LESSON PREVIEW

Ethics and Privacy Concerns

Ethics. Morals. Laws. Religious edicts. These all tell you how to behave in various situations, but are they the same thing? While there may be some overlap, these are all different concepts. This module is about ethics—and not just ethics in general, but ethics and ethical dilemmas in the workplace.

In a nutshell, you can think of ethics as a guideline for how people should act. Ethical behavior, especially in the workplace, is not a simple matter of what to do. There are many times when doing the ethical thing for some may infringe on the privacy rights of others, and there are times when protecting an individual's privacy in the workplace is not a straightforward matter.

This module is about ethics and the ethical dilemmas faced by managers in corporations and organizations. It is also about defining individuals' rights to privacy and how these rights can best be protected.

After completing this section, you will be able to:

- Describe the differences between ethics and morals.
- Describe how to deal with ethical violations in the workplace.
- Define the five dimensions of ethical behavior in the digital age.
- Describe steps involved in an ethical dilemma analysis.
- Describe the five basic ethical principles.
- Define privacy and the right to privacy in the digital age.
- Define the major privacy laws in the United States and around the world.
- Describe what cookies are, the risks cookies pose to privacy on the Internet, and how to manage cookies.
- Define spyware and distinguish between opt-in and opt-out systems.
- Define intellectual property, copyrights, and patents.
- Explain how corporations use Big Data, and describe issues relating to privacy and Big Data.
- Describe ways to protect your privacy such as passwords, antivirus protection, safe browsing, and credit monitoring.

NOTES

What Are Ethics?

Ethics can provide a framework that allows a person to lead a virtuous life. Ethics should not be confused with the legal system or with religious tenets. Laws and religion can provide guidelines for morality, but the legal system often has a difficult time enforcing ethical behavior.

The competing values and interests in management information systems lead to a large number of ethical dilemmas. While laws do not equate to ethics, a study of a society's legal guidance can frame an ethical study.

NOTES

Ethical Concerns and Issues Impacting MIS

The Internet can make it difficult to distinguish between fact and fiction.

The uncontrolled and rapid acceleration of data collection creates challenges to issues of personal privacy and the protection of intellectual property.

With so much financial and personal data available online, the incidences of identity theft and frauds such as wire-wire and ransomware attacks have also proliferated.

NOTES

Ethical Computer Behavior, Ethics Violations

It is important to set **ethical computer use standards** in the workplace. Many employees think they can use business computers like they use their home computers.

Inappropriate computer use in the workplace can lead to decreased individual and network performance, a breach of network security, loss of company data, and charges of harassment. Using employee monitoring software or remote desktop software can discourage this behavior.

The two major categories of computer and network ethics violations are:

1. **Illegal activity:** This involves using the business's computers or networks in a criminal act.
2. **Organizational policy violations:** These differ by company but include prohibitions against sending personal email, shopping online, visiting social media sites, or playing computer games. Managing policy violations is generally left to the discretion of the manager.

NOTES

Reporting Computer Ethics Violations

Most organizations require that all employees report any computer ethics violation to their supervisors or to the network administrator. Before reporting a perceived organizational policy violation, you should consider if what you witnessed was subject to misinterpretation. Remember that your employer probably did not hire you to monitor the activities of your coworkers.

NOTES

Five Dimensions of Ethical Behavior in the Digital Age

1. **Information rights:** There are ethical dilemmas regarding rights of individuals and organizations to privacy. Who has the right to know what about you? For example, who has the right to know how many sick days an employee has taken?
2. **Copyright and intellectual property rights:** Managers must ensure that they create an environment that rigorously protects intellectual property. For example, how should an employee use company software—to create his own essay or only for company work?
3. **Control and accountability:** Who is guilty when a violation of privacy takes place? Consider, for example, a foreign company publishes private information about an employee in a local company who stole from the local company. Is the local company to blame for not protecting the employee information better?
4. **Establishing standards:** Managers should always set an example, but the use of social media is the hardest to control. For example, an employee uses his role in the company on his personal social media page. Is that acceptable?
5. **Quality of life:** What does a society value more—the right to freedom of expression or the right to not be harmed by others? For example, the court finds one site unacceptable for viewers under 21, but are the users' rights violated by having to post their age?

NOTES

Making Responsible Decisions

If an organization strives to act ethically, all of the individuals in the organizations must act ethically, especially regarding information. The organization's leadership must exhibit irreproachable ethical behavior at all times. By acting unethically, managers give permission for all of their employees to act unethically. Also, by not enforcing strong ethical behavior, managers encourage unethical behavior.

