MODUL SITEM INFORMASI MANAGEMEN

(MAN 611)

MODUL PERTEMUAN 05

Ethical and Social Issues in Information System

DISUSUN OLEH

Dr. Fransiskus Adikara, S.Kom, MMSI

UNIVERSITAS ESA UNGGUL

2019

ETHICAL AND SOCIAL ISSUES

1. Kemampuan Akhir Yang Diharapkan

After reading this session, you will be able to answer the following questions:

1. What ethical, social, and political issues are raised by information systems?
2. What specific principles for conduct can be used to guide ethical decisions?
3. Why do contemporary information systems technology and the Internet pose challenges to the protection of individual privacy and intellectual property?
4. How have information systems affected everyday life?

2. Uraian dan Contoh

1. UNDERSTANDING ETHICAL AND SOCIAL ISSUES RELATED TO SYSTEMS

In the past 10 years, we have witnessed, arguably, one of the most ethically challenging periods for U.S. and global business. Table 4.1 provides a small sample of recent cases demonstrating failed ethical judgment by senior and middle managers. These lapses in ethical and business judgment occurred across a broad spectrum of industries.

In today's new legal environment, managers who violate the law and are convicted will most likely spend time in prison. U.S. federal sentencing guidelines adopted in 1987 mandate that federal judges impose stiff sentences on business executives based on the monetary value of the crime, the presence of a conspiracy to prevent discovery of the crime, the use of structured financial transactions to hide the crime, and failure to cooperate with prosecutors (U.S. Sentencing Commission, 2004).

Although business firms would, in the past, often pay for the legal defense of their employees enmeshed in civil charges and criminal investigations, firms are now encouraged to cooperate with prosecutors to reduce charges against the entire firm for obstructing investigations. These developments mean that, more than ever, as a manager or an employee, you will have to decide for yourself what constitutes proper legal and ethical conduct.

Although these major instances of failed ethical and legal judgment were not masterminded by information systems departments, information systems were instrumental in many of these frauds. In many cases, the perpetrators of these crimes artfully used financial reporting information systems to bury their decisions from public scrutiny in the vain hope they would never be caught.

We deal with the issue of control in information systems in Chapter 8. In this chapter, we talk about the ethical dimensions of these and other actions based on the use of information systems.

Ethics refers to the principles of right and wrong that individuals, acting as free moral agents, use to make choices to guide their behaviors. Information systems raise new ethical questions for both individuals and societies because they create opportunities for intense social change, and thus threaten existing distributions of power, money, rights, and obligations. Like other technolo- gies, such as steam engines, electricity, the telephone, and the radio, informa- tion technology can be used to achieve social progress, but it can also be used to commit crimes and threaten cherished social values. The development of information technology will produce benefits for many and costs for others.

Ethical issues in information systems have been given new urgency by the rise of the Internet and electronic commerce. Internet and digital firm technologies make it easier than ever to assemble, integrate, and distribute information, unleashing new concerns about the appropriate use of customer information, the protection of personal privacy, and the protection of intellectual property.

Other pressing ethical issues raised by information systems include estab- lishing accountability for the consequences of information systems, setting standards to safeguard system quality that protects the safety of the individual and society, and preserving values and institutions considered essential to the quality of life in an information society. When using information systems, it is essential to ask, “What is the ethical and socially responsible course of action?”

A MODEL FOR THINKING ABOUT ETHICAL, SOCIAL, AND POLITICAL ISSUES

Ethical, social, and political issues are closely linked. The ethical dilemma you may face as a manager of information systems typically is reflected in social and political debate. One way to think about these relationships is shown in Figure 4.1. Imagine society as a more or less calm pond on a summer day, a delicate ecosystem in partial equilibrium with individuals and with social and political institutions. Individuals know how to act in this pond because social institutions (family, education, organizations) have developed well-honed rules of behavior, and these are supported by laws developed in the political sector that prescribe behavior and promise sanctions for violations. Now toss a rock into the center of the pond. What happens? Ripples, of course.

Imagine instead that the disturbing force is a powerful shock of new informa- tion technology and systems hitting a society more or less at rest. Suddenly, individual actors are confronted with new situations often not covered by the old rules. Social institutions cannot respond overnight to these ripples—it may take years to develop etiquette, expectations, social responsibility, politically correct attitudes, or approved rules. Political institutions also require time before developing new laws and often require the demonstration of real harm before they act. In the meantime, you may have to act. You may be forced to act in a legal gray area.

