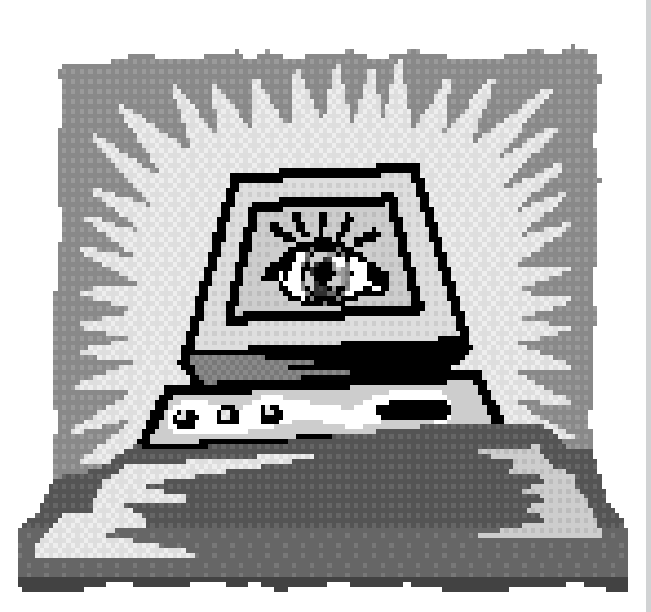
'Leave me alone!'



Your privacy online—and offline

Privacy Information
A Consumer Action Project

'Top Ten' ways to protect your privacy

• Pay an extra fee to have your phone number unlisted. Register your home and cell phone numbers with the National Do Not Call Registry (www.donotcall.gov).

• Get free copies of your credit report every year at www.annualcreditreport.com. Check it for errors and signs of identity theft.

• Screen cookies (page 6) or use a secure anonymous remailer site when you surf the Internet (page 7).

• Read the privacy policies on web sites before you do business or fill out forms on the sites, especially if the forms ask for personal information.

• Opt out of Direct Marketing Association members' direct mail campaigns and bulk e-mail servers (page 11).

• Call 888-5-OPTOUT (888-567-8688) to remove your name from credit reporting agency prescreening programs and stop receiving pre-screened credit and insurance offers.

• Tear up or shred documents that contain your name, address, Social Security number or bank or credit card account numbers before throwing them in the trash. At home and at the office, keep personal information in a locked drawer.

• When using a cell phone, payphone or your lap top computer in public, be conscious of anyone trying to overhear or see confidential information.

• When traveling, do not put your home address on your suitcase—just your phone number.

• Create strong passwords that can't be easily guessed to protect your financial accounts and phone records. Use random letters, numbers and symbols in the passwords.

What is privacy?

The legal right to privacy has been recognized in the U.S. since the late 1890s, but its roots go back much farther. The importance of privacy is spelled out broadly in the Bill of Rights, which limits the government's ability to interfere with individual liberty and recognizes our right to be left alone. While not specifically mentioned in the Constitution, it is generally accepted that U.S. residents have a right to be left alone and to be free of unwanted public scrutiny. The First Amendment protects an individual's freedom to speak, think, assemble, organize, worship and petition without government or private interference. The Fourth Amendment limits government intrusion into our "persons, houses, papers, and effects" and the Fifth Amendment protects against self-incrimination and keeps the government from forcing us to reveal private information.

Since Sept. 11, 2001, many serious concerns have been raised about the balance between personal privacy, civil liberties and national security. In the Internet age, questions also arise about the impact of marketing and sales on our privacy. Aided by computers and the Internet, today's marketing companies collect information from a variety of sources with a speed and efficiency that was not possible even a decade ago.

Some companies place a high importance on privacy, and refuse to sell or share the names, addresses and account information of their customers. But they are in the minority. Today, information is

currency bought and sold on the open market, and it may include details about you and your family, your job, your money, your health and your hobbies. Often, companies that have gathered such facts during sales and other transactions believe they own this information. The information collected about you usually winds up in databases used for marketing purposes, and may lead to your receiving countless solicitations by mail, telemarketing, faxes and e-mail. Reputable companies will allow you to remove your name from marketing lists ("opt out"), but in many cases you must take the initiative of doing this on a company-by-company basis.

What's so bad about collecting personal information about me?

Many people object on principle to the idea that information is collected about them—even if it is never used. They question why companies are permitted to collect and sell facts about what they buy or what hobbies they have, especially if they don't want the companies to do so.

You might not mind getting offers for credit cards in the mail, or hearing about travel opportunities over the phone or by fax. However, many people do object to marketers calling them at dinner time, filling their mail boxes with junk mail or sending annoying unsolicited bulk e-mail pitches ("spam"). If telemarketers annoy you, the law gives you the right to ask them to stop calling and to remove your name from their lists.

But unfortunately, you can't opt out of fraud and criminal activities. Unscrupulous individuals could be accessing information about you in company databases and files and using it to rip you off. There are many ways that crooks misuse personal information. Identity theft is a rapidly growing crime. With key facts about you, such as your name, address and Social Security number, impostors can establish credit in your name and charge goods and services —leaving you to unravel the damage. Thieves create unauthorized credit card transactions and forged checks to steal money from a victim's bank. Employees pilfer records from companies and sell

them to criminals. Your personal information can even help burglars find out when you are not at home so they can rob your house. By gaining access to phone numbers or credit card account numbers, unscrupulous companies could make bogus charges to your accounts ("cramming").

Privacy in cyberspace

Privacy & e-mail

The law recognizes few privacy rights in e-mail sent or received by an employee at work—even if the mail is personal. Even if your employer is not peeking at your messages, e-mail can easily end up in the wrong hands. Follow these tips to protect your privacy when using e-mail:

• Use caution when you hit "reply" or your message may go to people you did not want to receive it.

• Use a password to protect your account. A password will keep others—but not your employer—from accessing your e-mail account. Make sure your password is a strong combination of upper and lower case letters, numbers and symbols.

• Quit your e-mail program when not in use. Someone could read your mail, or use your account to send threatening messages.

• Consider using separate e-mail accounts. Use one on the Internet and one for personal or job-related communications.

• Opt out of spam messages. Reputable commercial e-mail offers have information on how to "unsubscribe." If not, you may be dealing with a disreputable marketing company. Don't reply to spam e-mails—by replying you will confirm that your e-mail address is valid, which may lead to more spam. To learn more, visit the FAQ section on the Coalition Against Unsolicited Commercial Email web site (www.cauce.org).

• Phishing is an e-mail fraud in which legitimate-looking e-mails are sent to trick recipients into giving out personal and financial information. These e-mails ask you to "confirm" personal information such as account numbers or passwords. The bottom line is, legitimate companies don't ask for personal information via e-mail. Forward phishing e-mails (and other suspicious e-mails) to the Federal Trade Commission at spam@uce.gov and to the company being impersonated.

• Opt out of e-mail offers when you purchase something online, or register for a web site.

• For sensitive e-mails, use cryptography software. There are software products that will put your e-mail messages in secret code ("encrypt") so that they cannot be read by anyone but the intended recipient. Pretty Good Privacy (PGP) encryption software is free for non-commercial use. To learn more about PGP and download the encryption software, visit www.pgpi.org.

Privacy on the Internet

As you surf the Internet, you are being tracked by organizations who want to know where you go, how long you stay and whether or not you sign up or buy something while visiting a web site.

Taming the cookie monster

Information on the Internet is gathered by "cookies," tiny electronic files that web sites put on a visitor's hard drive so that the site can remember things about the visitor: favorite stocks, username and password, or preferences in news topics, for example. Per-session cookies are stored in memory and are only available while you are on the web site and are deleted from your cache when you leave the web site.

A cookie identifies your computer by its "Internet protocol" (IP) number. Marketing companies known as "data miners" have found a way to link IP numbers with names, addresses and other information about you to create targeted marketing lists.

Some companies in the business of targeted behavioral advertising track users online using persistent cookies stored on your hard drive. The Network Advertising Initiative (NAI) has a "one stop" tool that allows you to opt-out of advertising by member networks. (Not all online advertising firms belong to NAI.) Go to www.networkadvertising.org, where you can check which ad networks have placed a cookie on your hard drive, and then submit opt-out requests for each network you prefer not to be targeted by. This must be done on all the computers you use.

You also can turn off cookies by going to the help section on your Internet browser program, such as Internet Explorer, Firefox or Safari, and follow the directions to disable or block cookies. However, if you disable cookie files, personalized web sites you have registered with will no longer recognize you and you may find it difficult to access certain sites.

Hide your identity

"Secure anonymous remailers" allow you to access web sites using a buffer between your own computer and the Internet, called "proxy" surfing. These services generally offer a range of monthly and yearly fees and include Anonymizer (www.anonymizer.com), Ultimate Anonymity (www.ultimate-anonymity.com), and FindNot (www.findnot.com).

Read the fine print

Reputable web sites will post their privacy policies in a prominent position. Most links to a company's privacy policy can be found on the home page (sometimes at the very bottom of the page) or in an "About Us" section. If you are going to do business on a site, or even register so that you can access free information, read its privacy policy. The policy should explain how the site will use

any information you provide and if there is any way to opt out of marketing programs. Lack of any privacy policy may be a red flag about the way a site views the rights of its visitors. However, some sites with prominently displayed privacy policies do nothing more than notify visitors that their information will be used for marketing, with no provision for opting out.

A seal of approval

Online "trustmarks," such as Trust-E (www.truste.org), Verisign (www.verisign.com), and BBB Online (www.bbbonline.org) help consumers screen web sites. (Just because a site bears one of these seals does not mean that it will provide the level of privacy you want.) Online seals should not be taken at face value, as they can be forged. You can test if a seal is valid by clicking on its symbol and matching the address of the site you are currently visiting to the one shown on the verification report.

Under lock and key

When you bank or buy things on the Internet, verify that your browser (Internet Explorer, Firefox, Safari, etc.) is in secure mode by looking at the web address bar. If secure, the web site address (URL) should begin with "https" (with an "s") instead of "http." In some browsers, you will see a tiny closed padlock or a key if you're secure. Most banks and sites that handle financial transactions and credit card sales post their security requirements on site. Unless your computer and browser meet the minimum security requirements, you will not be able to bank with or buy things from certain sites. You can usually upgrade your browser for free from the Internet.

Plastic protection

Use a credit card instead of a debit card when shopping online. When you use a credit card, $50 is the most you will ever be liable for because of fraud or unauthorized use. By law the liability for debit card fraud can be much higher, even unlimited in certain circumstances. Debit cards that have the Visa or MasterCard logo come with those companies' voluntary pledge to protect consumers from fraud. But unauthorized access to a debit card could wipe out your checking account and any other accounts you have linked to it, and could require that you wait a week or more for your money to be refunded.

Safeguarding your privacy

Restricting information collected about you

There are many ways to limit or control some of the information that is collected about you, but it's probably impossible to keep everything a secret. In order to guard your privacy in today's society, you will have to be vigilant and assertive in your day-to-day dealings with businesses.

Your Social Security number must be provided to certain government agencies, including tax authorities, the Social Security Administration and Medicare. Financial institutions are required to obtain each customer's Social Security number, but many businesses use this number to identify a customer when they don't have to. Any time you are asked for your Social Security number, question what it will be used for and if it's really needed. Sometimes another number or secret code can be substituted.

Before you do business with a company, find out its policy on selling or sharing customer data and whether you can opt out. Ask for a full explanation of the company policy—if an employee doesn't know, ask to speak to a supervisor. Once a company has sold information about you and your transactions to marketing firms, it can be too late to remove your name from marketing lists.

Marketers also cull information from warranty registration cards, product inquiries, online registration forms and surveys. Don't fill out questionnaires and contest and sweepstakes forms. To retain a product warranty, don't send back the registration card—just save the purchase receipt and any product numbers from the

box. This way you will have the information you need to prove that the product is still under warranty.

The three major credit reporting agencies, Equifax, Experian and Trans Union, allow you to opt out of having your credit file used for pre-screened credit offers. