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.

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

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.
**Basic Ethical Concepts**

- **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** – Do unto others as you would have them do unto you.
  - **Universalism** – if an action is not right for all situations, then it is not right for any specific situations.
  - **Slippery Slope** – if an action cannot be taken repeatedly, then it is not right to take it at all.
  - **Collective Utilitarian Principle** – take the action that achieves the greater value for all of society. It assumes one can prioritize values in a rank order and understand the consequences of various courses of action.
  - **Risk Aversion** – Take the action that produces the least harm, or the least potential cost.
  - **No Free Lunch** – assume that all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise.
  - **The New York Times Test** (Perfect Information Rule) – assume that the results of a decision will be the subject of the lead article in the NYT the next day. What will be the result?
  - **The Social Contract Rule** – can the society adopts the principle you are supporting?

**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

### Table 9.2

**PERSONAL INFORMATION COLLECTED BY E-COMMERCE SITES**

<table>
<thead>
<tr>
<th>Name</th>
<th>Bank accounts</th>
<th>ID numbers</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Credit card accounts</td>
<td>Personal data</td>
</tr>
<tr>
<td>Phone number</td>
<td>Gender</td>
<td>Transaction data</td>
</tr>
<tr>
<td>E-mail address</td>
<td>Age</td>
<td>Clickstream data</td>
</tr>
<tr>
<td>Social security number</td>
<td>Occupation</td>
<td>Education</td>
</tr>
</tbody>
</table>

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

### TABLE 9.7 FEDERAL TRADE COMMISSION’S FAIR INFORMATION PRACTICE PRINCIPLES

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice/Awareness (Core principle)</td>
<td>Sites must disclose their information practices before collecting data. Includes identification of collector, uses of data, other recipients of data, nature of collection (active/passive), voluntary or required, consequences of refusal, and steps taken to prevent confidentiality, integrity, and quality of the data.</td>
</tr>
<tr>
<td>Choice/Consent (Core principle)</td>
<td>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-out must be available.</td>
</tr>
<tr>
<td>Access/Participation</td>
<td>Consumers should have the ability to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.</td>
</tr>
<tr>
<td>Security</td>
<td>Data collectors must take reasonable steps to assure that consumer information is accurate and secure from unauthorized use.</td>
</tr>
<tr>
<td>Enforcement</td>
<td>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.</td>
</tr>
</tbody>
</table>

### TABLE 9.8 FTC RECOMMENDATIONS REGARDING ONLINE PROFILING

<table>
<thead>
<tr>
<th>Principle</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>Complete transparency to user by providing disclosure and choice options on the host Web site.</td>
</tr>
<tr>
<td>Choice</td>
<td>“Robust” notice for PI (time/place of collection; before collection begins). Clear and conspicuous notice for non-PI. Opt-in for PI; opt-out for non-PI.</td>
</tr>
<tr>
<td>Access</td>
<td>No conversion of non-PI to PI without consent. Opt-out from any and all network advertisers from a single page provided by the host Web site.</td>
</tr>
<tr>
<td>Security</td>
<td>Reasonable provisions to allow inspection and correction.</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Reasonable efforts to secure information from loss, misuse, or improper access.</td>
</tr>
<tr>
<td>Restricted collection</td>
<td>Done by independent third parties, such as seal programs and accounting firms.</td>
</tr>
</tbody>
</table>

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
Federal Privacy Law

Health Service Providers
From 21 December 2006, the private sector amendments to the Privacy Act 1988 (Cth) (the Act), will be in force. The Act includes provisions for the Health Service Providers (HSPs) in sections 70 and 71. This means that the HSPs will be subject to the Act. The Act will apply to individuals who are health service providers, for example, doctors. The Act also applies to health service providers who are not HSPs, for example, hospitals. The Act is designed to ensure that health service providers are able to provide quality health services to the public.

Private Sector Business
From 21 December 2006, the private sector amendments to the Privacy Act 1988 (Cth) will be in force. The Act includes provisions for the Private Sector Business (PSB) in sections 70 and 71. This means that the PSB will be subject to the Act. The Act will apply to individuals who are private sector businesses, for example, businesses that provide goods and services to the public. The Act also applies to private sector businesses who are not PSB, for example, companies. The Act is designed to ensure that private sector businesses are able to provide quality goods and services to the public.