NOTES

Five Steps to an Ethical Dilemma Analysis

1. **Get the facts:** Research the question. Look for hidden agendas.
2. **Determine who is affected:** Understand who will be affected by the final decision. Will you, as manager, benefit from one possible outcome?
3. **Search for precedents:** Use guidelines from the company to help your decision making. Talk to other managers who have faced a similar dilemma.
4. **List the options:** Write a list of all options and potential outcomes. The "Twitter test" asks you to think whether you would be comfortable if your decision was posted on Twitter.
5. **Make a decision and prepare for unintended consequences:** When you make a decision, prepare for consequences. There are almost always unforeseen consequences or ramifications of any decision.

NOTES

Five Basic Ethical Principles

1. **The principle of moral rights:** This posits that there exist certain moral values that should always be upheld. The question is, Does the employee's right to privacy supersede the efficient operation of the organization?
2. **The principle of virtue:** This requires the decision maker to consider what a highly moral person would do when faced with this question. This can help to remove self-interest from a decision.
3. **The principle of distributive justice:** This says rewards should be distributed equitably based on effort or productivity. The problem is that employees may judge "fairness" based only as it affects them.
4. **The universalist principle:** This states that a manager must ensure that a decision is fair to all involved. The problem is that protecting one employee's right to privacy may result in others not seeing why a decision is fair.
5. **The utilitarian principle:** This is based on the concept that the ends justify the means. The problem is that this may conflict with principles of moral rights or virtue and often does not take into account unforeseen consequences.

NOTES

Internet Privacy and Right to Privacy in the Digital Age

Privacy is the right to control what happens with an individual's personal information. **Internet privacy** is the right of personal privacy concerning the storing, distributing, and displaying of information concerning an individual via the Internet.

The UN General Assembly adopted **Resolution 68/167** in December 2013. It affirms that the rights held by people offline must also be protected online. However, the right to digital privacy under international law is not absolute. Internet users should be aware that digital privacy is not honored by many on the Internet.

NOTES

International Privacy Laws

International laws on Internet privacy vary greatly. It is very difficult to get nations across the globe to agree on standardized Internet privacy laws. Therefore, it is important to use discretion on the Internet when traveling or living abroad. The European Union's (EU) European Commission Data Protection Directive states that under EU law, personal data can only be gathered legally under strict conditions.

NOTES

U.S. Privacy Laws and Internet Privacy

The First Amendment

The First Amendment to the U.S. Constitution protects freedom of speech against all levels of government censorship. First Amendment protection extends to the Internet, which means there is little government filtering of content.

Attempts to legislate protection of children have failed, based on First Amendment rights. Parents should be aware and, if necessary, supervise the use of the Internet by children.

NOTES

Major U.S. Policies and Acts That Impact Privacy—Part 1

The **Digital Millennium Copyright Act** of 1998 implements treaties of the World Intellectual Property Organization (WIPO) and is comprised of five titles meant to protect intellectual property in digital formats.

The **Children's Internet Protection Act (CIPA)** of 2000 addresses children's access to harmful content over the Internet. Public schools and libraries must comply with Internet safety policies imposed by the government under this legislation. It specifically requires all pornographic sites to include age verification.

The **Electronic Communications Privacy Act** of 1986 protects email and VoIP communications by making it illegal to intercept calls or messages without a warrant.

NOTES

Major U.S. Policies and Acts That Impact Privacy—Part 2

The **USA PATRIOT Act/USA FREEDOM Act** was enacted to monitor terrorist activities and communications. It allows law enforcement to obtain information about online and offline communications related to terrorist activities without a warrant. Some parts of the PATRIOT Act expired in 2015, but many were restored with the USA FREEDOM Act. However, the National Security Agency (NSA) can no longer collect mass phone data, but phone companies must retain the data.

The **Federal Information Security Management Act (FISMA)** outlines a plan to protect government information and assets against cyberthreats and requires each federal agency to develop a plan for information security.

The **Cybersecurity Information Sharing Act (CISA)** is referred to as an antihacking statute. It created a network where information about cybersecurity threats can be shared between the government and technology companies. The **Computer Fraud and Abuse Act (CFAA)** prohibits accessing a computer or network without proper authorization.

