

Does Everybody Know Your Name?

Be a Power Reader

Make a Web A concept web is a picture of related ideas. Draw a circle in the middle of a piece of paper. Write the word “Privacy” in the circle (“level 1 circle”). As you read the article, create more circles (“level 2 circles”) with key ideas and connect them to the main circle. You may even want to connect smaller circles to the level 2 circles.

When you are finished, you will have a “picture” of the article to review.

Introduction



Michelle wants to call an old friend in a different state, but has lost her friend’s telephone number.

So, she goes to a Web site that helps people locate phone numbers. She enters the friend’s name, city, and state. Up pops the needed phone number. This Web site is an example of a **database**. It contains virtually all the information in public telephone books in the United States.

Databases and Privacy

Databases have always been around. What makes things different today is that computers and the Internet make it much easier to pull information out of these databases. And many of them can be accessed by anybody who can get on the Internet.

Many people think these online databases are great time-savers. However, others feel that they are invasions of their privacy. You may wonder, “Exactly what does the word *privacy* mean?” This is a hard question to answer. For this article, we will define **privacy** as an individual’s rights regarding the collection, storage, and use of data about his or her personal traits and activities.

You may be surprised to learn that detailed files about you are kept in databases. People look at the information in these databases to make decisions that affect your life. Because these databases have such a major impact on your life, it is important that their contents are accurate. It is also important that only authorized people be allowed to use this information.

Government and School Databases

Information about you was probably stored in a database the very first day of your life. The hospital where you were born probably had a patient database. Data such as your sex, weight, and height were entered into this database. The hospital created a birth certificate, which was given to the government. This information was placed in another database. At school, your grades, class schedule, and attendance records are probably kept in a computer database.

When your parents or guardians applied for your social security number, they had to supply the government with information such as your full name, date of birth, and parents’ names. The information in this social security database will follow you the rest of your life.

A major purpose of the government is to collect taxes. On the federal level, taxes are collected by the Internal Revenue Service (IRS). The IRS keeps enormous amounts of information on taxpayers. This information includes the amount of money a person earned in a specific year and the amount of taxes he or she paid. The IRS uses a person's social security number to keep track of these records. If this detailed financial information were to get into the wrong hands, it could be disastrous.

Credit Reports

When you get older, you may want to get a credit card. When people buy houses, they usually get a mortgage (a long-term loan to help buy property). Credit card companies and banks only want to lend money to people who are going to pay it back. So, they look at your credit report.

A **credit report** lists information such as any credit cards a person may have, how much he or she owes on these credit cards, and whether he or she makes payments on-time. Special credit reporting agencies keep all this information in databases. Only people who need this information for legitimate business purposes are allowed to access these databases.

It is important that the information in a person's credit report is accurate or he or she may not be allowed to borrow money.

Medical Records

It used to be that hospitals, doctors, and dentists had large rooms filled with nothing but filing cabinets. Each patient had a file folder. Some patients' files might have been several inches thick.



Healthcare workers used to keep patient information in paper files.

Today most healthcare providers store this same information in computer databases. Medical databases speed up our healthcare. They also reduce errors. If a doctor orders a blood test, the results can be entered directly into your database record. Some of these databases can even store images such as X rays.

Doctors must get your permission before releasing your medical records to anyone else. Medical records in computer databases must be carefully protected from people who are not authorized to use them.

Security and Protection

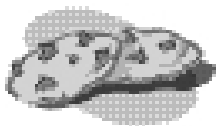
Some databases, such as the one Michelle used to find her friend's phone number, are public. Anybody can use them. Other databases are only to be accessed by authorized users. The people or group maintaining the database must make certain that only authorized people can access the data. For example if your school keeps your records in a computerized database, it is obligated to make certain that only authorized users (such as administrators and teachers) can access the database. The most common way of doing this is to require the user to enter a user ID (or account number) and a password. Only if a registered user ID and password are entered is the person allowed to use the database.

Hackers are people who access computer systems without authorization. Unfortunately, sometimes hackers are able to break through these security measures and access databases. This is especially true if the database can be accessed over the Internet. Hacking is illegal. Many young people have gotten in serious trouble for hacking. Besides, it's just wrong. If you know someone who has done hacking, explain to him or her how serious it is. Special computer applications, called **firewalls**, have been developed to keep hackers from using the Internet to illegally enter computer systems.

Online Privacy

Did you know that someone may be watching your every move while you're online?

Who Wants a Cookie?



We all know what's in the cookies we eat: flour, sugar, eggs, shortening, maybe chocolate chips.

But, there's another kind

of cookie that's used on the Web. This **cookie** is a small file that's stored on your computer's hard drive. When you go to some Web sites, a cookie may be placed on your computer. The file contains information about you. For example, if you go to a Web site that sells books, it can keep track of every book you've bought there. The Web site can then be "customized" according to your interests. For example, if you've bought several books on hockey, the site may show you a list of new hockey books that have just come out.

Cookies can contain other information. Many Web sites ask you whether you want them to "remember" your name and password. If you say yes, this information is stored in the cookie. The next time you go to the site, it will pull the information from the cookie. You will be logged on automatically. The cookie can also store a person's address and credit card information so that he or she does not need to enter them each time he or she places an order.

Some people think cookies are an invasion of our privacy. Web browsers such as Internet Explorer and Netscape Navigator can be set so that they will not allow your computer to accept cookies. However, many people put up with them because they make using the Web more convenient. You will have to decide whether this convenience is worth any loss of privacy.

Internet Spies

There's a special type of software that keeps track of the Web sites you surf, how much time you spend at each site, and how

much money you spend there. All of this is done without your even knowing about it. It's called **spyware**.

