9. Ethical, Social, and Political Issues in eCommerce

Alexander Nikov

Outline
1. Understanding Ethical, Social, and Political Issues in eCommerce
2. Privacy and Information Rights
3. Intellectual Property Rights
4. Governance
5. Public Safety and Welfare

Teaching Objectives
• Explain why e-commerce raises ethical, social, and political issues.
• Identify the main ethical, social, and political issues raised by e-commerce.
• Identify a process for analyzing ethical dilemmas.
• Explain basic concepts related to privacy.
• Identify the practices of e-commerce companies that threaten privacy.
• Describe the different methods used to protect online privacy.
• Explain the various forms of intellectual property and the challenges involved in protecting it.
• Explain how the governance of the Internet has evolved over time.
• Explain why taxation of e-commerce raises governance and jurisdiction issues.
• Identify major public safety and welfare issues raised by e-commerce

Discovering Law and Ethics in a Virtual World

Class Discussion
• Why is “mischief” in virtual worlds more difficult to stop? What constitutes mischief in Second Life?
• Which behaviors have been banned in Second Life?
• Is there a consensus regarding whether or not in-game gambling and other virtual crimes are also actual crimes? What is Second Life’s stance?
• How faithfully do you believe the law should be enforced in virtual worlds?
Outline

1. Understanding Ethical, Social, and Political Issues in eCommerce
2. Privacy and Information Rights
3. Intellectual Property Rights
4. Governance
5. Public Safety and Welfare

Understanding Ethical, Social, and Political Issues in eCommerce

- Internet, like other technologies, can:
  - Enable new crimes
  - Affect environment
  - Threaten social values

- Costs and benefits must be carefully considered, especially when there are 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:
  1. Information rights
  2. Property rights
  3. Governance
  4. Public safety and welfare
Basic Ethical Concepts

- Ethics
  - Study of principles used to determine right and wrong courses of action
- Responsibility
- Accountability
- Liability
  - Laws permitting individuals to recover damages
- Due process
  - Laws are known, understood
  - Ability to appeal to higher authorities to ensure laws applied correctly

Analyzing Ethical Dilemmas

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

Candidate Ethical Principles

- Golden Rule
- Universalism
- Slippery Slope
- Collective Utilitarian Principle
- Risk Aversion
- No Free Lunch
- The New York Times Test
- The Social Contract Rule
Outline

1. Understanding Ethical, Social, and Political Issues in eCommerce
2. Privacy and Information Rights
3. Intellectual Property Rights
4. Governance
5. Public Safety and Welfare

Privacy and Information Rights

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

Privacy and Information Rights

• 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 record keepers and individuals
Information Collected at eCommerce Sites

- Data collected includes
  - Personally identifiable information (PII)
  - Anonymous information
- Types of data collected
  - Name, address, phone, e-mail, social security
  - Bank and credit accounts, gender, age, occupation, education
  - Preference data, transaction data, clickstream data, browser type
Social Networks and Privacy

- Social networks
  - Encourage sharing personal details
  - Pose unique challenge to maintaining privacy
- Facebook’s facial recognition technology and tagging
- Personal control over personal information vs. organization’s desire to monetize social network

Mobile and Location-based Privacy Issues

- Smartphone apps
  - Funnel personal information to mobile advertisers for targeting ads
  - Track and store user locations
- 42% of users say privacy a concern
- Mobile Device Privacy Act
  - Not yet passed
  - Requires informing consumers about data collection

Profiling and Behavioral Targeting

- Profiling
  - Creation of digital images that characterize online individual and group behavior
  - Anonymous profiles
  - Personal profiles
- Advertising networks
  - Track consumer and browsing behavior on Web
  - Dynamically adjust what user sees on screen
  - Build and refresh profiles of consumers
- Google’s AdWord program

Profiling and Behavioral Targeting

- Deep packet inspection
- Business perspective:
  - Increases effectiveness of advertising, subsidizing free content
  - Enables sensing of demand for new products and services
- Critics’ perspective:
  - Undermines expectation of anonymity and privacy
  - Consumers show significant opposition to unregulated collection of personal information
Internet and Government Invasions of Privacy

- Various laws strengthen ability of law enforcement agencies to monitor Internet users without knowledge and sometimes without judicial oversight
  - CALEA, PATRIOT Act, Cyber Security Enhancement Act, Homeland Security Act
- Government agencies are largest users of private sector commercial data brokers
- Retention by ISPs of user data a concern

Legal Protections

- In the United States, explicitly granted or derived from
  - Constitution
    - First Amendment—guarantees freedom of speech and association
    - Fourth Amendment—protects against unreasonable search and seizure
    - Fourteenth Amendment—guarantees due process
  - Specific statutes and regulations (federal and state)
  - Common law