We can use this model to illustrate the dynamics that connect ethical, social, and political issues. This model is also useful for identifying the main moral dimensions of the information society, which cut across various levels of action—individual, social, and political.

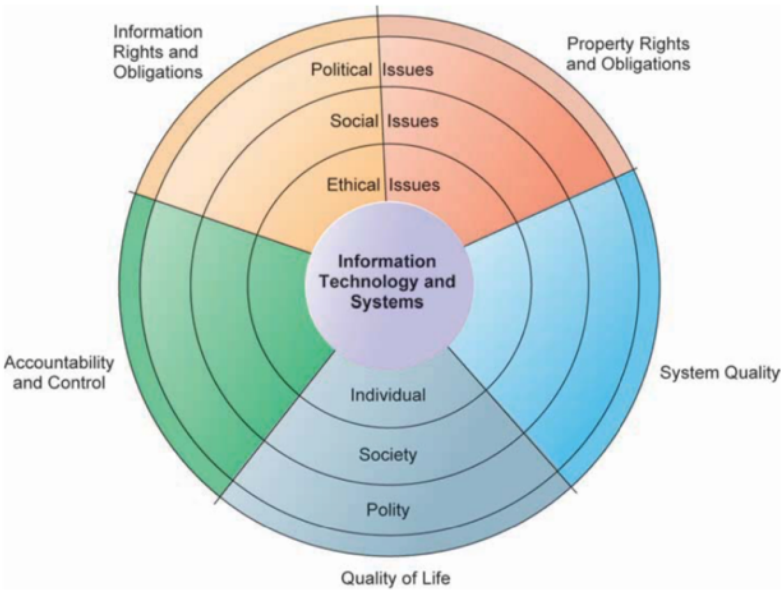
FIVE MORAL DIMENSIONS OF THE INFORMATION AGE

The major ethical, social, and political issues raised by information systems include the following moral dimensions:

- *Information rights and obligations.* What **information rights** do individuals and organizations possess with respect to themselves? What can they protect?
- P*roperty rights and obligations.* How will traditional intellectual property rights be protected in a digital society in which tracing and accounting for ownership are difficult and ignoring such property rights is so easy?
- *Accountability and control.* Who can and will be held accountable and liable for the harm done to individual and collective information and property rights?
- *System quality.* What standards of data and system quality should we demand to protect individual rights and the safety of society?
- *Quality of life.* What values should be preserved in an information- and knowledge-based society? Which institutions should we protect from violation? Which cultural values and practices are supported by the new information technology?

We explore these moral dimensions in detail in Section 4.3.

FIGURE 4.1 THE RELATIONSHIP BETWEEN ETHICAL, SOCIAL, AND 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.

KEY TECHNOLOGY TRENDS THAT RAISE ETHICAL ISSUES

Ethical issues long preceded information technology. Nevertheless, information technology has heightened ethical concerns, taxed existing social arrangements, and

made some laws obsolete or severely crippled. There are four key technological trends responsible for these ethical stresses and they are summarized in Table 4.2.

The doubling of computing power every 18 months has made it possible for most organizations to use information systems for their core production processes. As a result, our dependence on systems and our vulnerability to system errors and poor data quality have increased. Social rules and laws have not yet adjusted to this dependence. Standards for ensuring the accuracy and reliability of information systems (see Chapter 8) are not universally accepted or enforced.

Advances in data storage techniques and rapidly declining storage costs have been responsible for the multiplying databases on individuals—employ- ees, customers, and potential customers—maintained by private and public organizations. These advances in data storage have made the routine violation of individual privacy both cheap and effective. Very large data storage systems capable of working with terabytes of data are inexpensive enough for large firms to use in identifying customers.

Advances in data analysis techniques for large pools of data are another technological trend that heightens ethical concerns because companies and government agencies are able to find out highly detailed personal information about individuals. With contemporary data management tools (see Chapter 6), companies can assemble and combine the myriad pieces of information about you stored on computers much more easily than in the past.