The **Wiretap Act** is a federal law that protects person-to-person wire, oral, and electronic communications. It contains a variety of network crime statutes that include identity theft and unlawful access to stored communications.

NOTES

Challenges Facing Internet Privacy: Cookies

A **cookie** is a small text file of information created by a website that the web browser stores on the user's hard disk. The browser uses the information in the cookie when the site is revisited to customize the user's experience. **First-party cookies** are created by the visited website, and third-party cookies are created by an outside website. **Third-party cookies** are considered an invasion of privacy.

Session cookies are text files that are stored in temporary memory and are lost when the web browser is closed. They collect information about the start and end of a browsing session, analyze and measure web traffic on the web pages visited, and determine the web browser being used.

Persistent cookies are stored on the hard drive and are only lost if they are designed with an expiration date. Persistent cookies collect information about user preferences, username and password information, IP address, and web surfing behavior.

NOTES

Privacy Risks with Cookies and Managing Cookies

Cookies pose potential privacy risks. They can be used to collect and sell information about surfing habits to third parties. This can be used to create user profiles and monitor behavior by corporate and government entities.

Cookies can be managed through the browser's cookie settings and must be adjusted for each browser. In Settings, cookies can be deleted, blocked, and more.

NOTES

Spyware

Spyware collects keystrokes, passwords, account numbers, and more. It is commonly installed through free downloads. Common types of spyware include keystroke loggers and packet analyzers (sniffers).

Keystroke loggers record all actions typed on a keyboard and can record passwords and confidential information.

Packet analyzers or packet **sniffers** capture packets transmitted over a network. Legitimate sniffers are used for routine examination and problem detection. Unauthorized sniffers are used to steal information.

NOTES

Opt-in and Opt-out

Opt-in and opt-out are common methods used to gain consumer permission to access the consumer's information or to track behavior.

With an **opt-out** system, there may be a checked box that says the user agrees to something. To refuse that option, the user must uncheck the box.

With an **opt-in** system, the check box is empty and the user must check the box to agree.

Through these mechanisms, users often give businesses permission to collect data on their Internet behaviors without even realizing it.

NOTES

Intellectual Property: Copyrights and Patents

Intellectual property consists of human knowledge and ideas that are protected by law against unauthorized use. There are four categories of intellectual property protection: patents, trademarks, copyrights, and trade secrets.

The U.S. Copyright Office defines a **copyright** as a form of protection provided by the laws of the United States for "original works of authorship," including literary, dramatic, musical, architectural, cartographic, choreographic, pantomimic, pictorial, graphic, sculptural, and audiovisual creations. Copyright protection does not extend to any idea, procedure, process, system, title, principle, or discovery. Names, titles, short phrases, slogans, familiar symbols, mere variations of typographic ornamentation, lettering, coloring, and listings of contents or ingredients are not subject to copyright.

When the government grants an inventor the right to exclude others from the use of an invention for a period of time, this is called a **patent.** A **utility patent** is granted for a new machine or process. A **design patent** protects the unique appearance of an object. Patents are granted by the U.S. Patent and Trademark Office.

NOTES

The Digital Millennium Copyright Act

The **Digital Millennium Copyright Act (DMCA)** was signed into law by President Clinton in 1998. The Act implements two World Intellectual Property Organization (WIPO) treaties. The three titles in the DMCA that directly impact digital copyright issues are:

Title 1: WIPO Copyright and Phonograms Treaties and Implementation Act, which requires measures that make it difficult to copy analog video recordings.

Title 2: Online Copyright Infringement Liability Limitation protects Internet Service Providers (ISPs) from being sued for copyright infringement by the ISP's user.

Title 4: Contains miscellaneous provisions for digital copyrights and facilitates distance learning by allowing educational institutions latitude in the use of copyrighted material.

NOTES

Data, Structured Data, and Big Data

Data are the raw facts that describe the characteristics of an event, object, or set of information.

Structured data have a defined length, type, and format and include numbers, dates, or strings. The data are designed for input into databases.

Big Data refers to methodologies that deal with the vast amount of complex information that accumulates at high and accelerating velocity. Big Data uses predictive analytics to attempt to determine behavior. Traditional relational databases cannot manage the enormous amount of data generated by the IoT, so Big Data demands more advanced software solutions.

NOTES

Privacy Concerns Regarding Big Data

Big Data attempts to predict behavior by tracking incredibly large amounts of digital activity and using this past activity to determine what is likely to happen in the future.

