CHAPTER

Ethical and Social Issues in Information Systems

Module 3

Ethical and Social Issues in Information Systems

- Ethical issues and Privacy,
- Information Security.
- Threat to IS, and Security Controls

Ethics and Privacy

Ethics

- Ethics refers to principles of right and wrong that individuals use to make choices that guide their behaviour.
- Deciding right or wrong is not always easy or clear cut .
- There are many frameworks that can help us make ethical decisions.

Main Categories of Threats in Information Systems

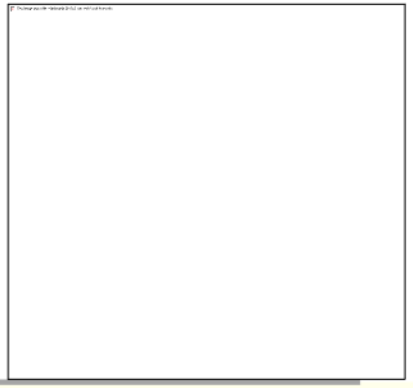
- **Human-Related Threats**
  - **Insider threats** – Employees or contractors misusing access (e.g., stealing data).
  - **Social engineering** – Manipulating people into revealing confidential information (phishing, pretexting).
  - **Human error** – Mistakes like sending sensitive files to the wrong person or misconfiguring security settings.

- **Technical / Cyber Threats**
  - **Malware** – Viruses, worms, Trojans, ransomware, spyware.
  - **Hacking** – Unauthorized access to systems to steal, alter, or destroy data.
  - **Denial-of-Service (DoS/DDoS) attacks** – Overloading systems to make them unavailable.
  - **Data breaches** – Unauthorized exfiltration of sensitive data.
  - **Zero-day exploits** – Attacks exploiting unknown vulnerabilities.

- **Physical Threats**
  - **Theft of hardware** – Laptops, servers, or storage devices stolen.
  - **Vandalism** – Damage to physical IT infrastructure.
  - **Natural disasters** – Fires, floods, earthquakes damaging systems.
  - **Power outages** – Interrupting operations and potentially causing data loss.

- **Environmental & Operational Threats**
  - **System failures** – Hardware or software breakdowns.
  - **Network failures** – Loss of connectivity disrupting services.
  - **Supply chain attacks** – Compromises introduced through third-party vendors.
- **Emerging Threats**
  - **Cloud security risks** – Misconfigured cloud storage, insecure APIs.
  - **IoT vulnerabilities** – Smart devices with weak security.
  - **AI-powered attacks** – Automated phishing, deepfake-based scams.

Ethical Issues



- Ethical Frameworks
- Ethics in the Corporate Environment
- Ethics and Information Technology

Ethical Frameworks

- Ethical frameworks in information systems provide a structured approach to understanding and addressing the moral issues that arise in the design, implementation, and use of information technologies.
- These frameworks help professionals navigate the complexities of ethical decision-making in a field where technology often outpaces regulation and societal norms.

Ethical Frameworks:

Below are some key ethical frameworks commonly applied in information systems:

- **Utilitarian Approach:** states that an ethical action is the one that provides the most good or does the least harm.

Utilitarian Approach (Most good / least harm)

- **Example:** A government decides to implement a vaccination program. Even if a few individuals may experience side effects, the overall benefit of preventing widespread disease and saving thousands of lives makes it ethically justifiable.
- **Business Example:** A company recalls a defective product to prevent harm to thousands of customers, even though it will lose millions of dollars in the short term.

- **Rights Approach:** maintains that an ethical action is the one that best protects and respects the moral rights of the affected parties.

Rights Approach (Protects moral rights)

- **Example:** A journalist refuses to reveal a confidential source, even under government pressure, because doing so would violate the source's right to privacy and protection.

Business Example:

- **Workplace:** An employee is allowed to refuse unsafe work, respecting their right to safety, even if it delays production.
- **Consumer Protection:** A bank keeps customer data private, even if selling it would generate profit, because clients have a right to confidentiality

Fairness Approach: posits that ethical actions treat all human beings equally, or, if unequally, then fairly, based on some defensible standard.

Fairness Approach (Equality and fairness)

- **Example:** A teacher gives all students equal access to learning resources and grades assignments based only on merit, not favoritism.
- **Business Example:** A company ensures that men and women receive equal pay for the same work, addressing unfair wage gaps.