Think of all the ways you generate computer information about yourself— credit card purchases, telephone calls, magazine subscriptions, video rentals, mail-order purchases, banking records, local, state, and federal government records (including court and police records), and visits to Web sites. Put together and mined properly, this information could reveal not only your credit information but also your driving habits, your tastes, your associations, what you read and watch, and your political interests.

Companies with products to sell purchase relevant information from these sources to help them more finely target their marketing campaigns. Chapters 5 and 10 describe how companies can analyze large pools of data from multiple sources to rapidly identify buying patterns of customers and suggest individ- ual responses. The use of computers to combine data from multiple sources and create electronic dossiers of detailed information on individuals is called **profiling**.

For example, several thousand of the most popular Web sites allow DoubleClick (owned by Google), an Internet advertising broker, to track the on visitor information DoubleClick gathers. DoubleClick uses this information to create a profile of each online visitor, adding more detail to the profile as the visitor accesses an associated DoubleClick site. Over time, DoubleClick can create a detailed dossier of a person's spending and computing habits on the Web that is sold to companies to help them target their Web ads more precisely.

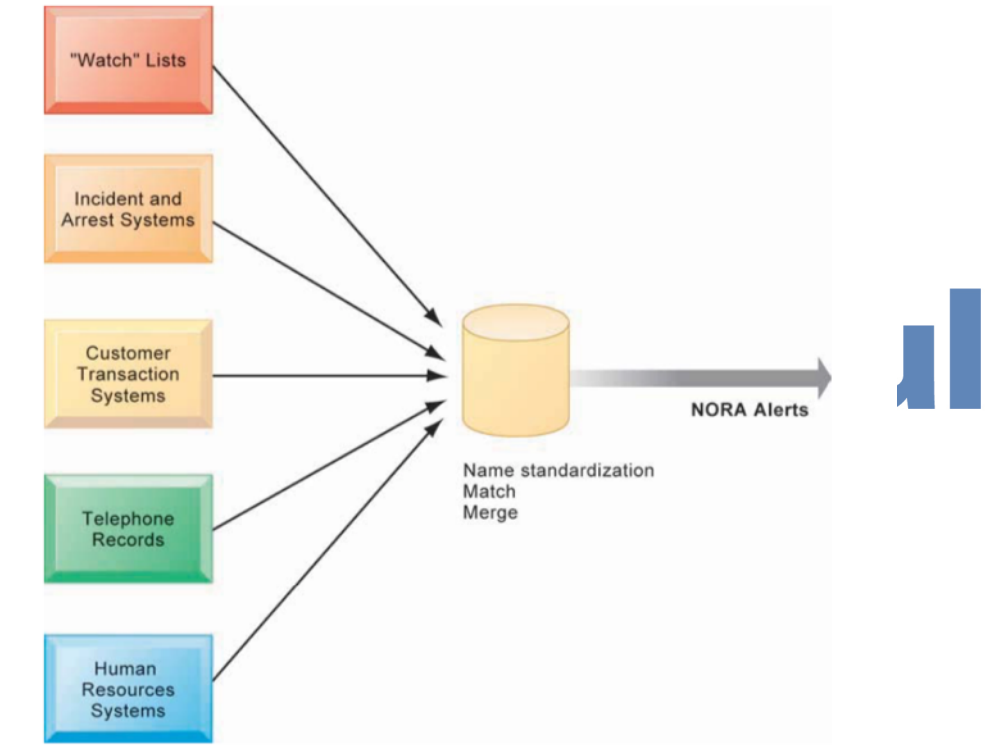
ChoicePoint gathers data from police, criminal, and motor vehicle records, credit and employment histories, current and previous addresses, professional licenses, and insurance claims to assemble and maintain electronic dossiers on almost every adult in the United States. The company sells this personal information to businesses and

government agencies. Demand for personal data is so enormous that data broker businesses such as ChoicePoint are flourishing. In 2011, the two largest credit card networks, Visa Inc. and MasterCard Inc., were planning to link credit card purchase information with consumer social network and other information to create customer profiles that could be sold to advertising firms. In 2012, Visa will process more than 45 billion transactions a year and MasterCard will process more than 23 billion transactions. Currently, this transactional information is not linked with consumer Internet activities.

