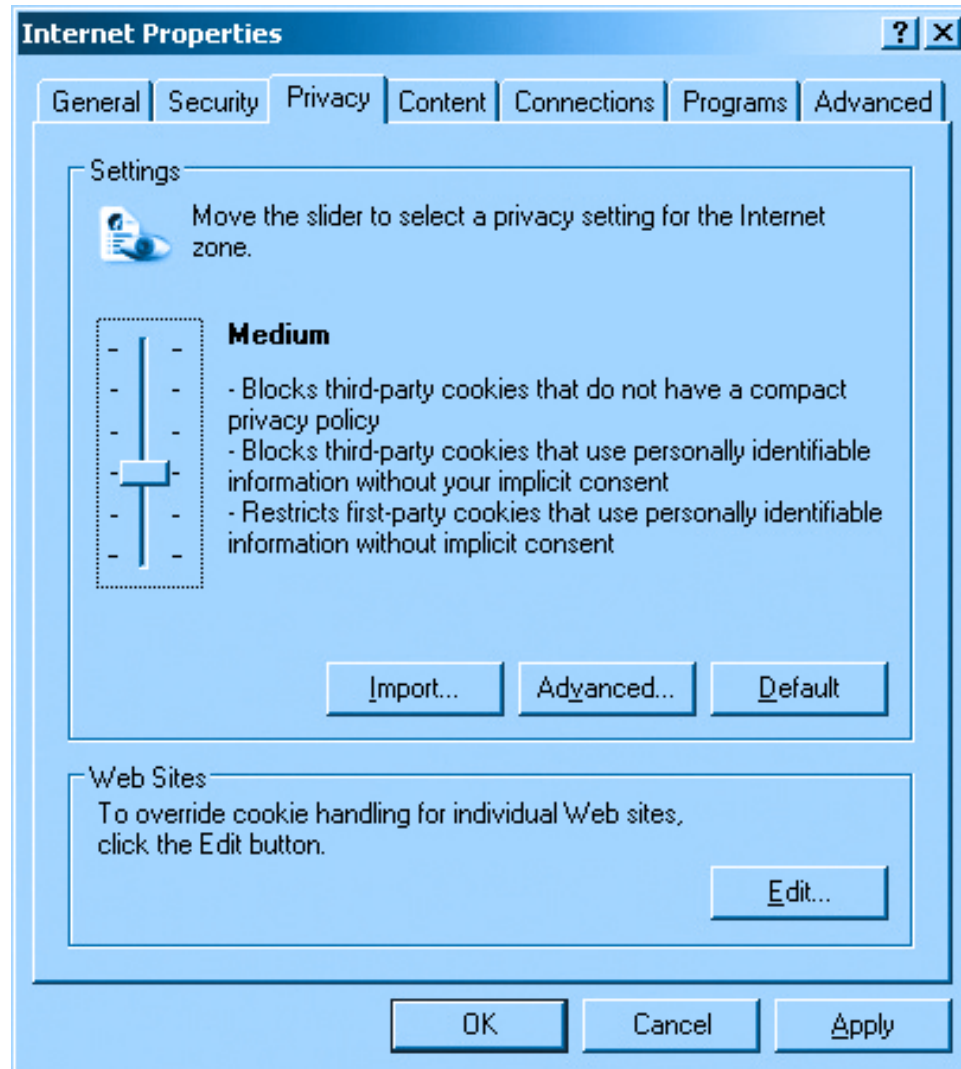
Figure 9.2(A), Page 527



SOURCE: W3C Platform for Privacy Preferences Initiative, 2003.

Internet Explorer 6.0's Implementation of P3P

Figure 9.2(B), Page 528





Insight on Technology: The Privacy Tug of War: Advertisers Vs. Consumers

Class Discussion

- What are some of the technologies being used to invade privacy?
- What are some of the technologies being used to protect privacy?
- Do you accept the trade off between privacy invasion and “free” Web content?
- Do consumers support the idea of giving up personal information in return for “free” content?

