

## **2 Privacy and Personal Information**

### **2.1 The Impact of Computer Technology**

#### **2.1.1 INTRODUCTION**

Computers are not necessary for the invasion of privacy. However, the use of computers has made new threats possible and old threats more potent.

Privacy is probably the “computer issue” that worries people most.

There are three key aspects of privacy:

- Freedom from intrusion—being left alone
- Control of information about oneself
- Freedom from surveillance

We give up some privacy for the benefits of dealing with strangers. We can choose to give up more in exchange for other benefits

We see a frequent tension between law enforcement and the privacy of innocent people.

*Personal information:* includes any information relating to or traceable to an individual person. It extends to any information from which a living individual can be identified.

#### **2.1.2 Risks of the Technology**

Computers and the Internet and World Wide Web make the collection, searching, analysis, storage, access, and distribution of large amounts of information much easier, cheaper, and faster than before.

We browse in libraries and bookstores with anonymity and can buy all sorts of magazines and newspapers for cash, but, on the Web, a record can be kept of every page we visit.

#### **INVISIBLE INFORMATION GATHERING**

*Invisible information gathering* describes collection of personal information about someone without the person’s knowledge.

Most people who used supermarket club cards now know they are trading a degree of privacy for discounts.

An Internet service provider (ISP) manages the connection between a user and the sites he or she is visiting. Thus the ISP “knows” every site we visit. Yahoo!, for example, collects four terabytes of log data daily.

*Cookies* are files a Web site stores on each visitor’s computer. A retail site may store the contents of our virtual “shopping cart” in a cookie. At first, cookies were controversial. Now more people are aware of cookies.

The software and sophisticated tools that Web sites use allow information about a visitor to be collected by advertisers on a site, not just the site sponsor itself.

DoubleClick, received people’s financial information from a Quicken Web site.

Some companies monitor the hard drives and search queries of people who use peer-to-peer systems to trade music and other files. QuickClick, a service of NBCi that enables the user to click on “any word, anywhere” and get information about it, collected more

than just the word clicked on and transmitted a user identification number with each selected word. A company offered a free program that changed a Web browser's cursor into a cartoon character or other image; millions of people installed the program, then later discovered that the program sent to the company a report of the Web sites its users, visited, along with the customer's serial number.

## **SECONDARY USE, COMPUTER MATCHING, AND PROFILING**

It is difficult for individuals to control their personal information if it is collected by one business, organization, or government agency and shared with or sold to others.

Sale of consumer information to marketers or other businesses

Use of numerous databases by the Internal Revenue Service.

Use of a supermarket's customer database to show alcohol purchases by a man who sued the store because he fell down.

*Computer matching* means combining and comparing information from different databases.

*Computer profiling* means using data in computer files to determine characteristics of people most likely to engage in certain behavior.

A few dozen federal agencies use computer profiling to identify people to watch—people who have committed no crime but might have a “propensity” to do so.

## **LOCATION, LOCATION, LOCATION**

Global positioning system (GPS) technology, satellites, and computer chips make it possible to track our movements and determine a person's current location.

Devices installed in rental cars, to locate them if they are stolen, can also be used to monitor or track drivers.

Some worry about abuse by government, saying that the government's ability to track and locate everyone by accessing the wireless telephone provider's system, the rental car system, and so forth, is a threat to our freedom.

### **2.2 “Big Brother Is Watching You.”**

Today, the government does not have to watch every move we make, because so many of our activities leave data trails in databases available to government agencies.

#### **2.2.1 Databases**

Government databases help government agencies determine eligibility for government jobs and benefits programs, detect fraud, recover payments on delinquent debts, collect taxes, and catch criminals.

The Privacy Act of 1974 and the Computer Matching and Privacy Protection Act of 1988 are two of the main laws that regulate the federal government's use of personal data.

The FBI kept files on civil rights activists, celebrities, and many other Americans.

The Internal Revenue Service (IRS) uses computers to match tax data on individuals and small businesses with a variety of federal and state government records.

In the 1990s, both the IRS and the FBI announced plans to drastically expand their databases.

The Selective Service bought the birthday list from a major ice cream parlor chain that gave free sundaes to customers on their birthdays. The list was used to find 18-year-old men who had not registered for the draft.

In 1996, Congress authorized millions of dollars to expand NCIC and link it to more databases.

Many government agencies, including the IRS, the FBI, and the INS, quietly found a way to access huge amounts of personal data not in their own databases: They buy personal information from private information service companies.