- **Common Good Approach:** highlights the interlocking relationships that underlie all societies. This approach argues that respect and compassion for all others is the basis for ethical actions.

Common Good Approach (Community well-being)

- **Example:** A city invests in public parks, libraries, and clean water systems, even though not everyone may directly use them, because they improve the quality of life for the whole community.
- **Business Example:** A tech company creates open-source software to benefit developers worldwide, strengthening the broader digital community.

Utilitarian Approach

Principle: This framework focuses on the consequences of actions, aiming to maximize overall happiness or utility. Decisions are considered ethical if they result in the greatest good for the greatest number of people.

Application in Information Systems: When designing a system, a utilitarian approach would weigh the benefits and harms to all stakeholders. For example, implementing a data tracking system might be justified if it significantly improves user experience or security, even if it slightly compromises individual privacy.

Rights Approach:

Principle: This framework is centered on the protection and respect for individual rights. Actions are ethical if they uphold the fundamental rights of individuals, such as the right to privacy, freedom of expression, and ownership of personal data.

Application in Information Systems: A rights-based approach would argue against practices like unauthorized data collection or censorship, as these violate the rights of individuals. Information systems should be designed to protect user rights and ensure that they are not infringed upon.

Fairness Approach:

- The Fairness Approach is an ethical framework that emphasizes treating all people equally and fairly. It is rooted in the principle that ethical actions should promote fair treatment and justice for all individuals, ensuring that no one is unfairly advantaged or disadvantaged.

Key Principles of the Fairness Approach:

- **Equality**: Every individual should be treated equally, with no discrimination based on arbitrary factors such as race, gender, socioeconomic status, or other personal characteristics.
- **Impartiality**: Decisions should be made impartially, without bias or favoritism, ensuring that everyone is given a fair chance.
- **Justice**: The Fairness Approach seeks to ensure that benefits and burdens are distributed justly, meaning that no group or individual should bear an unfair share of the negative consequences of a decision.

Fairness Approach: cont..
Application in Information Systems

- **Algorithmic Fairness**: When developing algorithms, especially those used in decision-making processes like hiring, credit scoring, or law enforcement, the Fairness Approach would require that these algorithms do not perpetuate or exacerbate existing biases. For example, an algorithm used in hiring should not favor candidates of a particular gender or ethnicity unless such criteria are legally required.

- **Access to Technology**: The Fairness Approach would also advocate for equal access to technology. This means addressing the digital divide, where some individuals or communities have less access to technology and information resources than others. Efforts should be made to ensure that all groups have equitable access to the benefits of information systems.

Fairness Approach: cont..
Application in Information Systems

- **Data Privacy and Protection**: Fairness in handling user data is another critical aspect. Organizations should ensure that data collection and usage policies do not disproportionately affect certain groups. For instance, privacy settings and data protection mechanisms should be equally robust for all users.
- **Transparency in Decision-Making**: Fairness also demands transparency in how decisions are made within information systems. Users should be informed about how their data is used and how decisions affecting them are made, ensuring that they have the ability to contest or appeal decisions that they believe to be unfair.

Common Good Approach

- The Common Good Approach is an ethical framework that emphasizes the importance of actions and policies that contribute to the welfare of the community as a whole.
- It is rooted in the belief that society should work together to achieve shared benefits and ensure that the needs of all its members are met.
- This approach prioritizes the well-being of the collective over individual interests, aiming to create systems that enhance the common good.

Key Principles of the Common Good Approach:

- **Community Welfare**: The focus is on promoting the well-being of the community or society as a whole. This includes considering how decisions affect public health, safety, security, and overall quality of life.

- **Interdependence**: Recognizes that individuals are part of a larger social fabric, where the actions of one person or group can significantly impact others. Therefore, ethical decisions should consider the broader implications for society.

- **Shared Responsibility**: Encourages individuals and organizations to take responsibility for contributing to the common good, whether through ethical business practices, public policies, or community engagement.

Common Good Approach

Application in Information Systems:

- **Public Health and Safety**: Information systems can be designed to support public health initiatives, such as tracking the spread of diseases or managing emergency responses. For example, a health information system that aggregates data to identify and respond to outbreaks benefits the entire community by protecting public health.
- **Sustainable Development**: Information systems can play a crucial role in promoting sustainable practices that benefit society. For instance, developing systems that optimize energy use or reduce waste can contribute to environmental sustainability, which is a key aspect of the common good.
- **Access to Information**: Ensuring that all members of society have access to accurate and relevant information is crucial for the common good. This includes developing systems that make educational resources, government services, and public information widely accessible, regardless of socioeconomic status.
- **Digital Inclusion**: The Common Good Approach would advocate for efforts to close the digital divide, ensuring that underserved communities have access to the internet, technology, and digital literacy training. This promotes social equity and ensures that all members of society can participate fully in the digital economy.

Five Steps of the General Ethical Framework

1. Recognize the Issue
2. Get the Facts
3. Evaluate Alternative Actions
4. Make a Decision and Test It
5. Act and Reflect on the Outcome of Your Decision

Five Steps of the General Ethical Framework

1. **Recognize an ethical issue:**
   - Could this decision or situation damage someone or some group?
   - Does this decision involve a choice between a good and a bad alternative?
   - Does this issue involve more than simply legal considerations? If so, then in what way?
2. **Get the facts:**
   - What are the relevant facts of the situation?
   - Do I have sufficient information to make a decision?
   - Which individuals and/or groups have an important stake in the outcome?
   - Have I consulted all relevant persons and groups?

Five Steps of the General Ethical Framework

3. **Evaluate alternative actions:**
   - WhWhich option will produce the most good and do the least harm? (the utilitarian approach)
   - ich option best respects the rights of all stakeholders? (the rights approach)
   - Which option treats people equally or proportionately? (the fairness approach)
   - Which option best serves the community as a whole, and not just some members? (the common good approach)
4. **Make a decision and test it:**
   - Considering all the approaches, which option best addresses the situation?
5. **Act and reflect on the outcome of your decision:**
   - How can I implement my decision with the greatest care and attention to the concerns of all stakeholders?
   - How did my decision turn out, and what did I learn from this specific situation?

Ethics in the Corporate Environment

- Many companies and professional organizations develop their own codes of ethics.
- A **code of ethics** is a collection of principles intended to guide decision making by members of the organization.

Ethics in the Corporate Environment

- **Fundamental Tenets of Ethics:**
- **Responsibility:** means that you accept the consequences of your decisions and actions.
- **Accountability:** refers to determining who is responsible for actions that were taken.
- **Liability:** a legal concept that gives individuals the right to recover the damages done to them by other individuals, organizations, or systems.

Case Study 1: Algorithmic Bias in Hiring

Scenario:

- A large corporation implements an AI-powered recruitment system to streamline the hiring process.
- The system is trained on historical hiring data to screen resumes and rank candidates. However, after a year of using the system, the company notices that very few women and minority candidates are advancing to the interview stage.

Ethical Issue:

- The algorithm is perpetuating biases present in the historical data, leading to discriminatory outcomes in the hiring process. This raises ethical concerns regarding fairness, equality, and non-discrimination.

Case 1…

Analysis Using Ethical Frameworks:

- **Fairness Approach**: The hiring algorithm should be designed to treat all candidates equally, ensuring that the biases in historical data do not influence current decisions.
- **Justice and Fairness**: The company must address the unfair distribution of opportunities and ensure that the system promotes equal treatment regardless of gender or ethnicity.
- **Rights-based Ethics**: The right to equal employment opportunities is being violated by the biased algorithm, necessitating corrective action.

Case 1..

Solution:

The company should re-evaluate the AI system by:

- **Auditing the Algorithm**: Conducting an audit to identify and understand the sources of bias in the training data and algorithmic decisions.
- **Bias Mitigation**: Implementing techniques to reduce or eliminate biases, such as using more diverse training data and applying fairness constraints in the algorithm.
- **Human Oversight**: Incorporating human decision-makers in the recruitment process to review and validate the AI's recommendations, ensuring that no biased decisions are made.
- **Continuous Monitoring**: Establishing ongoing monitoring of the system to detect and address any new biases that may emerge over time

Case Study 3: Social Media Manipulation

Scenario:

- A social media platform is found to have algorithms that prioritize sensational and polarizing content because it drives higher engagement. This has led to the spread of misinformation and increased social division, with significant real-world consequences.