### TABLE 8.4 FEDERAL AND STATE PRIVACY LAWS

<table>
<thead>
<tr>
<th>NAME</th>
<th>DESCRIPTION</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>GENERAL FEDERAL PRIVACY LAWS</strong></td>
<td></td>
</tr>
<tr>
<td>Freedom of Information Act of 1966</td>
<td>Gives people the right to inspect information about themselves held in government files; also allows other individuals and organizations the right to request disclosure of government records based on the public's right to know.</td>
</tr>
<tr>
<td>Privacy Act of 1974, as amended</td>
<td>Regulates the federal government's collection, use, and disclosure of data collected by federal agencies. Gives individuals a right to inspect and correct records.</td>
</tr>
<tr>
<td>Electronic Communications Privacy Act of 1986</td>
<td>Regulates the federal government's collection, use, and disclosure of data collected by federal agencies.</td>
</tr>
<tr>
<td>Computer Matching and Privacy Protection Act of 1988</td>
<td>Regulates computerized matching of files held by different government agencies.</td>
</tr>
<tr>
<td>Driver's Privacy Protection Act of 1994</td>
<td>Limits access to personal information maintained by state motor vehicle departments to those with legitimate business purposes. Also gives drivers the option to prevent disclosure of driver's license information to marketers and the general public.</td>
</tr>
<tr>
<td>E-Government Act of 2002</td>
<td>Regulates the collection and use of personal information by federal agencies.</td>
</tr>
<tr>
<td><strong>FEDERAL PRIVACY LAWS AFFECTING PRIVATE INSTITUTIONS</strong></td>
<td></td>
</tr>
<tr>
<td>Fair Credit Reporting Act of 1970</td>
<td>Regulates the credit investigating and reporting industry. Gives people the right to inspect credit records if they have been denied credit and provides procedures for correcting information.</td>
</tr>
<tr>
<td>Family Educational Rights and Privacy Act of 1974</td>
<td>Requires schools and colleges to give students and their parents access to school records and to allow them to challenge and correct information; limits disclosure of such records to third parties.</td>
</tr>
<tr>
<td>Right to Financial Privacy Act of 1978</td>
<td>Regulates the financial industry's use of personal financial records; establishes procedures that federal agencies must follow to gain access to such records.</td>
</tr>
<tr>
<td>Privacy Protection Act of 1980</td>
<td>Prohibits government agents from conducting announced searches of press offices and files if no one in the office is suspected of committing a crime.</td>
</tr>
<tr>
<td>Cable Communications Policy Act of 1984</td>
<td>Regulates the cable industry's collection and disclosure of information concerning subscribers.</td>
</tr>
<tr>
<td>Video Privacy Protection Act of 1988</td>
<td>Prevents disclosure of a person's video rental records without court order or consent.</td>
</tr>
<tr>
<td>Child Online Privacy Protection Act (1998)</td>
<td>Prohibits deceptive practices in connection with the collection, use, and/or disclosure of personal information from and about children on the Internet.</td>
</tr>
<tr>
<td>Financial Modernization Act (Gramm-Leach-Bliley Act (1999)</td>
<td>Requires financial institutions to inform consumers of their privacy policies and permits consumers some control over their records.</td>
</tr>
<tr>
<td>Health Insurance Portability and Accountability Act of 1996 (HIPAA)</td>
<td>Requires health care providers and insurers and other third parties to promulgate privacy policies to consumers and establishes due process procedures.</td>
</tr>
</tbody>
</table>
Informed Consent

- U.S. firms can gather and redistribute transaction information without individual's informed consent
  - Illegal in Europe
- Informed consent:
  - 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

The FTC’s Evolving Privacy Approach

- Fair Information Practice principles (1998)
  - Notice
  - Choice
  - Access
  - Security
  - Enforcement
  - Restricted collection
- New privacy framework (2010)
  - Privacy by design
  - Simplified choice
  - Greater transparency

FTC’s Fair Information Practice Principles

<table>
<thead>
<tr>
<th><strong>Notice/Awareness</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Sites must disclose 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</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Choice/Consent</strong></th>
</tr>
</thead>
<tbody>
<tr>
<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-in/Opt-out must be available.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Access/Participation</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Consumers should be able to review and contest the accuracy and completeness of data collected about them in a timely, inexpensive process.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Security</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Data collectors must take reasonable steps to assure that consumer information is accurate and secure from unauthorized use.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Enforcement</strong></th>
</tr>
</thead>
<tbody>
<tr>
<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>