Information Privacy Principles under the Privacy Act 1988

- Principle 1: Manner and purpose of collection of personal information
- Principle 2: Solicitation of personal information from individual concerned
- Principle 3: Solicitation of personal information generally
- Principle 4: Storage and security of personal information
- Principle 5: Information relating to records held by record-keeper
- Principle 6: Access to records containing personal information
- Principle 7: Alteration of records containing personal information
- Principle 8: Record-keeper to check accuracy etc of personal information
- Principle 9: Personal information to be used only for relevant purposes
- Principle 10: Limits on use of personal information
- Principle 11: Limits on disclosure of personal information

Commonwealth and ACT Government Agencies

National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act 2000)

- Principle 1: Collection
- Principle 2: Use and disclosure
- Principle 3: Data quality
- Principle 4: Data security
- Principle 5: Anonymity
- Principle 6: Access to records
- Principle 7: Identifiers
- Principle 8: Health sector
- Principle 9: Data destruction
- Principle 10: Sensitive information

The National Privacy Principles in the Privacy Amendment (Private Sector) Act 2000: PDF, Word 2
Insight on Business: Chief Privacy Officers

- 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 Billey 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


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

- 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?
all e-mail systems have these problems

- Anyone can read company email. Email can be read by the company.
- Documents can be intercepted on the way to the sender's storage. The data can be altered. Your email may have been altered before the day of the week.
- The documents are in use.

SafeMosaic® is the leading secure communications system, eliminating concerns about confidentiality and data sensitivity.

SafeMosaic® provides total privacy by presenting the digital signature of the encrypted message. The sender can set policies for the recipient to use the personal data, even if the data is lost or damaged.

DiskVac

DiskVac is a simple, easy-to-use utility that securely removes the free-space of files. It is accomplished through multiple fragmentation of blocks on random ARDS to prevent data retrieval.

Our Review:

DiskVac is a simple, easy-to-use utility that securely removes the free-space of files. It is accomplished through multiple fragmentation of blocks on random ARDS to prevent data retrieval.

Download Software: 
Windows 9x/Me/NT/2000/XP
Free Software: Yes
Trial Version: Yes
Support: Support is not available. If you have any questions, feel free to contact the developer at support@diskvac.com.

If you wish to register and receive the full version of this software, visit the DiskVac product website.
Intellectual Property Rights

- 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

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

Patents: Business Methods and Processes

- 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

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
Trademarks: Online Infringement and Dilution

- **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

Types of Trademark Abuse on Internet

- **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

The Australian Guidelines for Electronic Commerce

- On 17 March 2006, the Treasury in consultation with the Commonwealth Consumer Affairs Advisory Council (CCAAC) released the **Australian Guidelines for Electronic Commerce (Guidelines)**.
  - The objective of the Guidelines is to enhance consumer confidence by providing guidance to businesses engaged in business-to-consumer (B2C) electronic commerce. The Guidelines replace the **Australian E-commerce Best Practice Model** which was released in 2000.

The Australian Guidelines for Electronic Commerce

- While the Guidelines are mainly targeted at Australian traders dealing in B2C electronic commerce, international businesses are also encouraged to utilise the Guidelines, and they can be equally applied when engaging in business-to-business (B2B) electronic commerce.

when engaging in B2C electronic commerce, businesses should:

- adopt fair business practices
- ensure that specialised software or hardware is not required for the electronic delivery of goods and services unless the requirement is made clear beforehand
- make reasonable adjustment in the provision of goods and services to ensure that they can be accessed by people with a disability
- ensure that advertising material is clearly identifiable and distinguishable from other content
when engaging in B2C electronic commerce, businesses should:

- take special care in advertising that is aimed at children
- provide consumers with accurate and accessible information that allows the business involved to be identified
- provide sufficient information setting out the terms, conditions and costs of a transaction, including a prominently displayed total minimum price for the product or service on offer

when engaging in B2C electronic commerce, businesses should:

- give consumers the opportunity to advise them of the purpose for which they are entering the transaction
- respect the privacy of consumers and as a minimum ensure compliance with the National Privacy Principles contained in Schedule 3 to the Privacy Act 1988
- provide reliable, useable and secure payment mechanisms

when engaging in B2C electronic commerce, businesses should:

- inform the consumer about any security and authentication mechanisms that are used
- establish internal complaint handling mechanisms
- provide information on any external dispute resolution systems that are available.
- For a copy of the Guidelines see the Australian Government Treasury website

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)

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
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

Taxation
• 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)

Public Safety and Welfare
• Efforts to control gambling and restrict sales of drugs and cigarettes
  ▪ Currently mostly regulated by state law

Insight on Society: The Internet Drug Bazaar
• 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?