Ethical Issue:

- The platform's algorithms are contributing to the spread of harmful content and misinformation, raising ethical concerns about the platform's responsibility for the societal impact of its technology.

CASE 3...

Analysis Using Ethical Frameworks:

- **Utilitarianism**: The harm caused by the spread of misinformation and societal division outweighs the benefits of increased user engagement.
- **Virtue Ethics**: The platform's actions reflect a lack of moral responsibility, as it prioritizes profit over the well-being of its users and society.
- **Common Good Approach**: The platform has a responsibility to promote the common good by curbing the spread of misinformation and fostering a healthier public discourse.

CAS3E 3..

Solution:

- The social media platform should consider the following actions:
- **Algorithmic Adjustment**: Modify the algorithms to prioritize content that is informative and trustworthy, rather than simply sensational or polarizing.
- **Content Moderation**: Strengthen content moderation efforts to detect and remove misinformation, including partnerships with fact-checking organizations.
- **Transparency and Accountability**: Increase transparency about how algorithms work and involve external stakeholders in reviewing and auditing the platform's practices.
- **Promoting Digital Literacy**: Launch initiatives to educate users about identifying misinformation and understanding the impact of algorithms on content visibility.

Case Study 4: Ethical Use of Customer Data in E-commerce

Scenario:

- An e-commerce company uses customer data to personalize advertisements and product recommendations. However, the data is also being sold to third-party advertisers without explicit customer consent, leading to targeted ads that customers find invasive and manipulative.

Ethical Issue:

- The sale and use of customer data without consent raise significant privacy concerns and questions about the ethical use of personal information.

CASE 4...

Analysis Using Ethical Frameworks:

- **Rights-based Ethics**: Customers have a right to control their personal information, and the company's actions violate this right.
- **Ethics of Care**: The company should consider its responsibility to care for its customers by protecting their privacy and respecting their autonomy.

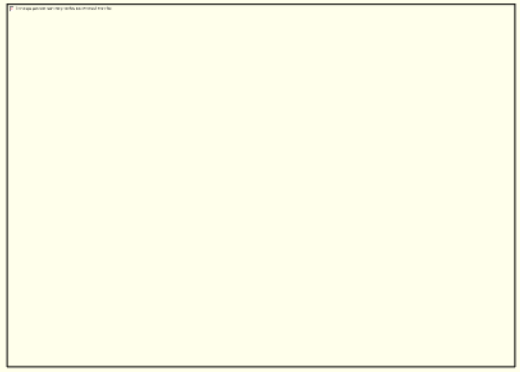
CASE 4..

Solution:

The e-commerce company should take the following steps:

- **Informed Consent**: Revise privacy policies to ensure that customers are fully informed about how their data will be used and explicitly consent to any data-sharing practices.
- **Opt-out Options**: Provide clear and easy-to-use options for customers to opt out of data sharing and targeted advertising.
- **Data Transparency**: Offer customers access to the data collected about them and explain how it is being used.
- **Ethical Data Practices**: Commit to ethical data practices by limiting data sharing to trusted partners and using data in ways that align with customer expectations and privacy rights.

IT'S ABOUT BUSINESS 6.1



- **Cheating Is Risky for Business Students**
  1. As the Turnitin database expands rapidly by incorporating a growing number of papers and essays, what will be the impact on subsequent papers submitted to it?
  2. Discuss the ethical implications of writing a paper yourself that you know contains some plagiarized material and then using Turnitin's service yourself.

Ethics and Information Technology

- **Privacy Issues:** involve collecting, storing, and disseminating information about individuals.
- **Accuracy Issues:** involve the authenticity, fidelity, and correctness of information that is collected and processed.
- **Property Issues:** involve the ownership and value of information.
- **Accessibility Issues:** revolve around who should have access to information and whether they should pay a fee for this access.

Privacy

- **Privacy:** the right to be left alone and to be free of unreasonable personal intrusions.
- **Information Privacy:** the right to determine when, and to what extent, information about you can be gathered and/or communicated to others.