Intellectual Property Rights

- Intellectual property: Encompasses all tangible and intangible products of human mind
- Major ethical issue: How should we treat property that belongs to others
- Major social issue: Is there continued value in protecting intellectual property in the Internet age?
- Major political issue: If, and if so, how, should Internet and e-commerce be regulated/governed to protect intellectual property
- Main types of intellectual property protection:
 - Copyright
 - Patent
 - Trademark law



Copyright: The Problem of Perfect Copies and Encryption

- Copyright law: Protects original forms of expression (but not ideas) from being copied by others for a period of time
- Look and feel copyright infringement lawsuits involve distinction between an idea and its expression
- Fair use doctrine: Under certain circumstances, permits use of copyrighted materials without permission
- Digital Millennium Copyright Act of 1998 (DMCA): First major effort to adjust copyright laws to Internet age
- DMCA implements WIPO treaty that makes it illegal to make, distribute, or use devices that circumvent technology-based protections of copyrighted materials

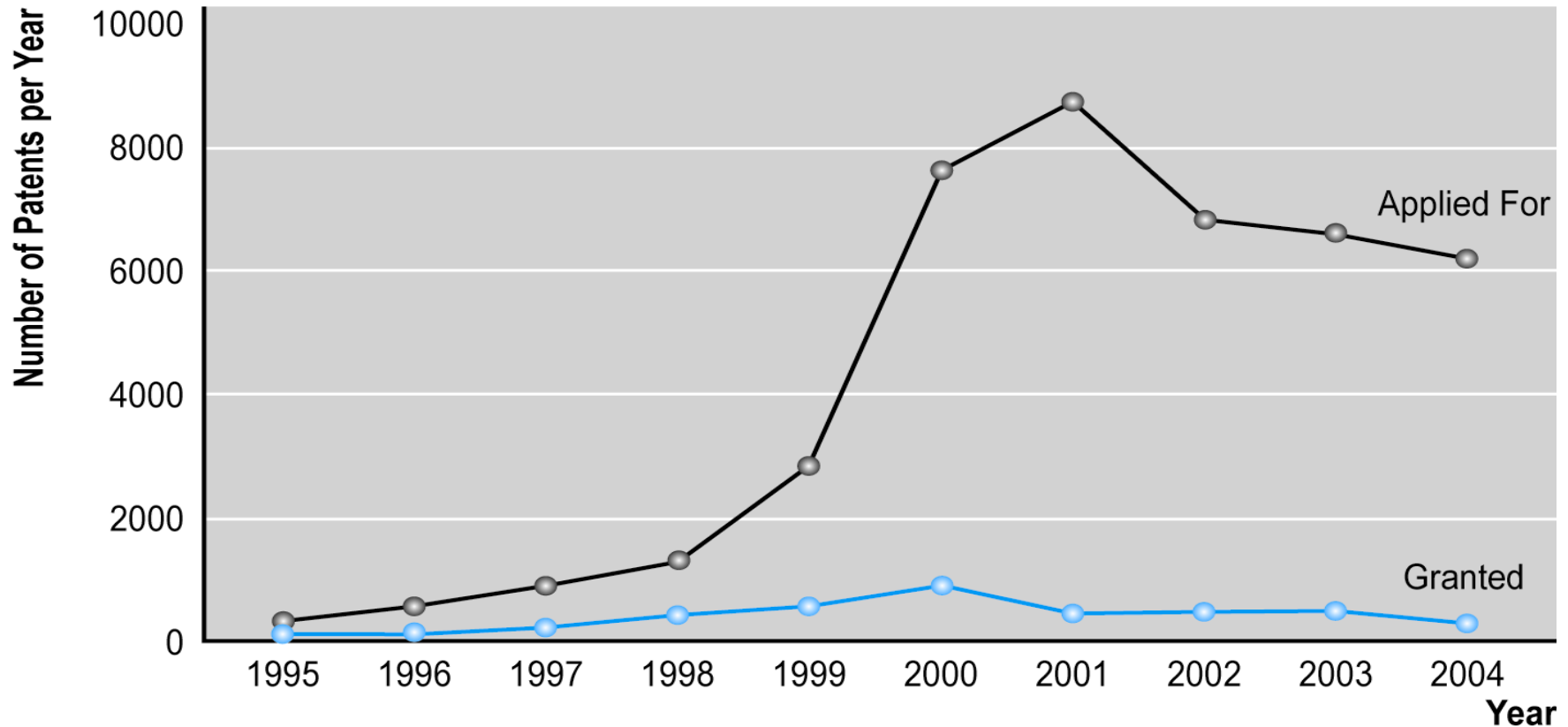


Patents: Business Methods and Processes

- Patent: Grants owner a 20-year exclusive monopoly on ideas behind an invention
- Most of early inventions that made Internet and e-commerce possible were not patented by their inventors
- With commercial development of Internet, came desire for patents
- Business methods patents have been widely sought by Internet and e-commerce companies
- Many business methods Internet patents granted are overbroad, and if enforced, would significantly impact e-commerce

Internet and E-Commerce Business Method Patents

Figure 9.3, Page 538



SOURCE: Based on data from United States Patent and Trademark Office, 2005.

Trademarks: Online Infringement and Dilution

- Trademark: Mark used to identify and distinguish goods, and indicate their source
- Trademarks protect public by ensuring it gets what it pays for/expects to receive; protects trademark owner against piracy and misappropriation
- Infringement: Use of a trademark that creates confusion with existing marks, causes consumers to make market mistakes or misrepresents origins of goods
- Anticybersquatting Consumer Protection Act (ACPA): Creates civil liabilities for anyone who attempts in bad faith to profit from an existing famous or distinctive trademark by registering an Internet domain name that is identical or confusingly similar

Types of Trademark Abuse on Internet

- Cybersquatting: Registration of infringing domain name, or other Internet use, of existing trademark, for purpose of extorting payments from legitimate owners