ChoicePoint culls data from the three big credit bureaus, numerous local, state, and federal government agencies, telephone records, liens, deeds, and many other sources.

In 2001, the firm had more than 10 billion records in its system. ChoicePoint's clients include at least 35 government agencies.

If the government is not allowed to collect certain data, then it should not be allowed to buy it.

The federal government maintains a database of people who have legally bought certain prescription medications.

### **BURDEN OF PROOF AND “FISHING EXPEDITIONS”**

Do databases and search technologies simply make the work of law-enforcement agencies more efficient, or do they fundamentally change the relationship between citizen and government?

### **OBEYING THE RULES**

Quis custodiet ipsos custodiet? (Who will guard the guards themselves?) - Juvenal

In 1996 Congress investigated a “secret” database maintained by the White House on 200,000 people with more than a hundred fields of data for each person, including ethnic and political information.

According to another GAO report, abuses of the FBI's NCIC by employees of law-enforcement agencies include selling information to private investigators, snooping on political opponents, and altering or deleting information.

A high-ranking IRS official was indicted for selling information from tax files.

A 1999 GAO report found that while the IRS had made significant improvements over prior years, the tax agency still failed to adequately protect people's financial and tax information.

Computers provide a new enormously powerful tool for investigation, surveillance, and intrusion into our personal lives. We should expect government to meet an especially high standard for privacy protection.

### **2.2.2 The Fourth Amendment and Expectation of Privacy**

## **WEAKENING THE FOURTH AMENDMENT**

Many laws allow law enforcement agencies to get information from nongovernmental databases without a court order.

The comprehensive federal medical privacy rules issued in 2001 allow law enforcement agencies to access medical records without court orders.

What level of access should the FBI have to the logs maintained by ISPs and Web sites we visit?

## **SATELLITE SURVEILLANCE AND THERMAL IMAGING**

Satellites use various computer technologies to take detailed photographs of the earth.

The constitutional status of searching by satellite remains open, and government agencies continue to use the images.

In 2001, the Supreme Court ruled that police could not use thermal imaging devices to search a home from the outside without a search warrant.

## **AUTOMATED TOLL COLLECTION AND ITEMIZED PURCHASE RECORDS**

Many bridges, tunnels, and toll roads now use automated toll-collection systems.

The database used for billing drivers contains a record of where and when a person traveled (and, in some cases, how fast).

They keep a detailed computerized record, 24 hours a day, of every vehicle using the system.

The head of the American Booksellers Association commented that “From a First Amendment perspective, having the government be able to go in and review an individual’s buying or reading patterns will have an incredible chilling effect.”

## **SUPREME COURT DECISIONS AND EXPECTATION OF PRIVACY**

*Katz v. United States*, in 1967: The court said that the Fourth Amendment “protects people, not places,” and that what a person “seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”

If we share information with businesses such as our bank, then we have no reasonable expectation of privacy for that information (*United States v. Miller*, 1976).

Should the capabilities of new technology give government agencies access to formerly private or ephemeral information without the protection of the Fourth Amendment?

### **2.2.3 More Search and Surveillance Tools**

#### **ELECTRONIC BODY SEARCHES**

Several airports use an X-ray device that displays on a computer screen the image of a person’s body without clothes.

Once the computer captures the image, it can store and copy it.

Among the people singled out as suspected drug smugglers and scanned by the machine at Kennedy Airport in New York in 2000, only 5% were actually carrying drugs.

Is routinely exposing images of our naked bodies to guards an acceptable trade-off of privacy for security?

The government is funding development of a variety of devices that can search through a person's clothing from a distance, without the person's knowledge or cooperation, to detect hidden weapons. These devices have valuable security applications, but the technology can be used for random searches, without search warrants or probable cause, on unsuspecting people. Clearly, guidelines are needed for acceptable uses of such machines.

### **WHO'S GOT YOUR PICTURE?**

Cameras alone raise some privacy issues. When combined with face-recognition systems, they raise even more.

The Tampa, Florida police used a computer system to scan the faces of all 100,000 fans and employees who entered the 2001 Super Bowl (causing some reporters to dub it Snooper Bowl).

There are more than 500,000 CCTV cameras in England, many outdoors in public places to deter crime.

Many applications of CCTV and face-recognition systems are reasonable, positive uses of the technology for security and crime prevention. How should we distinguish appropriate from inappropriate uses?