Privacy

- Electronic Surveillance
- Personal Information in Databases
- Information on Internet Bulletin Boards, Newsgroups, and Social Networking Sites
- Privacy Codes and Policies
- International Aspects of Privacy

Privacy: Two Rules

- Court decisions in many countries have generally followed two rules
  - The right to privacy is not absolute, Privacy must be balanced against the needs of society.
  - The public's right to know supersedes the individual's right to privacy.

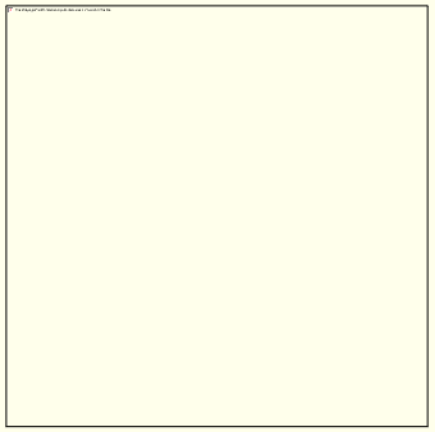
Electronic Surveillance

- Electronic surveillance is rapidly increasing
- Emerging Technologies increase monitoring of human activity
- Facial Recognition
- Geotagging
- Photo tagging

Electronic Surveillance

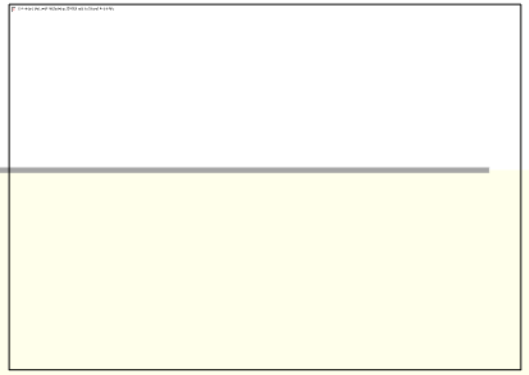
- **Electronic Surveillance:** conducted by employers, the government, and other institutions. Surveillance cameras track you at airports, subways, banks, and other public venues. Inexpensive digital sensors are now incorporated into laptop webcams, video-game motion sensors, smartphone cameras, utility meters, passports, employee ID cards high-resolution photographs taken from the air or from the street by Google or Microsoft , your license plates will be recorded and time-stamped as you drive down a city street, cross a toll bridge, or park at a shopping mall.

IT'S ABOUT BUSINESS 6.2



- **Those Mannequins Are Watching You**
  1. Is using EyeSee mannequins in stores an ethical practice? Why or why not? Support your answer.
  2. If stores notify people that they may be filmed, do the stores have to indicate how they might be filmed (i.e., by mannequins)? What are the ethical implications of how stores make these notifications?
  3. Would knowing that the mannequins may be watching you change your shopping behavior? Why or why not? Explain your answer.
  4. What are the privacy implications of the EyeSee mannequins, given that stores already have security cameras placed in strategic locations?

Personal Information in Databases



- Major Concerns:
  - Do you know where the records are?
  - Are the records accurate?
  - Can you change inaccurate data?
  - How long will it take to make a change?
  - Under what circumstances will the personal data be released?

Personal Information in Databases (continued)

- Major Concerns:
  - How are the data used?
  - To whom are the data given or sold?
  - How secure are the data against access by unauthorized people?

Information on Internet Bulletin Boards, Newsgroups, and Social Networking Sites

- Every day we see more and more **electronic bulletin boards, newsgroups, electronic discussions such as chat rooms, and social networking sites**. These sites appear on the Internet, within corporate intranets, and on blogs.
- **Blog (Web Log):** an informal, personal journal that is frequently updated and is intended for general public reading.
- How does society keep owners of bulletin boards from disseminating information that may be offensive to readers or simply untrue? This is a difficult problem because it involves the conflict between freedom of speech on the one hand and privacy on the other.
- **Conflict between freedom of speech and privacy than the Internet**. Many Web sites contain anonymous, insulting information on individuals, who typically have little recourse in the matter. The vast majority of the U.S. firms use the Internet in examining job applications, including searching on Google and on social networking sites