FTC Recommendations: Online Profiling

<table>
<thead>
<tr>
<th>Principle</th>
<th>Recommendation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Notice</td>
<td>Complete transparency to user by providing disclosure and choice options on the host Web site. &quot;Robust&quot; notice for PII (time/place of collection; before collection begins). Clear and conspicuous notice for non-PII.</td>
</tr>
<tr>
<td>Choice</td>
<td>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.</td>
</tr>
<tr>
<td>Access</td>
<td>Reasonable provisions to allow inspection and correction.</td>
</tr>
<tr>
<td>Security</td>
<td>Reasonable efforts to secure information from loss, misuse, or improper access.</td>
</tr>
<tr>
<td>Enforcement</td>
<td>Done by independent third parties, such as seal programs and accounting firms.</td>
</tr>
<tr>
<td>Restricted Collection</td>
<td>Advertising networks will not collect information about sensitive financial or medical topics, sexual behavior or sexual orientation, or use Social Security numbers for profiling.</td>
</tr>
</tbody>
</table>

The European Directive on Data Protection

- Privacy protection much stronger in Europe than the United States
- European approach:
  - Comprehensive and regulatory in nature
  - 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 programs:
  - Private, self-regulating policy and enforcement mechanism that meets objectives of government regulations and legislation, but does not involve government regulation or enforcement
  - E.g., privacy seal programs (TRUSTe, BBB Reliability Seal)
- Industry associations include:
  - Online Privacy Alliance (OPA)
  - Network Advertising Initiative (NAI)
    - CLEAR Ad Notice Technical Specifications
- Privacy advocacy groups
  - E.g., Epic.org
- Emerging privacy protection business

Technological Solutions

- Spyware
- Pop-up blockers
- Secure e-mail
- Anonymous remailers, surfing
- Cookie managers
- Disk/file erasing programs
- Policy generators
- Public key encryption
- Privacy Policy Reader/Platform for Privacy Preferences (P3P):
  - Comprehensive technological privacy protection standard
  - Works through user’s Web browser
  - Communicates a Web site’s privacy policy
  - Compares site policy to user’s preferences or to other standards such as FTC’s FIP guidelines or EU’s Data Protection Directive
**TABLE 8.7 PRIVACY ADVOCACY GROUPS**

<table>
<thead>
<tr>
<th>ADVOCACY GROUP</th>
<th>FOCUS</th>
</tr>
</thead>
<tbody>
<tr>
<td>Epic.org (Electronic Privacy Information Center)</td>
<td>Washington-based watch-dog group Tracks international privacy developments</td>
</tr>
<tr>
<td>PrivacyInternational.org</td>
<td>Foundation- and business-supported group with a legislative focus Clearinghouse sponsored by EPIC and Privacy International</td>
</tr>
<tr>
<td>Cdt.org (Center for Democracy and Technology)</td>
<td>Educational clearinghouse Industry-supported clearinghouse</td>
</tr>
<tr>
<td>Privacy.org</td>
<td></td>
</tr>
<tr>
<td>Privacyrights.org</td>
<td></td>
</tr>
<tr>
<td>Privacyalliance.org</td>
<td></td>
</tr>
</tbody>
</table>


---

**TABLE 8.8 TECHNOLOGICAL PROTECTIONS FOR ONLINE PRIVACY**

<table>
<thead>
<tr>
<th>TECHNOLOGY</th>
<th>PRODUCTS</th>
<th>PROTECTION</th>
</tr>
</thead>
<tbody>
<tr>
<td>Spyware blockers</td>
<td>Spyware Doctor, ZoneAlarm, Ad-Aware and Spybot—Search &amp; Destroy (Spybot-S&amp;D) (freeware)</td>
<td>Detects and removes spyware and adware, keyloggers, and other malware</td>
</tr>
<tr>
<td>Pop-up blockers</td>
<td>Browsers: Firefox, Internet Explorer 6.0 SP2 and 7, Safari, Opera; Others: Google, Yahoo, MSN, Add-ons (STOpzilla, AdBlock, No Ads)</td>
<td>Prevents calls to ad servers that push pop-up, pop-under, and leave-behind ads, restricts downloading of images at user request</td>
</tr>
<tr>
<td>Secure e-mail</td>
<td>ZT, Technologies: SafeMessage.com, Hotmail.com, Pretty Good Privacy (PGP)</td>
<td>E-mail and document encryption</td>
</tr>
<tr>
<td>Anonymous remailers</td>
<td>W3-Anonymous Remailer, Jack B. Ymble, Java-Anonymous Proxy</td>
<td>Send e-mail without trace</td>
</tr>
<tr>
<td>Anonymous surfing</td>
<td>Freedom Web Secure, Anonymous4.com, Tor, GreeneMail</td>
<td>Surf without a trace</td>
</tr>
<tr>
<td>Cookie managers</td>
<td>CookieCrasher, and most browsers</td>
<td>Prevents client computer from accepting cookies</td>
</tr>
<tr>
<td>Disk/file erasing programs</td>
<td>Multitask File Wiper, Eraser, DiskSecure 2.0</td>
<td>Completely erases hard drive and floppy files</td>
</tr>
<tr>
<td>Policy generators</td>
<td>OECD Privacy Policy Generator</td>
<td>Automates the development of an OECD privacy compliance policy</td>
</tr>
<tr>
<td>Privacy Policy Reader</td>
<td>P3P</td>
<td>Software for automating the communication of privacy policies to users</td>
</tr>
<tr>
<td>Public Key Encryption</td>
<td>PGP Desktop</td>
<td>Program that encrypts your mail and documents</td>
</tr>
</tbody>
</table>