### **FIGHTING TERRORISM**

A face-recognition system will not stop a terrorist whose photo is not in the database of suspected terrorists.

The difficult task of choosing the right tools to use and the right trade-off between security and the privacy, freedom, and convenience of innocent people remains.

## **2.3 Consumer Information**

### **2.3.1 Databases and Marketing**

If you enter a contest or fill out a warranty questionnaire, information about you will be entered into a database and probably made available to direct marketers.

The ads you see on your computer screen while visiting certain Web sites are different from the ads seen by others; they are chosen for you by software, based on your previous activity at the site (or other sites).

A purchase of pasta or the fact that someone reads weather reports on the Web is not particularly personal or sensitive.

But would a customer be happy being on a list of people considered likely to buy a product for adults who are incontinent?

Would a customer be happy that a store has a record of how many packs of cigarettes, bottles of brandy, or contraceptives he or she buys?

Consumer data can leak in ways that can threaten people's safety.

### 2.3.2 Children on the Web

### 2.3.3 Credit Bureaus

### 2.3.4 Principles for Data Collection and Use

The first principle for ethical treatment of personal information is *informed consent*

After informing people about what an organization does with personal information, the next simplest and most desirable policy is to give people a choice about whether the data collected about them is distributed to other businesses or organizations and is used to send advertisements.

*Opt out and opt in.*

A policy of destroying records that are old or no longer needed protects privacy

#### **PRIVACY PRINCIPLES FOR PERSONAL DATA:**

1. Collect only the data needed.
2. Inform people when data about them are being collected, what is collected, and how it will be used. (Do not use invisible information gathering techniques without informing people.)
3. Offer a way for people to opt out from mailing lists and from transfer of their data to other parties.
4. Provide stronger protection for sensitive data. For example, use an opt-in policy for disclosure of medical data.
5. Keep data only as long as needed.
6. Maintain accuracy and security of data.
7. Provide a way for people to access and correct data stored about them.

## 2.4 More Privacy Risks

### 2.4.1 Social Security Numbers and National ID Systems

*The real danger is the gradual erosion of individual liberties through automation, integration, and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.*

-US. Privacy Protection Study Commission, 1977

Although the risks of careless treatment of SSNs is high, government and businesses have only recently begun to treat them with appropriate security.

When SSNs first appeared in 1936, they were for the exclusive use of the Social Security program. The government assured the public at the time that it would not use the numbers for other purposes. Only a few years later, in 1943, President Roosevelt signed an executive order requiring federal agencies to use the SSN for new record systems. In 1961, the IRS began using it as the taxpayer ID. So now employers and others who must report to the IRS require it. In 1976, state and local tax, welfare, and motor-vehicle

departments received authority to use the SSN. A 1988 federal law requires that parents provide their SSN to get a birth certificate for a child. The IRS requires taxpayers to report the SSN for each child over one year old claimed as a dependent (or provide other proof of the existence of the child). A 1996 law authorized use of SSNs for occupational licenses and marriage licenses. Although we were promised otherwise, the SSN has become a general identification number.

#### **2.4.2 Personal Health and Medical Information**

Information about alcoholism, sexually transmitted disease, psychiatric treatment, and suicide attempts is very personal. We might strongly desire to keep other health problems private even if they do not have negative social connotations.

Various database-access controls for computerized records increase a patient's privacy. On the other hand, many kinds of medical information in databases and on the Web face the same privacy risks as other personal data.

In 2001, after years of controversy, the federal government issued comprehensive medical privacy regulations, effective in 2003, covering both electronic and paper records.

Two proposals related to medical privacy and computer technology:

- Creation of a government or quasi-government national database containing health and personal information on virtually all Americans.
- Requirement for everyone to have a national electronic health ID card. The card would be used to verify a person's eligibility for health care, to store data, and to access medical records.

A national database and medical ID cards have significant privacy risks.

Privacy is threatened by the possibility that the Social Security number (SSN) will be used as the health identification number or that a health ID card will become a *de facto* national ID card.

If secure, unique, universal identification system is developed for health care, it would be hard for the government to resist using it as a replacement for the SSN.

#### **2.4.3 Public Records: Access vs Privacy**

Many government databases contain "public records," that is, records that are available to the general public. Examples include bankruptcy records, arrest records, marriage-license applications, divorce proceedings, property-ownership records (including mortgage information), salaries of government employees, and wills. These have long been public, but available on paper in government offices.

The federal Driver's Privacy Protection Act of 1994 prohibits unauthorized disclosure of state motor-vehicle-department records.

The Ethics in Government Act requires federal judges (about 1600 of them) to file financial disclosure reports.

Judges object that information in the records can disclose where family members work or go to school, putting them at risk from defendants who are angry at a judge.

Under the old rules, people requesting access to a judge's financial statement had to sign a form disclosing their identity.

Digital signatures might be routinely used in the future, but that raises another issue: How will we distinguish data that requires identification and a signature for access from data the public should be free to view anonymously, to protect the viewer's privacy?

## **2.5 Protecting Privacy: Education, Technology, and Markets**

### **2.5.1 Awareness**

The first step in protecting privacy from the risks of computer technology is awareness of how the technology works, how it is being used, what the risks are, and what tools are available to reduce exposure and unwanted uses of personal data.

### **2.5.2 Privacy Technologies and Market Responses**

#### **PRIVACY-ENHANCING TECHNOLOGIES**

Companies like Anonymizer.com and Zero-Knowledge Systems, Inc., provide services with which people can surf the Web anonymously, leaving no record of the sites they visit.

A well-designed database for sensitive information includes several features to protect against leaks, intruders, and unauthorized access by employees.

The computer system keeps track of information about each access, including the ID of the person looking at a record and the particular information viewed or modified. This is called an *audit trail*.

#### **PAYING FOR CONSUMER INFORMATION**

Many stores give discounts to shoppers who use cards that enable tracking of their purchases.

- Free PC
- ComScore Networks, Inc
- All Advantage

The success of these businesses shows that many people do not consider the intrusion of online ads to be extremely bothersome, nor their Web surfing to be particularly sensitive. They are willing to trade some privacy for other things. People who value their privacy more highly do not sign up.

Lauren Weinstein, founder of Privacy Forum, argues that less affluent people. To whom the attraction of free services may be strong, will be "coerced" into giving up their privacy.

#### **ARE BUSINESSES GETTING THE MESSAGE?**

It has become common for credit card companies Web sites, Internet service providers, cable companies, health companies, magazines, retail chains, and so on to have explicit policy statements about how they use the information collected from their subscribers and customers.

Web-site operators pay thousands, sometimes millions, of dollars to companies that do *privacy audits*.

IBM and Microsoft decided to remove their Internet advertising from Web sites that do not post clear privacy policies.

## **2.6 Protecting Privacy: Law and Regulation**

### **2.6.1 Philosophical Views**

#### **WARREN AND BRANDEIS: THE INVIOLEATE PERSONALITY**

Warren and Brandeis base their defense of privacy rights on, in their often-quoted phrase, the principle of “an inviolate personality.”

#### **JUDITH JARVIS THOMSON: IS THERE A RIGHT TO PRIVACY?**

Our rights to our person and our bodies include the right to decide to whom to show various parts of our bodies. By walking around in public, most of us waive our rights to prevent others from seeing our faces.

According to Thomson, our right to our person includes the right to decide who may listen to us. Someone who eavesdrops on our intimate conversations at home violates our right to our person. If we speak in public, we waive the right, and people may listen.

Thomson concludes, “I suggest it is a useful heuristic device in the case of any purported violation of the right to privacy to ask whether or not the act is a violation of any other right, and if not whether the act really violates a right at all.”

#### **APPLYING THE THEORIES**

How do the theoretical arguments apply to the privacy issues related to the vast amount of personal data in computerized databases and the practice of tracking our activities on the Web?

An important aspect of both the Warren and Brandeis paper and the Thomson paper is that of consent. There is no privacy violation if information is obtained or published with the person’s consent.

#### **TRANSACTIONS**

How to apply philosophical and legal notions of privacy to transactions, which automatically involve more than one person.

There is no clear reason for either party to the transaction to have more right than the other to control information about the transaction. If a confidentiality agreement is made, then the parties are obliged to respect it.

If control of the information about the transaction is to be assigned to one of the parties, we need a firm philosophical foundation for choosing which party gets it.

All transactions are really between people, even if indirectly.

The free-market view treats both parties equally, whereas the consumer-protection view includes arguments for treating the parties differently.

## **2.6.2 Contrasting Viewpoints**

### **THE FREE-MARKET VIEW**

Market supporters prefer to avoid restrictive legislation and detailed regulation for several reasons. They argue that the political system is a worse system than the free market for determining what consumers want in the real world of trade-offs and costs.