The privacy concerns with the use of Big Data are significant. Is it appropriate to track Internet use or buyer behavior? Electronic medical records place millions of patients' private data on the Internet. Millions more voluntarily have their DNA tested and loaded on servers at many sites. This data can be used to predict future health issues and buying behavior. The impact on personal privacy cannot be overstated.

NOTES

Corporation Use of Big Data

Corporations attempt to use all the information collected from Big Data for insight to improve their profits. Big Data has been extremely effective in logistics and supply chain management. Weather predictions allow businesses to anticipate risks and the associated expense involved. Insurance companies use Big Data in actuarial analysis for more accurate risk estimates. These are only a few of the ways Big Data is used by corporations, but many corporations find the greatest value of collecting Big Data is by selling it to other corporations.

NOTES

Three Methods for Collecting Big Data

Direct inquiry: This is the primary method used to gather data. Many sites simply ask users for their data. Methods of direct inquiry include loyalty cards or apps that track consumer spending with the agreement of the customer, fitness apps that track workouts, and surveys.

Indirect tracking: Cookies and web beacons allow companies to track website visitors' browsing habits. Sites can add links and follow activity through the link activation. Often, users of mobile games unknowingly give permission to game developers to track their phones' browser activity.

Third-party data purchase: Several large corporations purchase and sell consumer data. Database marketing companies track consumer behavior and sell this information to media companies, marketers, retailers, and other organizations.

NOTES

Protecting Big Data

Any Big Data storage system must protect the integrity and security of the data. High-profile data breaches have occurred often in the past several years and prove that no data system is truly secure.

The estimated cost of data breaches is forecast to be in the trillions of dollars. In 2019 alone, a collection of 2.7 billion identity records was posted on the Internet for sale.

A major transition in the Big Data security sector is to move all data storage to a third-party Cloud storage. It is argued that Cloud service providers can install far better security measures than that of all but the largest data security firms. Cloud storage also greatly reduces the human factor in data protection. Either through ignorance or through negligence, over half of all data breaches can be traced to human error.

NOTES

Protecting Your Privacy: Passwords

Completely safeguarding your information privacy in the digital era is essentially impossible. However, there are steps that can be taken to reduce risks.

A strong **password** is the first line of defense in safeguarding your digital privacy. A password is a secret code that helps prevent unauthorized access to data and user accounts. However, passwords only identify the authenticity of the password, not the user. Other security measures must be used to verify the authenticity of a user.

Password management software can help keep passwords safe. When you log in to a secure site, the password management software offers to save your identification. When you return to that site, it will automatically complete the login using your saved information, but will generate a new password for the next login.

NOTES

Protecting Your Privacy: Antivirus Protection

Antivirus software scans files to identify and remove computer viruses and other malicious programs to identify and remove viruses and malware.

Signature-based detection looks for virus signatures to identify the virus.

Heuristic-based detection looks for malware by examining files for suspicious characteristics without an exact signature match.

Antivirus software can be free or fee based. Free antivirus programs come with basic detection and protection. Fee-based software usually comes with more features, and it normally includes technical support while most free software does not.

Free antivirus programs come with advertising, which can be annoying, but the malware detection performance is excellent and performs almost as effectively as their fee-based counterparts.

NOTES

Safe Browsing and Online Purchasing

One way to help stay safe online is to use the browser's **private browsing mode**. When private browsing has been activated, the browser will not store cookies.

Private browsing does not securely hide your identity because your IP address can still be tracked. A **Virtual Private Network (VPN)** can help protect your online identity because it essentially hides your IP address by running your communications through a secure network.

Make sure the sites you shop from have "https" at the beginning of the URL. **HTTPS** is the secure version of the HTTP protocol. Always use a credit card, not a debit card, when shopping online. This gives you a layer of security between your cash and hackers on the Internet. Using your debit card can give hackers direct access to your checking accounts.

NOTES

Credit Monitoring

Bad credit can cost you thousands of dollars in high interest rates, or prevent you from buying a car, renting an apartment, obtaining a security clearance, or getting a job.

You are entitled to one free credit report of your Fair Isaac Corp (FICO) score from each of three reporting agencies each year. These agencies are TransUnion, Equifax, and Experian.

Checking your own credit score is considered a “soft inquiry” and does not affect your credit rating. You should also check your bank accounts for unusual activity. Combining this with monitoring your credit reports is usually enough to alert you to credit fraud. You can also buy credit monitoring.

NOTES