- Cyberpiracy: Involves same behavior as cybersquatting, but with intent of diverting traffic from legitimate site to infringing site
- Metatagging: Using another's trademarks as metatags in a misleading or confusing manner
- Keywording: Using another's trademarks as keywords on search engines in a misleading or confusing manner
- Deep linking: Bypassing target site's home page and going directly to content page
- Framing: Displaying content of another site within frame or window

Governance

- Involves issue of social control
- Primary questions:
 - Who will control Internet and e-commerce
 - What elements will be controlled and how
- Stages of governance and e-commerce
 - Government Control Period (1970–1994)
 - Privatization (1995–1998)
 - Self-Regulation (1995–present)
 - Government Regulation (1998–present)



Who Governs E-commerce and the Internet?

- Currently we are in a mixed mode policy environment where self-regulation, through a variety of Internet policy and technical bodies, co-exists with limited government regulation
- Not true that Internet cannot be controlled. In fact, Internet can be very easily controlled, monitored, and regulated from a central location (such as done by China, Singapore, etc.)

Taxation

- Issue of taxation of e-commerce sales illustrates complexity of governance and jurisdiction issues
- National and international character of Internet sales wreaking havoc on traditional taxation schemes in U.S. based on local commerce and local jurisdictions
- December 2004: Congress extended tax moratorium on “multiple or discriminatory taxes on electronic commerce” until November 2007
- Unlikely that comprehensive, integrated rational approach to taxation issue will be determined for some time to come

Public Safety and Welfare

- Protection of children and strong sentiments against pornography
 - Passing legislation that will survive court challenges has proved difficult:
 - Communications Decency Act struck down
 - Children's Online Protection Act struck down (but still be considered by lower courts)
 - Children's Internet Protection Act upheld by Supreme Court (requires schools and libraries to install technology protection measures)
- Efforts to control gambling and restrict sales of drugs and cigarettes
 - Currently mostly regulated by state law

Insight on Society: The Internet Drug Bazaar

Class Discussion

- What's wrong with buying prescription drugs online, especially if the prices are lower?
- What are the risks and benefits of online pharmacies?
- Should online pharmacies require a physician's prescription?
- How do online pharmacies challenge the traditional business model of pharmacies and drug firms?
- Why hasn't federal legislation been adopted?
- Who benefits and who loses from online pharmacies?