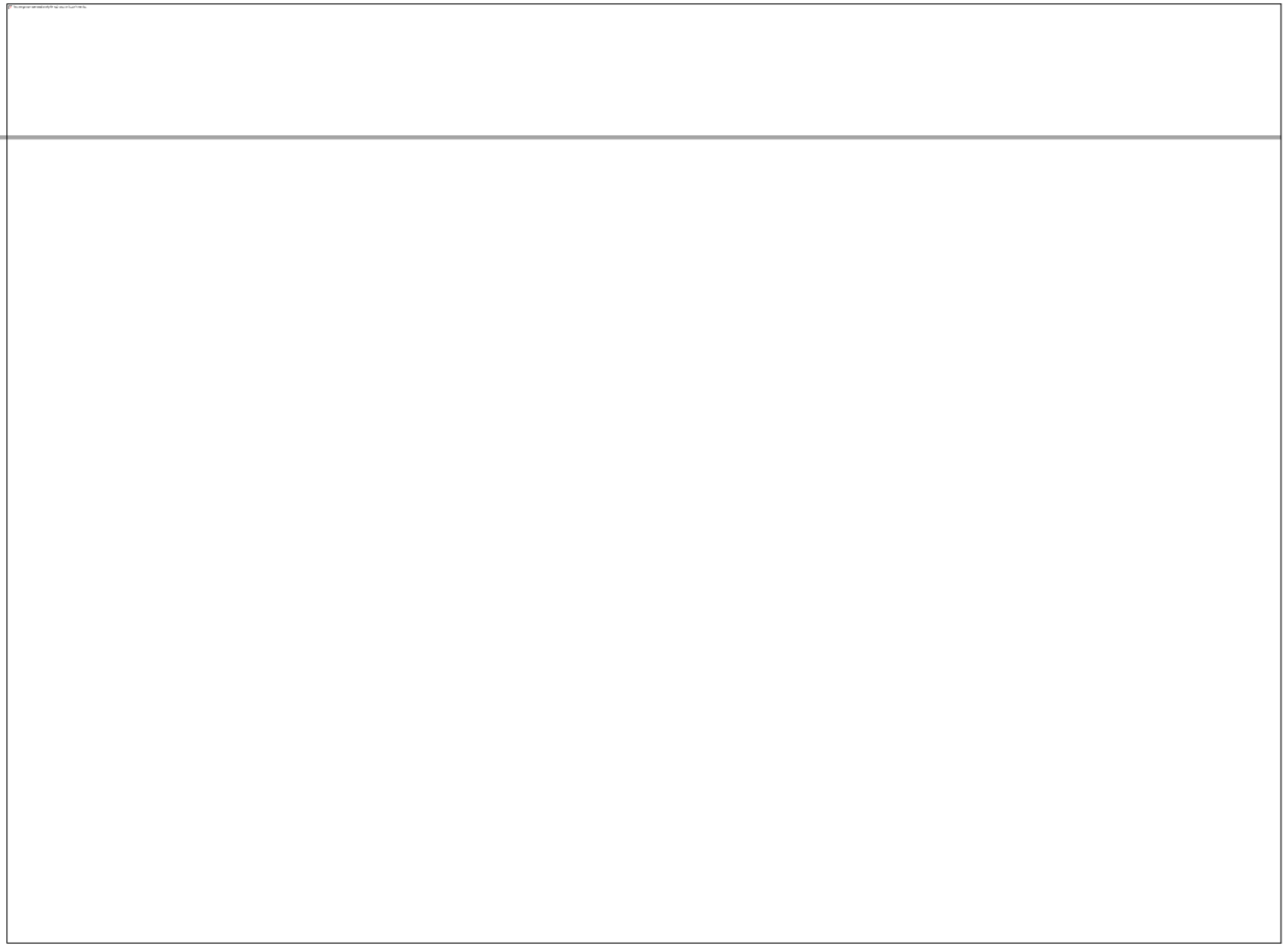
IT'S ABOUT BUSINESS 6.3

- **Google Glass: Big Brother Really Is Watching You**
  1. Apply the general framework for ethical decision making to Google Glass.
  2. Do you feel that the functionality offered by Google Glass outweighs the potential loss of privacy that the technology could create? Why or why not? Support your answer.
  3. Would you use Google Glasses? Why or why not? Support your answer.
  4. If you were at a party or at a bar, would you be comfortable speaking to someone who was wearing Google Glasses? Would you be comfortable just being in the room with someone wearing Google Glasses? Why or why not? Support your answer.