A new data analysis technology called **nonobvious relationship aware- ness (NORA)** has given both the government and the private sector even more powerful profiling capabilities. NORA can take information about people from many disparate sources, such as employment applications, telephone records, customer listings, and "wanted" lists, and correlate relationships to find obscure hidden connections that might help identify criminals or terrorists (see Figure 4.2).

NORA technology scans data and extracts information as the data are being generated so that it could, for example, instantly discover a man at an airline ticket counter who shares a phone number with a known terrorist before that person boards an airplane. The technology is considered a valuable tool for homeland security but does have privacy implications because it can provide such a detailed picture of the activities and associations of a single individual.

FIGURE 4.2 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.

Finally, advances in networking, including the Internet, promise to greatly reduce the costs of moving and accessing large quantities of data and open the possibility of mining large pools of data remotely using small desktop machines, permitting an invasion of privacy on a scale and with a precision heretofore unimaginable.

2. ETHICS IN AN INFORMATION SOCIETY

Ethics is a concern of humans who have freedom of choice. Ethics is about individual choice: When faced with alternative courses of action, what is the correct moral choice? What are the main features of ethical choice?

BASIC CONCEPTS: RESPONSIBILITY, ACCOUNTABILITY,

AND LIABILITY

Ethical choices are decisions made by individuals who are responsible for the consequences of their actions. **Responsibility** is a key element of ethical action. Responsibility means that you accept the potential costs, duties, and obligations for the decisions you make. **Accountability** is a feature of systems and social institu- tions: It means that mechanisms are in place to determine who took responsible action, and who is responsible. Systems and institutions in which it is impossible to find out who took what action are inherently incapable of ethical analysis or ethical action. **Liability** extends the concept of responsibility further to the area of laws. Liability is a feature of political systems in which a body of laws is in place that permits individuals to recover the damages done to them by other actors, systems, or organizations. **Due process** is a related feature of law-governed soci- eties and is a process in which laws are known and understood, and there is an ability to appeal to higher authorities to ensure that the laws are applied correctly.

These basic concepts form the underpinning of an ethical analysis of infor- mation systems and those who manage them. First, information technologies are filtered through social institutions, organizations, and individuals. Systems do not have impacts by themselves. Whatever information system impacts exist are products of institutional, organizational, and individual actions and behav- iors. Second, responsibility for the consequences of technology falls clearly on the institutions, organizations, and individual managers who choose to use the technology. Using information technology in a socially responsible manner means that you can and will be held accountable for the consequences of your actions. Third, in an ethical, political society, individuals and others can recover damages done to them through a set of laws characterized by due process.

ETHICAL ANALYSIS

When confronted with a situation that seems to present ethical issues, how should you analyze it? The following five-step process should help:

1. *Identify and describe the facts clearly*. Find out who did what to whom, and where, when, and how. In many instances, you will be surprised at the errors in the initially reported facts, and often you will find that simply getting the facts

straight helps define the solution. It also helps to get the opposing parties involved in an ethical dilemma to agree on the facts.

2. *Define the conflict or dilemma and identify the higher-order values involved.* Ethical, social, and political issues always reference higher values. The parties to a dispute all claim to be pursuing higher values (e.g., freedom, privacy, protection of property, and the free enterprise system). Typically, an ethical issue involves a dilemma: two diametrically opposed courses of action that support worthwhile values. For example, the chapter-ending case study illustrates two competing values: the need to improve health care record keeping and the need to protect individual privacy.
3. *Identify the stakeholders.* Every ethical, social, and political issue has stakeholders: players in the game who have an interest in the outcome, who have invested in the situation, and usually who have vocal opinions. Find out the identity of these groups and what they want. This will be useful later when designing a solution.
4. *Identify the options that you can reasonably take.* You may find that none of the options satisfy all the interests involved, but that some options do a better job than others. Sometimes arriving at a good or ethical solution may not always be a balancing of consequences to stakeholders.
5. *Identify the potential consequences of your options.* Some options may be ethically correct but disastrous from other points of view. Other options may work in one instance but not in other similar instances. Always ask yourself, "What if I choose this option consistently over time?"

