Indiana University
Multi-campus Modular
Computing Curriculum

Introduction to Computing

Module # 12: Computers and Privacy

Prerequisite Skills

- general concepts of computer databases and networks.

Goals

- Be alert to some of the ways in which computer information systems can be used to violate the privacy of individuals.
- Understand what is meant by "privacy" and why we have a right to it.
- Understand our legal and common sense options for protection of privacy.
- Act in a manner that respects the privacy rights of others.

1 Incidents

A woman in New York received a phone call from a man who was selling long-distance telephone services. When she told him that she only very rarely made long-distance calls, he said that telephone records showed she made frequent calls to Connecticut, New Jersey, and Delaware. The salesman hung up when the woman demanded to know how he had obtained her calling records. (Linowes 1993)

A man's wallet was stolen. The thief adopted his identity and became involved in a robbery and murder in Los Angeles. Later, when the real owner of the identity was stopped for a traffic violation, he was arrested because the Los Angeles Police Department's database identified him as a murder suspect. Although the man was released from jail within a few days, he was subsequently arrested five times in a period of fourteen months because of the same incorrect computer records. (Forester and Morrison 1994)

Computers make it possible to monitor the activities of people on the job on an unprecedented scale. At Electronic Banking System Inc., a "lockbox" service which processes payments and donations for companies and charities, computers measure the keystroke and error correction rates of data entry personnel. The pressure of the quotas (8500 keystrokes per hour), combined with other dehumanizing work conditions, causes tension, loneliness, stress-related illness, and feelings of paranoia. (Horowitz 1994) Electronic badges can track employee movements throughout the workday—including trips to the rest room. Email and voice mail can be read by employers.

Subscription lists to magazines, information from product registration cards, and records of credit card purchases are routinely sold to direct marketing organizations, which use the lists to mail advertisements directly to the homes of likely prospects.

Over 450 firms are engaged primarily in the business of buying, reprocessing, and selling data about individual Americans. The "big three" are the major credit bureaus, TRW Credit Data, Equifax, and Trans Union. (Forester and Morrison 1994) Together, these three credit bureaus maintain 400,000,000 credit records. (Laudon 1996)

Surveys of credit reports indicate that between 40 and 50 percent of reports from credit bureaus such as TRW Credit Data, Equifax, and Trans Union contain errors. A doctor in Norwich, Connecticut was refused a car loan because, according to his TRW credit report, he owed thousands of dollars in back taxes. When the bank investigated, it found that, because of an error by a TRW investigator, every taxpayer in Norwich was listed as having tax problems. (Linowes 1993)

The Medical Information Bureau (MIB) collects data from insurance companies and answers 15,000 inquiries per year. In one known case, a woman's MIB records incorrectly stated that she was HIV infected. Had she been denied life insurance on the basis of this misinformation, she probably would never have known the reason why. (Forester and Morrison 1994)

The FBI's National Crime Information Center (NCIC) contains records on eight million Americans, or one out of every thirty citizens. (Forester and Morrison 1994)

2 How Have Computers and Social Change Affected Privacy?

Computers have exacerbated the problem of privacy in several ways: size of databases, ease of exchanging data, ease of collecting data, and permanence of records.

The computerization of records makes it easy to store *very large* databases (more individuals in a database and more data about each individual). The computer also makes it possible to collect information which was not practical before, such as records of telephone calls, cable TV usage, credit card purchases, and, of course, whatever a person has been doing on the computer.

Computer networking makes it possible to *exchange* such information very easily. Once collected, data can be sold or traded, or freely given away. Errors sometimes spread more rapidly than they can be corrected. Computer data can also be stolen. The task of preventing data from being seen by those who are not authorized belongs to the art of computer *security*.

Computer records tend to be more *permanent* than paper records, because they take up far less space. Consequently, something a person did at the age of ten can remain on his computer record forever. If school records were made accessible to employers, insurance companies, and various government agencies, for example, there would be a danger that remarks about Johnny by his fourth-grade teacher, or testing in the ninth grade, might haunt him for the rest of his life. (Johnson 1985)

The large scale, exchangeability, and relative permanence of computerized databases about individuals is not all bad. Most of these records exist to serve a legitimate need: the need of businesses, government agencies, and other organizations to make informed decisions—decisions about hiring, giving credit, paying insurance benefits, issuing insurance policies, and so on.