Privacy Codes and Policies

- **Privacy Policies (or Privacy Codes):** an organization's guidelines for protecting the privacy of its customers, clients, and employees.
- **Opt-Out Model of Informed Consent:** permits the company to collect personal information until the customer specifically requests that the data not be collected.
- **Opt-In Model of Informed Consent:** Privacy advocates prefer this model, which prohibits an organization from collecting any personal information unless the customer specifically authorizes it.
- **Platform for Privacy Preferences (P3P):** a protocol that automatically communicates privacy policies between an electronic commerce Web site and visitors to that site. P3P enables visitors to determine the types of personal data that can be extracted by the sites they visit.

Privacy Policy Guidelines: A Sampler



International Aspects of Privacy

- **Safe Harbor:** The U.S. Department of Commerce, in consultation with the European Union, developed a "safe harbor" framework to regulate the way that the U.S. companies export and handle the personal data (e.g., names and addresses) of European citizens.
- **The European Community Commission (ECC) (1998):** issued guidelines to all of its member countries regarding the rights of individuals to access information about themselves. The EU data protection laws are stricter than the U.S. laws and therefore could create problems for the U.S.-based multinational corporations, which could face lawsuits for privacy violations.

THE RELATIONSHIP AMONG ETHICAL, SOCIAL, POLITICAL ISSUES IN AN INFORMATION SOCIETY

The introduction of new information technology has a ripple effect, raising new ethical, social, and political issues that must be dealt with on the individual, social, and political levels. These issues have five moral dimensions: information rights and obligations, property rights and obligations, system quality, quality of life, and accountability and control.

Understanding Ethical and Social Issues Related to Systems

- Five moral dimensions of the information age:
  - Information rights and obligations
  - Property rights and obligations
  - Accountability and control
  - System quality
  - Quality of life

Understanding Ethical and Social Issues Related to Systems

- Key technology trends that raise ethical issues
  - Doubling of computer power
    - More organizations depend on computer systems for critical operations.
  - Rapidly declining data storage costs
    - Organizations can easily maintain detailed databases on individuals.
  - Networking advances and the Internet
    - Copying data from one location to another and accessing personal data from remote locations are much easier.