CANDIDATE ETHICAL PRINCIPLES

Once your analysis is complete, what ethical principles or rules should you use to make a decision? What higher-order values should inform your judgment? Although you are the only one who can decide which among many ethical prin- ciples you will follow, and how you will prioritize them, it is helpful to consider some ethical principles with deep roots in many cultures that have survived throughout recorded history:

1. Do unto others as you would have them do unto you (the **Golden Rule**). Putting yourself into the place of others, and thinking of yourself as the object of the decision, can help you think about fairness in decision making.
2. If an action is not right for everyone to take, it is not right for anyone **(Immanuel Kant's Categorical Imperative)**. Ask yourself, "If everyone did this, could the organization, or society, survive?"
3. If an action cannot be taken repeatedly, it is not right to take at all **(Descartes' rule of change)**. This is the slippery-slope rule: An action may bring about a small change now that is acceptable, but if it is repeated, it would bring unacceptable changes in the long run. In the vernacular, it might be stated as "once started down a slippery path, you may not be able to stop."
4. Take the action that achieves the higher or greater value **(Utilitarian Principle)**. This rule assumes you can prioritize values in a rank order and understand the consequences of various courses of action.
5. Take the action that produces the least harm or the least potential cost **(Risk Aversion Principle).** Some actions have extremely high failure costs of very low probability (e.g., building a nuclear generating facility in an urban area) or extremely high failure costs of moderate probability (speeding and automobile

accidents). Avoid these high-failure-cost actions, paying greater attention to high-failure-cost potential of moderate to high probability.

6. Assume that virtually all tangible and intangible objects are owned by someone else unless there is a specific declaration otherwise. (This is the **ethical "no free lunch" rule.)** If something someone else has created is useful to you, it has value, and you should assume the creator wants compensation for this work.

Actions that do not easily pass these rules deserve close attention and a great deal of caution. The appearance of unethical behavior may do as much harm to you and your company as actual unethical behavior.

PROFESSIONAL CODES OF CONDUCT

When groups of people claim to be professionals, they take on special rights and obligations because of their special claims to knowledge, wisdom, and respect. Professional codes of conduct are promulgated by associations of professionals, such as the American Medical Association (AMA), the American Bar Association (ABA), the Association of Information Technology Professionals (AITP), and the Association for Computing Machinery (ACM). These professional groups take responsibility for the partial regulation of their professions by determining entrance qualifications and competence. Codes of ethics are promises by professions to regulate themselves in the general interest of society. For exam- ple, avoiding harm to others, honoring property rights (including intellectual property), and respecting privacy are among the General Moral Imperatives of the ACM's Code of Ethics and Professional Conduct.

3. THE MORAL DIMENSIONS OF INFORMATION SYSTEMS

In this section, we take a closer look at the five moral dimensions of informa- tion systems first described in Figure 4.1. In each dimension, we identify the ethical, social, and political levels of analysis and use real-world examples to illustrate the values involved, the stakeholders, and the options chosen.

INFORMATION RIGHTS: PRIVACY AND FREEDOM IN

THE INTERNET AGE

Privacy is the claim of individuals to be left alone, free from surveillance or interference from other individuals or organizations, including the state. Claims to privacy are also involved at the workplace: Millions of employees are subject to electronic and other forms of high-tech surveillance. Information technology and systems threaten individual claims to privacy by making the invasion of privacy cheap, profitable, and effective.

The claim to privacy is protected in the U.S., Canadian, and German constitutions in a variety of different ways and in other countries through various statutes. In the United States, the claim to privacy is protected primar- ily by the First Amendment guarantees of freedom of speech and association, the Fourth Amendment protections against unreasonable search and seizure of one's personal documents or home, and the guarantee of due process.

Table 4.3 describes the major U.S. federal statutes that set forth the conditions for handling information about individuals in such areas as credit reporting, education, financial records, newspaper records, and electronic communications. The Privacy Act of 1974 has been the most important of these laws, regulating the federal government's collection, use, and disclosure of information. At present, most U.S. federal privacy laws apply only to the federal government and regulate very few areas of the private sector.