In the "good old days," when most people lived in small communities, computer assistance was neither available nor needed to make such decisions. People knew each other, and what they didn't know from direct observation, they heard from their neighbors and acquaintances. Many business decisions were based on direct personal knowledge. The banker and the constable would have known that Huck Finn's Pap was a drunk. The "database" was a distributed and redundant neural system stored in people's heads; the "network" was village gossip.

This kind of personal knowledge no longer exists for a vast majority of Americans. It is not uncommon for a person born in Missouri or Indiana to move to California, then to Florida three years later, and a few years after that to Michigan. Most of us live in large cities; there are over 130 metropolitan areas with populations in excess of a quarter million. Even moving across town in Dayton or Indianapolis, let alone Chicago, would put us in a completely different social environment. The scale of businesses and government agencies has also increased. Large banks, insurance companies, and mail order firms can serve tens of thousands of customers all across the country. With the increasing scale of cities and organizations and the high mobility of twentieth-century life, the information that direct observation and the village grapevine can no longer supply is now provided by computer databases and networks. (Johnson 1985, Kling 1996b)

3 What is a Right to Privacy?

The "right to privacy" may mean different things to different people and in different contexts.

In one sense, it is the right not to be intruded upon in the privacy of one's home. This includes both the right not to be observed, and the right not to be bothered with unwanted "visitors," such as door-to-door and telephone salespeople. "A man's home is his castle." But computers are seldom used to invade the sanctuary of people's homes, so we will not discuss this further.

Warren and Brandeis (1890) argued that the common law recognized a kind of privacy right, namely a "right to be let alone," which they believed to be grounded on the principle of "an inviolate personality." By this, they meant a right to reserve one's thoughts and feelings from expression, or, if one chose to express them, to limit that expression to particular individuals or groups, such as one's close friends, family, or associates. For example, to publish someone's personal letters in the newspaper, or to publish a description of an unfinished work of art, or a catalog of a private collection of jewels or curiosities, without permission, would ordinarily be a violation of privacy understood in this sense. Such descriptions and catalogs may "show the bent and turn of the mind, the feelings and taste of the artist" or collector. They argued that this right extended beyond written and artistic expressions to "personal appearance, sayings, acts, and to personal relation[s], domestic or otherwise," and in general to "the facts relating to [one's] private life, which he has seen fit to keep private." A man may choose to conduct himself privately in a way which is quite harmless, but which, if it were publicly known, would subject him to ridicule, sarcasm, financial loss, ruin, or the embitterment of life. However, if privacy is a right to be protected, it does not depend on these possible evils; its justification is in the intrinsic dignity due to human nature.

Privacy violations may be more or less severe depending on the media used to publicize the information. Warren and Brandeis were primarily concerned about printed gossip which was, even in those days, appearing in the newspapers. They did not consider oral gossip to be such a serious matter, partly because it could not spread so far by word of mouth, would not ordinarily reach the ears of strangers, and partly because the person being gossiped about normally would not have the "pain and mortification" of knowing about it, unless it attacked his reputation. In one respect, computer data about individuals is like oral gossip: the person that the data is about does not ordinarily know about the data. Most of us have never seen our credit reports, medical records, or FBI files. In other respects, it is more like gossip printed in the newspaper: it is widely circulated, and may be seen by strangers. In yet another way, some computer data is unlike both oral and printed gossip: it is often not seen by human beings at all, strangers or otherwise. For example, direct mail advertisements are printed and addressed by computers from machine-readable files; it is extremely unlikely that any *person* has read the files on which these mailings are based. Considering that much of the "private" data which is collected about individuals is processed entirely by machines, we can conclude that, for these particular databases at least, computer data which touches one's *reputation* (e.g., credit worthiness or insurability) is the greatest cause for concern. However, the unauthorized revelation of thoughts and feelings may also be a matter of concern. It may seem that computer databases do not collect information about the thoughts and feelings about individuals, and they do not—directly. However, indirectly, a person's purchasing patterns, financial transactions, etc., say a great deal about the ways she thinks and feels. Even now, computer "data mining" programs are probably at work in scores of information bureaus trying to analyze these patterns.