---

**Internet Explorer 11 and Google Chrome Implementation of P3P**

**How P3P Works**

1. http GET request P3P policy files
2. send P3P policy files
3. http GET request Web page
4. send Web page
5. display page and policy to user

A simple http transaction with P3P added

Figure 8.2(A), Page 522 SOURCE: W3C Platform for Privacy Preferences Initiative, 2003.
Outline

1. Understanding Ethical, Social, and Political Issues in eCommerce
2. Privacy and Information Rights
3. Intellectual Property Rights
4. Governance
5. Public Safety and Welfare

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:
  - How can Internet and e-commerce be regulated or governed to protect intellectual property?

Intellectual Property Protection

- Three main types of protection:
  1. Copyright
  2. Patent
  3. Trademark law
- Goal of intellectual property law:
  - Balance two competing interests—public and private
- Maintaining this balance of interests is always challenged by the invention of new technologies

Copyright

- 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
- Fair use doctrine
- Digital Millennium Copyright Act, 1998
  - First major effort to adjust copyright laws to Internet age
  - Implements WIPO treaty that makes it illegal to make, distribute, or use devices that circumvent technology-based protections of copyrighted materials
### Patents

- Grant owner 20-year monopoly on ideas behind an invention
  - Machines
  - Man-made products
  - Compositions of matter
  - Processing methods
- Invention must be new, non-obvious, novel
- Encourages inventors
- Promotes dissemination of new techniques through licensing
- Stifles competition by raising barriers to entry

### eCommerce Patents

- 1998 State Street Bank & Trust vs. Signature Financial Group
  - Business method patents
- Most European patent laws do not recognize business methods unless based on technology
- Examples
  - Amazon’s one-click purchasing
  - DoubleClick’s dynamic delivery of online advertising

### Table 8.9: Fair Use Considerations to Copyright Protections

<table>
<thead>
<tr>
<th>Fair Use Factor</th>
<th>Interpretation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Character of use</td>
<td>Nonprofit or educational use versus for-profit use.</td>
</tr>
<tr>
<td>Nature of the work</td>
<td>Creative works such as plays or novels receive greater protection than factual accounts, e.g., newspaper accounts.</td>
</tr>
<tr>
<td>Amount of work used</td>
<td>A stanza from a poem or a single page from a book would be allowed, but not the entire poem or a book chapter.</td>
</tr>
<tr>
<td>Market effect of use</td>
<td>Will the use harm the marketability of the original product? Has it already harmed the product in the marketplace?</td>
</tr>
<tr>
<td>Context of use</td>
<td>A last-minute, unplanned use in a classroom versus a planned infringement.</td>
</tr>
</tbody>
</table>

### Table 8.10: The Digital Millennium Copyright Act

<table>
<thead>
<tr>
<th>Section</th>
<th>Importance</th>
</tr>
</thead>
<tbody>
<tr>
<td>Title I, WIPO Copyright and Performances and Phonograms Treaties Implementation</td>
<td>Makes it illegal to circumvent technological measures to protect works for either access or copying or to circumvent any electronic rights management information.</td>
</tr>
<tr>
<td>Title II, Online Copyright Infringement Liability Limitation</td>
<td>Requires ISPs to “take down” sites they host if they are infringing copyrights, and requires search engines to block access to infringing sites. Limits liability of ISPs and search engines.</td>
</tr>
<tr>
<td>Title III, Computer Maintenance Competition Assurance</td>
<td>Permits users to make a copy of a computer program for maintenance or repair of the computer.</td>
</tr>
<tr>
<td>Title IV, Miscellaneous Provisions</td>
<td>Requires the copyright office to report to Congress on the use of copyright materials for distance education; allows libraries to make digital copies of works for internal use only; extends musical copyrights to include “webcasting.”</td>
</tr>
</tbody>
</table>

Trademarks

- Identify, distinguish goods, and indicate their source
  - Purpose
    - Ensure consumer gets what is paid for/expected to receive
    - Protect owner against piracy and misappropriation
- Infringement
  - Market confusion
  - Bad faith
- Dilution
  - Behavior that weakens connection between trademark and product

TABLE 8.11  SELECTED E-COMMERCE PATENTS

<table>
<thead>
<tr>
<th>COMPANY</th>
<th>SUBJECT</th>
<th>UPDATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Akamai</td>
<td>Internet content delivery</td>
<td>A broad patent granted in 2006 covering techniques for expediting the flow of information over the Internet. Akamai sued Digital Island (subsequently acquired by Cable &amp; Wireless) for violating the patent. In 2007, a jury found in favor of Akamai. In 2008, the district court ruled in favor of Akamai and awarded $1 billion in damages. Akamai sued in July 2009. Akamai did not settle the suit.</td>
</tr>
<tr>
<td>DoubleClick</td>
<td>Dynamic delivery of online advertising</td>
<td>Originally granted in 2000, DoubleClick sued competitors 24/7 Real Media and IBC for violating the patent. DoubleClick and Google settled in 2008. The lawsuit was dismissed in 2009.</td>
</tr>
<tr>
<td>Overture</td>
<td>Pay for performance search</td>
<td>System and method for determining a price for a network transaction based on information obtained from the search request. Overture was acquired by Google in 2007. Google settled the lawsuit in 2008.</td>
</tr>
<tr>
<td>Coovert Digital</td>
<td>Purchase technology</td>
<td>Patent for a system and method for processing transactions over the Internet. Coovert Digital was acquired by Cato in 2008. Cato filed suit against Amazon.com for patent infringement in 2007. The case was settled in 2009.</td>
</tr>
<tr>
<td>MercExchange</td>
<td>Auction technology</td>
<td>Patent for online auctions and database search. Originally granted in 1995. eBay ordered to pay $25 million to MercExchange in 2003 for infringements. In 2007, the U.S. district court denied a motion for reversed patent invalidation against eBay using the &quot;Bayh-Dole&quot; methods, and moved to the final stage of allowing the damages owed to be paid. The case was settled in 2009.</td>
</tr>
<tr>
<td>Google</td>
<td>Search technology</td>
<td>Patent for a system and method for processing transactions over the Internet. Google's PageRank patent was filed in 1998 and granted in 2005.</td>
</tr>
</tbody>
</table>
Trademarks and the Internet

- Cybersquatting
  - Anticybersquatting Consumer Protection Act (ACPA)
-Cyberpiracy
  - Typosquatting
- Metatagging
- Keywording
- Deep linking
- Framing

Outline

1. Understanding Ethical, Social, and Political Issues in eCommerce
2. Privacy and Information Rights
3. Intellectual Property Rights
4. Governance
5. Public Safety and Welfare

Governance

- Primary questions
  - Who will control Internet and e-commerce?
  - What elements will be controlled and how?
- Stages of governance and e-commerce
Who Governs eCommerce and the Internet?

- Currently: mixed mode policy environment
  - Self-regulation, through variety of Internet policy and technical bodies, co-exists with limited government regulation
- ICANN in charge of Domain Name System
- Internet can be very easily controlled, monitored, and regulated from a central location (e.g., China, Singapore, etc.)

### Taxation

- E-commerce taxation illustrates complexity of governance and jurisdiction issues
- U.S. sales taxed by states and local government
- MOTO retailing
- E-commerce benefits from tax “subsidy”
- October 2007: Congress extends tax moratorium for an additional seven years
- Unlikely that comprehensive, integrated rational approach to taxation issue will be determined for some time to come

### Net Neutrality

- Neutrality: All Internet traffic treated equally—all activities charged the same rate, no preferential assignment of bandwidth
- Backbone providers vs. content providers
- December 2010 FCC approved “compromise” net neutrality rules
- Telecom providers adopting compromise position between wired and mobile wireless access
Outline

1. Understanding Ethical, Social, and Political Issues in eCommerce
2. Privacy and Information Rights
3. Intellectual Property Rights
4. Governance

5. Public Safety and Welfare

Public Safety and Welfare

• Protection of children and strong sentiments against pornography
  – Passing legislation that will survive court challenges has proved difficult
• Efforts to control gambling and restrict sales of drugs and cigarettes
  – Currently mostly regulated by state law
  – Unlawful Internet Gambling Enforcement Act