Spyware may be downloaded onto your computer's hard disk from a Web site you have visited. If you download free software from a Web site, it may have spyware hidden in it. After following your online actions for a while, the spyware "reports home."

Companies use this information for many purposes. One is to send you e-mail advertisements based on what they've learned about your interests. Some companies even make money selling the information to other businesses. For example, if you visit music Web sites, your e-mail address may be sold to companies who sell CDs or stereo equipment. Pretty soon you're receiving e-mail advertisements about Web sites' specials on CD players! This is one reason that we receive so much **spam** (junk e-mail).

Fortunately, if you are concerned about spyware, there are applications you can download that will protect you against spyware.

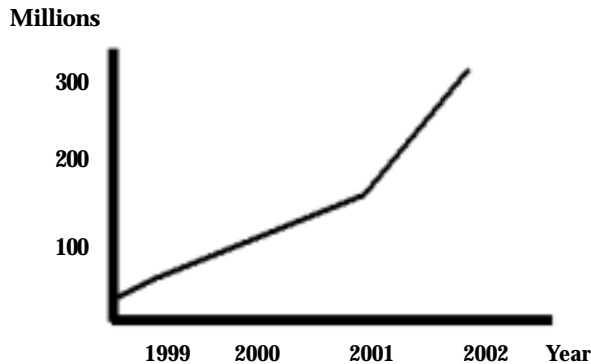
Identity Theft

Vic Sanchi is a doctor in the Midwest. One day, he began getting bills for credit card accounts that he had never opened. It turned out that someone had opened four different credit card accounts in his name. Apparently, the person had gotten enough information (maybe from stealing his mail or going through his trash) to open these accounts. Over three months, the person charged more than \$40,000 worth of goods on the Internet. It took Dr. Sanchi over a year and many hours of his time to straighten out the mess.

Dr. Sanchi was a victim of **identity theft**. Identity theft involves pretending to be someone you are not. For example, a person may steal someone's credit card numbers and use them to purchase items on the Web. Or the thief may get enough information about a person (such as a

social security number, birth date, address, and so on) in order to get false documents such as a driver's license.

The thief can then use these documents to cash checks or charge items to the person's credit cards. There were over one-half million victims of identity theft in 2001, and each year the number is growing.



Losses because of identity theft are increasing.

Identity theft has always been around. However, the Internet makes it easier to do. Thieves can use the Internet to locate information about individuals. When making a purchase online, the seller does not know that a 20-year-old man is using a 60-year-old woman's credit card.

What Can You Do?

Americans like convenience. We want to be able to go online to transfer money from a checking account to a savings account. We want to make online purchases with our credit cards. Fortunately, there are some things you can do reduce the chances of someone stealing your identity.

- When you are conducting a financial transaction on the Internet, make sure that you are using a secure site. You can identify a secure site by the small yellow padlock in the lower-right corner of the window.

- Guard your social security number. Don't give your social security number to anyone unless you believe he or she has a legitimate need for it.
- It is best only to make online purchases from sites that you have (or someone you trust has) previously used.
- Don't give credit card information over the telephone or on the Internet unless you know and trust the people you are dealing with.

Your parents and teachers may have other suggestions for you. As you get older, you will learn additional ways to protect yourself.

There may come a time in your life when you will be working with sensitive information. For example, you may have access to the employee records for a company where you are working. You will want to be careful to follow any rules regarding accessing this database. For example, you may have access to records that show how much money different workers are earning. You should not share this kind of information with other people. You also will want to guard your account number and password. In short, guard other people's privacy as you would want your own guarded.

Watchdogs

We all know that a watchdog is a specially trained guard dog that protects something valuable, such as a home or business. There are also groups that act as watchdogs for our privacy. These organizations want to make certain that people aren't getting information about us that they should not have. Three of these organizations are the Electronic Privacy Information Center (EPIC), the Electronic Frontier Foundation, and Privacy.org.

These organizations warn us when they believe others are infringing on our right to privacy. They try to make certain that the government enforces laws concerning who can access certain types of information. They also encourage the government to pass laws that will keep certain information private.



Many organizations fight to protect people's privacy.



Review Questions

1. Lists three types of databases that probably contain information on you.
2. What are some of the things you can do to reduce the chances of being a victim of identity theft?
3. In your own words, define the word *privacy*.
4. What is spyware? What is its purpose?
5. What is a credit report? For what do businesses use credit reports?



What Do You Think?

1. Can you think of any additional things you can do to prevent your identity from being stolen? Can you think of anything businesses can do to reduce the amount of identify theft?
2. What do you think about cookies? Are you for or against them? Why?
3. This article talked about spyware being used mainly by businesses to try to sell us items. Can you think of any other ways spyware might be used?

Glossary

cookie A small file that a Web site stores on your hard drive. It contains information such as how often you visit the site, what you have purchased from it, and possibly ordering information such as your address and credit card number.

credit report A record listing information such as the kinds of credit cards you have, how much you owe on these credit cards, and whether you make your payments on time.

database A group of records that can be accessed in many different ways. Each record contains a collection of information, such as all the available information on a single individual.

firewall An application that prevents an outsider from accessing your computer over a network such as the Internet.

hacker Someone who accesses computer systems without authorization. Hacking is illegal.

identify theft Pretending to be someone you are not, usually for financial gain, such as illegally charging items to that person's credit cards or withdrawing funds from his or her checking account.

privacy An individual's rights regarding the collection, storage, and use of data about his or her personal characteristics and activities.

spam E-mail that is sent to you without your requesting it; it is usually trying to sell you something.

spyware Applications that are installed on your computer's hard drive without your knowledge. They then track your behavior while you are on the Internet and report back.