Most American and European privacy law is based on a regime called **Fair Information Practices (FIP)** first set forth in a report written in 1973 by a federal government advisory committee and updated most recently in 2010 to take into account new privacy-invading technology (FTC, 2010; U.S. Department of Health, Education, and Welfare, 1973). FIP is a set of principles governing the collection and use of information about individuals. FIP principles are based on the notion of a mutuality of interest between the record holder and the individual. The individual has an interest in engaging in a transaction, and the record keeper—usually a business or government agency—requires infor- mation about the individual to support the transaction. Once information is gathered, the individual maintains an interest in the record, and the record may not be used to support other activities without the individual's consent. In 1998, the FTC restated and extended the original FIP to provide guidelines for protecting online privacy. Table 4.4 describes the FTC's Fair Information Practice principles.

Internet Challenges to Privacy

Internet technology has posed new challenges for the protection of individual privacy. Information sent over this vast network of networks may pass through many different computer systems before it reaches its final destination. Each of these systems is capable of monitoring, capturing, and storing communications that pass through it.

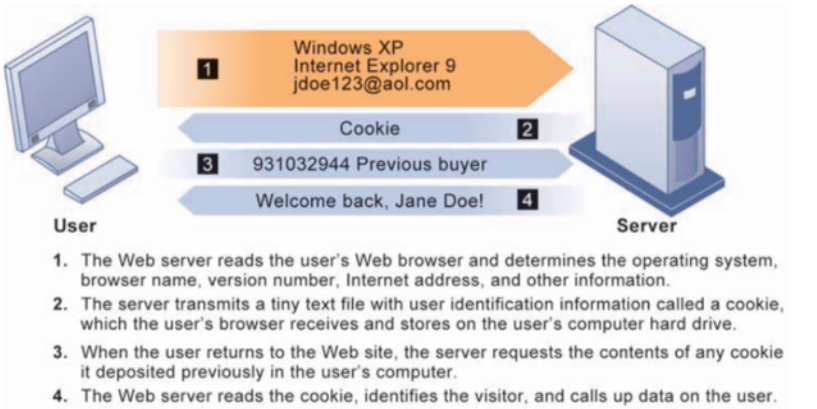
Web sites track searches that have been conducted, the Web sites and Web pages visited, the online content a person has accessed, and what items that person has inspected or purchased over the Web. This monitoring and tracking of Web site visitors occurs in the background without the visitor's knowledge. It is conducted not just by individual Web sites but by advertising networks such as Microsoft Advertising, Yahoo, and DoubleClick that are capable of tracking personal browsing behavior across thousands of Web sites. Both Web site publishers and the advertising industry defend tracking of individuals across the Web because doing so allows more relevant ads to be targeted to users, and it pays for the cost of publishing Web sites. In this sense, it's like broadcast television: advertiser-supported content that is free to the user. The commercial demand for this personal information is virtually insatiable.

Cookies are small text files deposited on a computer hard drive when a user visits Web sites. Cookies identify the visitor's Web browser software and track visits to the Web site. When the visitor returns to a site that has stored a cookie, the Web site software will search the visitor's computer, find the cookie, and know what that person has done in the past. It may also update the cookie, depending on the activity during the visit. In this way, the site can customize its content for each visitor's interests. For example, if you purchase a book on Amazon.com and return later from the same browser, the site will welcome you by name and recommend other books of interest based on your past purchases. DoubleClick, described earlier in this chapter, uses

cookies to build its dossiers with details of online purchases and to examine the behavior of Web site visi- tors. Figure 4.3 illustrates how cookies work.

Web sites using cookie technology cannot directly obtain visitors' names and addresses. However, if a person has registered at a site, that information can be combined with cookie data to identify the visitor. Web site owners can also combine the data they have gathered from cookies and other Web site monitor- ing tools with personal data from other sources, such as offline data collected from surveys or paper catalog purchases, to develop very detailed profiles of their visitors.

FIGURE 4.3 HOW COOKIES IDENTIFY WEB VISITORS



1. The Web server reads the user's Web browser and determines the operating system, browser name, version number, Internet address, and other information.
2. The server transmits a tiny text file with user identification information called a cookie, which the user's browser receives and stores on the user's computer hard drive.
3. When the user returns to the Web site, the server requests the contents of any cookie it deposited previously in the user's computer.
4. The Web server reads the cookie, identifies the visitor, and calls up data on the user.

Cookies are written by a Web site on a visitor's hard drive. When the visitor returns to that Web site, the Web server requests the ID number from the cookie and uses it to access the data stored by that server on that visitor. The Web site can then use these data to display personalized information.

There are now even more subtle and surreptitious tools for surveillance of Internet users. So-called "super cookies" or Flash cookies cannot be easily deleted and can be installed whenever a person clicks on a Flash video. These so-called "Local Shared Object" files are used by Flash to play videos and are put on the user's computer without their consent. Marketers use Web beacons as another tool to monitor online behavior. **Web beacons**, also called *Web bugs* (or simply "tracking files"), are tiny software programs that keep a record of users' online clickstream and report this data back to whomever owns the tracking file invisibly embedded in e-mail messages and Web pages that are designed to monitor the behavior of the user visiting a Web site or sending e-mail. Web bea- cons are placed on popular Web sites by third-party firms who pay the Web sites a fee for access to their audience. So how common is Web tracking? In a path- breaking series of articles in the *Wall Street Journal* in 2010 and 2011, research- ers examined the tracking files on 50 of the most popular U.S Web sites. What they found revealed a very widespread surveillance system. On the 50 sites, they discovered 3,180 tracking files installed on visitor computers. Only one site, Wikipedia, had no tracking files. Some popular sites such as Dictionary. com, MSN, and Comcast, installed more than 100 tracking files! Two-thirds of the tracking files came from 131 companies whose primary business is identify- ing and tracking Internet users to create consumer profiles that can be sold to advertising firms looking for specific types of customers. The biggest trackers were Google, Microsoft, and Quantcast, all of whom are in the business of sell- ing ads to advertising firms and marketers. A follow-up study in 2012 found the situation had worsened: tracking on the

50 most popular sites had risen nearly five fold! The cause: growth of online ad auctions where advertisers buy the data about users' Web browsing behavior.

Other **spyware** can secretly install itself on an Internet user's computer by piggybacking on larger applications. Once installed, the spyware calls out to Web sites to send banner ads and other unsolicited material to the user, and it can report the user's movements on the Internet to other computers. More information is available about intrusive software in Chapter 8.

About 75 percent of global Internet users use Google Search and other Google services, making Google the world's largest collector of online user data. Whatever Google does with its data has an enormous impact on online privacy. Most experts believe that Google possesses the largest collection of personal information in the world—more data on more people than any government agency. The nearest competitor is Facebook.

After Google acquired the advertising network DoubleClick in 2007, Google has been using behavioral targeting to help it display more relevant ads based on users' search activities and to target individuals as they move from one site to another in order to show them display or banner ads. Google allows tracking software on its search pages, and using DoubleClick, it is able to track users across the Internet. One of its programs enables advertisers to target ads based on the search histories of Google users, along with any other informa- tion the user submits to Google such as age, demographics, region, and other Web activities (such as blogging). Google's AdSense program enables Google to help advertisers select keywords and design ads for various market segments based on search histories, such as helping a clothing Web site create and test ads targeted at teenage females. A recent study found that 88 percent of 400,000 Web sites had at least one Google tracking bug.

Google has also been scanning the contents of messages received by users of its free Web-based e-mail service called Gmail. Ads that users see when they read their e-mail are related to the subjects of these messages. Profiles are developed on individual users based on the content in their e-mail. Google now displays targeted ads on YouTube and on Google mobile applications, and its DoubleClick ad network serves up targeted banner ads.

The United States has allowed businesses to gather transaction information generated in the marketplace and then use that information for other market- ing purposes without obtaining the informed consent of the individual whose information is being used. An **opt-out** model of informed consent permits the collection of personal information until the consumer specifically requests that the data not be collected. Privacy advocates would like to see wider use of an **opt-in** model of informed consent in which a business is prohibited from collecting any personal information unless the consumer specifically takes action to approve information collection and use. Here, the default option is no collection of user information.

The online industry has preferred self-regulation to privacy legislation for protecting consumers. The online advertising industry formed the Online Privacy Alliance to encourage self-regulation to develop a set of privacy guide- lines for its members. The group promotes the use of online seals, such as that of TRUSTe, certifying Web sites adhering to certain privacy principles. Members of the advertising network industry,

including Google's DoubleClick, have created an additional industry association called the Network Advertising Initiative (NAI) to develop its own privacy policies to help consumers opt out of advertising network programs and provide consumers redress from abuses.