Market supporters argue that laws requiring specific policies or prohibiting certain kinds of contracts violate the freedom of choice of both consumers and businesses.

Consumers should have the freedom to sell personal data if they choose.

### **THE CONSUMER-PROTECTION VIEW**

Advocates of strong privacy regulation emphasize all the unsettling business uses of personal information we have mentioned throughout this chapter. They argue for more stringent consent requirements, strong limitations on secondary uses, legal restrictions on consumer profiling, and prohibitions on certain types of contracts or agreements to disclose data.

The ACLU's Privacy and Technology Project who urged a Senate committee studying confidentiality of health records to "re-examine the traditional reliance on individual consent as the linchpin of privacy laws."

Businesses sometimes don't follow their stated policies. All businesses must be required to adopt pro-privacy policies.

The consumer-protection viewpoint sees privacy as a right rather than something to be bargained about.

## **2.6.3 Contracts and Regulations**

### **BASIC LEGAL FRAMEWORK**

A good basic legal framework that defines and enforces legal rights and responsibilities is essential to a complex, robust society and economy.

We can apply the idea of contract enforcement to the published privacy policies of businesses, organizations, and Web sites. The Toysmart case is an example, Toysmart, a Web-based seller of educational toys, collected extensive information on about 250,000 visitors to its Web site, including family profiles, shopping preferences, and names and ages of children. Toysmart had promised not to release this personal information. When the company filed for bankruptcy in 2000, it had a large amount of debt and virtually no assets—except its customer database, which was valued highly. Toysmart's creditors wanted the database sold to raise funds to repay them. Toysmart offered the database for sale, causing a storm of protest. Consistent with the interpretation that Toysmart's policy was a contract with the people in the database, the bankruptcy-court settlement reached in 2001 included destruction of the customer database.

### **REQUIRING SPECIFIC CONSENT POLICIES**

The principle of informed consent can be incorporated into law in a variety of ways differing in their levels of control:

1. Businesses and organizations must clearly state their policy for use of personal information. If a person proceeds and makes a purchase, explores the Web site, provides information, and so on, consent to the policy is assumed.
2. Businesses and organizations must provide an opt-out option.
3. Businesses and organizations must use an opt-in policy.
4. Businesses and organizations must obtain consumer consent for each individual secondary use, disclosure, or transfer of their personal information.

## **REGULATION**

We must evaluate regulatory solutions by considering effectiveness, cost and benefits, side effects, and ease of use (clarity).

The actual laws that get passed often depend more on the current focus of media attention and special-interest pressure than on well thought-out principles and true cost/benefit trade-offs.

Regulations often have high costs, both direct dollar costs to business (and, ultimately consumers) and hidden or unexpected costs, such as loss of services or increased inconvenience.

## **OWNERSHIP OF PERSONAL DATA**

The concept of property rights can be very useful even when applied to intangible property (intellectual property, for example), but there are problems in using this concept for personal information.

Do you own your birthday? Or does your mother own it? After all, she was a more active participant in the event!

Facts cannot be copyrighted.

Judge Richard Posner argued that a person should not have a property right to “discreditable” personal information (e.g., one’s criminal history or credit history) or other information whose concealment aids people in misrepresentation, fraud, or manipulation.

## **PRIVACY REGULATIONS IN THE EUROPEAN UNION**

The European Union (EU) passed a comprehensive privacy directive covering processing of personal data. It defines “processing” to include collection, use, storage, retrieval, transmission, destruction, and other actions.

The general principles set forth in the directive include:

1. Personal data may be collected only for specified, explicit purposes and must not be processed for incompatible purposes.
2. Data must be accurate and up to date. Data must not be kept longer than necessary.
3. Processing of data is permitted only if the person consented unambiguously, or if the processing is necessary to fulfill contractual or legal obligations, or if

the processing is needed for tasks in the public interest or by official authorities to accomplish their tasks (or a few other reasons).

4. Special categories of data, including ethnic and racial origin, political and religious beliefs, health and sex life, and union membership, must not be processed without the subject's explicit consent. Member nations may outlaw processing of such data even if the subject does consent.
5. People must be notified of the collection and use of data about them. They must have access to the data stored about them and a way to correct incorrect data.
6. Processing of data about criminal convictions is severely restricted.

Some civil libertarians believe that the European Directive does not provide enough protection from use of personal data by government agencies.

The EU Data Privacy Directive prohibits transfer of personal data to countries outside the European Union that do not have an adequate system of privacy protection.