More recent writers, who are concerned specifically with *computer-related* invasion of privacy, tend to define privacy as the right of individuals to control information about themselves (Johnson 1985, Kling 1996b). This right would include, for example, the right to limit access to their medical records, and the right to know about and to correct their credit reports. Individuals could want to control information about themselves because it is damaging (e.g., they have committed crimes), because it is irrelevant to a decision (an employer does not need to know your spouse's occupation in order to hire you), or because it is inaccurate. Apart from the consequences of use of information, many people want to control it because they feel that the facts of their lives are, as it were, their property. "People often feel wronged when the information about them is revealed even though the information is not damaging and the only consequence is that others now know what they did not know before." (Johnson 1985)

If I have a right to control the information about myself, it is obvious that that right is not unlimited. For example, if I have been convicted of a violent crime, my neighbors and potential associates have a right to know about it; it is, and must be, a matter of public record. If people were routinely able to control their credit records to the extent of hiding the fact that they failed to repay a loan, the whole system of buying on credit would quickly come to an end. Moreover, some information is more sensitive than other information and has more need to be controlled. What I say confidentially to my lawyer, to my doctor, or in the confessional is very private and deserves the highest level of protection. While my exact salary and bank balance is a secret that I treasure, a general idea can be formed of my financial situation merely by looking at the house I live in and the cars I drive. The number of my children and my tastes in literature and music are less closely guarded secrets, not really guarded at all, but it would be a shock to find an article about them in the newspaper or on the World-Wide Web. Finally, it would be ridiculous for anyone to have to ask my permission to tell another person about my general appearance, my profession, or where I live. There are degrees of privacy; some information is more confidential than other information.

If you haven't done anything wrong, do you have nothing to worry about? Well, there is certainly inaccuracy to be worried about. But even when there is no wrongdoing to hide and no inaccuracy, there is still the indignity of privacy intrusion. Everybody knows what married couples do in bed, and everybody knows what people do on the toilet, and everyone knows there is nothing wrong with these activities. Still, no human being wants to be observed or recorded doing them. (Dogs, on the other hand, don't care who's watching.) The respect due to human nature is violated by intrusions of this kind. Likewise, our personal thoughts and feelings, unless and to the extent that we choose to reveal them, deserve protection from unwanted snooping, electronic or otherwise.

4 What Can Be Done to Protect Privacy?

4.1 Legal Rights

In the U. S., the law on privacy derives from three sources: common law, the constitution, and federal and state legislation.

The Constitution does not explicitly mention a right to privacy. Nevertheless, the Fourth Amendment provides an important zone of privacy in "the right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures." This prohibits the police (without a warrant or probable cause) from searching computer files in our homes. Other privacy protections have been found in the Fifth Amendment (self-incrimination), the Ninth Amendment (rights reserved to the people), and the Fourteenth Amendment (due process of law). However, it's not *this* kind of privacy invasion that raises most concern in connection with computers.

Common law, in most states, has recognized four kinds of torts (grounds for civil lawsuits) involving privacy:

1. intruding upon solitude or seclusion;
2. appropriating a person's name or image for commercial purposes;
3. publicly disclosing private facts; and
4. publicity that puts a person in a false light.

The right to privacy in our homes is also protected by property law. Private individuals, just like the police, cannot search computer files in my home, but for a different reason: they would be trespassing.

Beginning in 1970, Congress has passed specific laws relating to privacy.

The *Fair Credit Reporting Act* (1970) aims to avoid reporting obsolete or incorrect credit information. The law provides that people must be informed why they have been denied credit. They have the right to challenge information kept by a credit rating company and to add information to the file. The credit company doeds not have to change data in its file just because it is challenged, but it must at least put in a statement of the person's point of view about it.

The *Freedom of Information Act* (1970) gives people the right to see any information about them collected by any federal agency.

The *Federal Privacy Act* (1974) says that the government must have a reason for collecting or disclosing personal information. The information cannot be used for another purpose without the consent of the individual whom it concerns. The agency which collects the information is responsible for its accuracy; individuals have the right to inspect their records, and may ask a judge to order an error to be corrected, if the agency does not do so. The act also prohibits any secret personal information systems run by the government.

The *Privacy Protection Act* (1980) protects materials (such as computer files) from search and seizure by the government if there is reason to believe the owner of the materials intends to publish them. (There are exceptions if a criminal offense is involved and for emergency situations.)