Individual firms like Microsoft, Mozilla Foundation, Yahoo, and Google have recently adopted policies on their own in an effort to address public concern about tracking people online. Microsoft has promised to ship its new Internet Explorer 10 Web browser with the opt-out option as the default in 2012. AOL established an opt-out policy that allows users of its site to not be tracked. Yahoo follows NAI guidelines and also allows opt-out for tracking and Web beacons (Web bugs). Google has reduced retention time for tracking data.

In general, most Internet businesses do little to protect the privacy of their customers, and consumers do not do as much as they should to protect themselves. For commercial Web sites that depend on advertising to support themselves, most revenue derives from selling customer information. Of the companies that do post privacy polices on their Web sites, about half do not monitor their sites to ensure they adhere to these policies. The vast majority of online customers claim they are concerned about online privacy, but less than half read the privacy statements on Web sites. In general, Web site privacy policies require a law degree to understand and are ambiguous about key terms (Laudon and Traver, 2013).

In one of the more insightful studies of consumer attitudes towards Internet privacy, a group of Berkeley students conducted surveys of online users, and of complaints filed with the FTC involving privacy issues. Here are some of their results: people feel they have no control over the information collected about them, and they don't know who to complain to. Web sites collect all this information, but do not let users have access, the Web site policies are unclear, and they share data with "affiliates" but never identify who the affili- ates are and how many there are. Web bug trackers are ubiquitous and users are not informed of trackers on the pages users visit. The results of this study and others suggest that consumers are not saying "Take my privacy, I don't care, send me the service for free." They are saying "We want access to the information, we want some controls on what can be collected, what is done with the information, the ability to opt out of the entire tracking enterprise, and some clarity on what the policies really are, and we don't want those policies changed without our participation and permission." (The full report is available at knowprivacy.org.)

4. Latihan dan Jawaban

1) What ethical, social, and political issues are raised by information systems?

   Information technology is introducing changes for which laws and rules of acceptable conduct have not yet been developed. Increasing computing power, storage, and networking capabilities—including the Internet—expand the reach of individual and organizational actions and magnify their impacts. The ease and anonymity with which information is now communicated, copied, and manipulated in online environments pose new challenges to the protection of privacy and intellectual property. The main ethical, social, and political issues raised by information systems center around information rights and obligations, property rights and obligations, accountability and control, system quality, and quality of life.

2) What specific principles for conduct can be used to guide ethical decisions?

Six ethical principles for judging conduct include the Golden Rule, Immanuel Kant's Categorical Imperative, Descartes' rule of change, the Utilitarian Principle, the Risk Aversion Principle, and the ethical "no free lunch" rule. These principles should be used in conjunction with an ethical analysis.

3) Why do contemporary information systems technology and the Internet pose challenges to the protection of individual privacy and intellectual property?

Contemporary data storage and data analysis technology enables companies to easily gather personal data about individuals from many different sources and analyze these data to create detailed electronic profiles about individuals and their behaviors. Data flowing over the Internet can be monitored at many points. Cookies and other Web monitoring tools closely track the activities of Web site visitors. Not all Web sites have strong privacy protection policies, and they do not always allow for informed consent regarding the use of personal information. Traditional copyright laws are insuffi- cient to protect against software piracy because digital material can be copied so easily and transmit- ted to many different locations simultaneously over the Internet.

4) How have information systems affected everyday life?

Although computer systems have been sources of efficiency and wealth, they have some negative impacts. Computer errors can cause serious harm to individuals and organizations. Poor data quality is also responsible for disruptions and losses for businesses. Jobs can be lost when computers replace workers or tasks become unnecessary in reengineered business processes. The ability to own and use a computer may be exacerbating socioeconomic disparities among different racial groups and social classes. Widespread use of computers increases opportunities for computer crime and computer abuse. Computers can also create health problems, such as RSI, computer vision syndrome, and technostress.

5. Daftar Pustaka

1. Management Information Systems, Managing Digital Firm, 11th Ed, Kenneth C. Laudon, Jane. P. Laudon. (L&L)
2. Management Information Systems With Misource 2007, 8th Ed James A. O'brien, And George Marakas
3. Managing Information Technology 5th Edition Martin, Brown, Dehayes