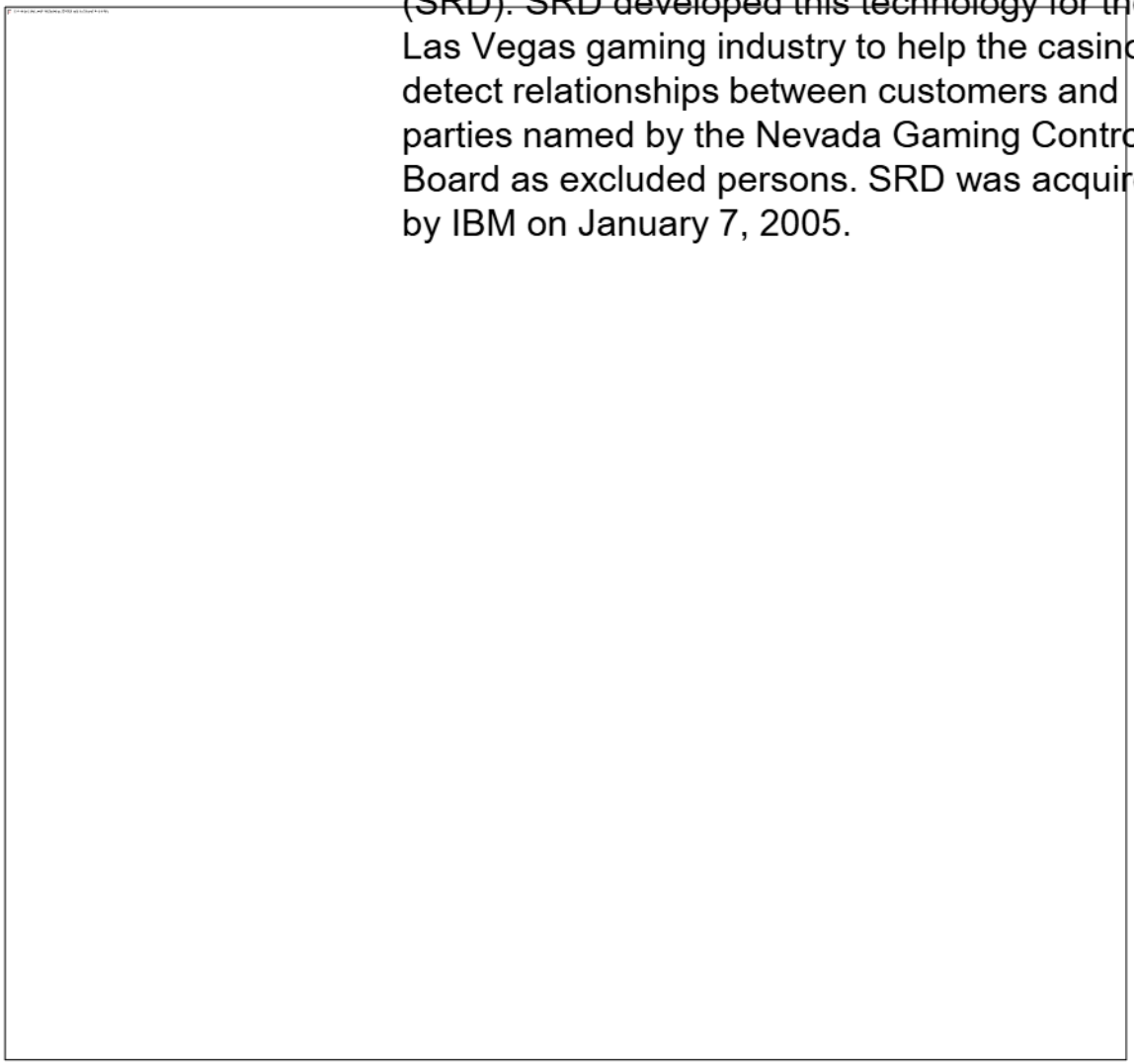
Understanding Ethical and Social Issues Related to Systems

- Advances in data analysis techniques
  - Profiling
    - Combining data from multiple sources to create records of detailed information on individuals
  - Nonobvious relationship awareness (NORA)
    - Combining data from multiple sources to find unclear hidden connections that might help identify criminals or terrorists
- Mobile device growth
  - Tracking of individual cell phones

NONOBVIOUS RELATIONSHIP AWARENESS (NORA)

NORA technology can take information about people from disparate sources and find obscure, nonobvious relationships. It might discover, for example, that an applicant for a job at a casino shares a telephone number with a known criminal and issue an alert to the hiring manager.

NORA is a technology that mines data resources to determine the relationships between people. Non-Obvious Relationship Awareness was created by Systems Research and Development (SRD). SRD developed this technology for the Las Vegas gaming industry to help the casinos detect relationships between customers and parties named by the Nevada Gaming Control Board as excluded persons. SRD was acquired by IBM on January 7, 2005.



Introduction to Information Security

- Information Security
- Threat
- Exposure
- Vulnerability
- Five Key Factors Increasing Vulnerability
- Cybercrime

Introduction to Information Security

- **Security:** the degree of protection against criminal activity, danger, damage, and/or loss.
- **Information Security:** all of the processes and policies designed to protect an organization's information and information systems (IS) from unauthorized access, use, disclosure, disruption, modification, or destruction.

Introduction to Information Security

- **Threat:** any danger to which a system may be exposed.
- **Exposure:** of an information resource is the harm, loss, or damage that can result if a threat compromises that resource.
- **Vulnerability:** the possibility that the system will be harmed by a threat.
- **Cybercrime:** refers to illegal activities conducted over computer networks, particularly the Internet.

Introduction to Information Security

Five Key Factors Increasing Vulnerability

1. Today's interconnected, interdependent, wirelessly networked business environment
2. Smaller, faster, cheaper computers and storage devices
3. Decreasing skills necessary to be a computer hacker
4. International organized crime taking over cybercrime
5. Lack of management support

Introduction to Information Security

- **Cybercrime:** refers to illegal activities conducted over computer networks, particularly the Internet.
- iDefense (http://labs.idefense.com), a company that specializes in providing security information to governments and Fortune 500 companies.