The *Electronic Communications Privacy Act* (1986) prohibits the "unauthorized interception and disclosure of electronic communications, while in transit or in storage" (Rosenoer 1997). The prohibition applies both to the government and to non-government organizations and persons. In effect, the law makes it illegal to "listen in" on someone else's email or other electronic communications. People whose messages are intercepted may sue for damages. There are certain exceptions for system operators. Also, note that internal email networks maintained by corporations may be exempt, i.e., employers may be allowed to monitor employee email, unless the company gave its employees a reasonable expectation that their email messages were private. Many government email messages are also excepted, as they are considered public records.

While not directly aimed to protect privacy, the *Computer Fraud and Abuse Act* makes it a crime to obtain unauthorized access to a computer system. This, of course, legally protects personal data (among other things) from "hackers" who break into a computer system.

Other federal laws include the Right to Financial Privacy Act (1988), the Family Educational Right to Privacy Act (1988), the Video Privacy Protection Act (1988), and the Cable Communications Policy Act (1984).

American federal legislation on privacy has been piecemeal. Only the federal government and a few specific industries (education, videotape rental, and cable TV) are affected. Medical, insurance, and employment records are completely unregulated. States have often taken a more aggressive legislative approach to privacy than the federal government, but all a privacy invader need do to circumvent state laws is move to another state.

Legal protection for privacy as affected by computer databases appears to be stronger in Europe than in the U.S. In the United Kingdom, for example, the Data Protection Act of 1984 requires individuals or organizations which routinely process personal data to register with the government, describing the kinds of data they collect and the uses they make of it. In most cases, individuals may obtain copies of personal information about them in computerized databases and can insist on corrections for incorrect or obsolete data. Victims of data misuse or error may complain to the Data Protection Registrar, as well as go to court—important, because lawsuits are an expensive way to obtain privacy. To resolve the problem, the Registrar may require the database owner to take corrective action or face criminal penalties (Forester and Morrison 1994). However, some observers question whether the stricter privacy laws in European countries have actually resulted in any greater privacy for their citizens, and propose, instead, a market-based approach to personal information (Laudon 1996)

4.2 Common Sense

Don't give away unnecessary personal information. If you are filling out a product warranty or registration card, and you don't want the whole world to know your income or hobbies, don't answer those questions.

Especially avoid giving away your social security number (SSN). Far too many databases are keyed by social security number. Once someone has your SSN, they can potentially get information about you from any of these databases (in part because data base owners tend to assume that anyone who knows your SSN is, in fact, you). Any government agency—federal, state, or local—that asks for your social security number must provide a Privacy Act Statement which tells you:

- Whether giving your SSN is required or voluntary;
- What statutory authority they have for asking for it;
- How they will use it; and
- What happens if you don't give it.

If giving your SSN is voluntary, it's your choice. If it's a non-government organization that wants to know your social security number, you normally have the option of not doing business with them, but there are often less drastic measures you can take. For tips on dealing with over-inquisitive organizations, see Hibbert 1996.

Check your credit reports *well before* you apply for a major loan. If there is an error, it can take months to get it corrected. You can get a free copy of your credit report from TRW by calling (800) 392-1122.

You can get a copy or a report of your file from the Medical Information Bureau. Their address is P. O. Box 105, Essex Station, Boston, MA 02112; telephone (617) 426-3660.

If you don't want to receive direct mail advertising and/or telephone sales calls, you can register your preference with the Direct Marketing Association at one or both of the following addresses:

- Mail Preference Service, P. O. Box 9008, Farmingdale, NY 11735.
- Telephone Preference Service, P. O. Box 9014, Farmingdale, NY 11735.

Some direct marketers fail to respect these preferences, especially for the telephone. But then you can feel quite free about telling them to go to hell.

4.3 Ethical Responsibilities of Computer Professionals, Managers, and System Users

Computer professionals designing systems that will contain individual, personal data—as well as managers and users of such systems—should always respect the privacy rights of those individuals. In particular, they should seek to:

- Avoid collecting unnecessary data.
- Allow data access only to authorized persons.
- Make sure the data are accurate.
- Provide individuals with the chance to review data about themselves, and to correct it if needed.
- Don't collect personal information for one purpose and then let it be used for some other purpose, without the consent of the individuals it is about.
- Dispose of the data after a reasonable period of time.

(Association for Computing Machinery 1992)

System designers should avoid using social security numbers (SSNs) as keys to databases if it is not necessary. SSNs are a poor choice for a database ID (see Hibbert 1997).

Invasive monitoring of employees by computer may be legal—for the present—but it certainly is not a move designed to foster good employer-employee relations.

4.4 Anonymity

Pseudonyms (i.e. "pen names") are widely used on the Internet, especially in some of the commercial online services. It is also possible to send messages anonymously, by sending them to an "anonymous remailer" which strips the message of all identifying information.

Pseudonymity and anonymity can be abused. For example, an anonymous defamatory message was sent to the Prodigy bulletin board in 1994, accusing Stratton Oakmont Inc., a securities investment banking firm, of "major criminal fraud" (Rosenoer 1997). Other immoral and illegal activities, such as sexual harrassment, personal threats, and money laundering, could be carried out by means of anonymous or pseudonymous messages.

However, it is important to realize that both anonymity and pseudonymity can provide considerable social benefits. Several famous authors are best known to us by their pseudonyms: Mark Twain, O. Henry, Voltaire, and George Eliot. Benjamin Franklin and Charles Dickens also wrote under pseudonyms. Anonymous political writing has also been important—for example, the Federalist Papers. People may choose to write anonymously, or using a pseudonym, for quite legitimate reasons, one of which is to preserve their privacy even as they express their views in public. The right to speak anonymously is part of the right to speak freely, which is protected by the First Amendment. Of course, this does not apply to non-protected forms of speech, such as libel, slander, and fraud. (Rosenoer 1997)

4.5 Encryption

Encryption is the act of encoding messages. The secrecy provided by encryption is required for secure messages for electronic banking and other financial transactions, as well as many other legitimate data communications. (It is also, of course, useful for spies, criminals, and terrorists.) To send a secret message, you would use a *key* to encrypt (encode) the message before sending it. A key is simply some pattern of digits used to guide the encryption algorithm. The receiver of the message would then use the key to decrypt (decode) the message at the other end.

In *public key encryption* schemes, there are two keys. The first key, called the public key, is used to encrypt the message. The other key, the private key, is used to decrypt. Importantly, the public key cannot be used to decrypt the message, only to encrypt. For example, if you wanted to send your bank a confidential message, you would first obtain the bank's public key. This would be easy to get, since it's public. Using the public key, you would encrypt the message and transmit it to the bank. The bank would then use its private key to decrypt the message it received.

An example of an encryption program, which is freely available, is PGP (TM) "Pretty Good (TM) Privacy"[1].

The United States National Security Agency has opposed the development of reasonable standards for encryption from the beginning. The U. S. government has also restricted the export of strong encryption technology. More recently, it has sought to promote "key escrow" arrangements whereby the government would keep, in effect, a spare key to everybody's encryption programs. Would you trust the government with your private key? Should you also keep a spare key to your house at the police station?

5 References

Association for Computing Machinery (1992). "Code of Ethics and Professional Conduct." *Communications of the ACM* 36 (Feb. 1993): 99–103. Reprinted in Kling 1996a.

Forester, Tom, and Perry Morrison (1994). *Computer Ethics: Catuionary Tales and Ethical Dilemmas in Computing.* MIT Press, 2nd ed.

Johnson, Deborah G. *Computer Ethics.* Prentice-Hall, 1985.

Hibbert, Chris (1996). "What to do when they ask for your Social Security Number."[2] A version of this appears in Kling 1997.

Horowitz, Tony (1994). "Mr. Edens Profits from Watching His Workers' Every Move." *Wall Street Journal*, Dec. 1, 1994, p. A11; reprinted in Kling 1996a.

Kling, Rob, ed. (1996a). *Computerization and Controversy: Value Conflicts and Social Choices,* Academic Press, 2nd ed.

Kling, Rob (1996b). "Information Technologies and the Shifting Balance between Privacy and Social Control," in Kling 1996a.

Laudon, Kenneth (1996). "Markets and Privacy." In Kling 1996a, pp. 697–726.

[1] http://web.mit.edu/pgp/

[2] http://snyside.sunnyside.com/cpsr/privacy/ssn/ssn.faq.html

Linowes, David F. (1993). “Your Personal Information Has Gone Public.” *Illinois Quarterly* 6: 22–24. Reprinted in Kling 1996a.

Orwell, George. *1984.* Harcourt Brace Jovanovich, 1949.

Rosenoer, Jonathan (1997). *CyberLaw: The Law of the Internet.* Springer-Verlag.

Warren, Samuel D., and Louis D. Brandeis (1890). “The Right to Privacy.” *Harvard Law Review* 4: 193–220.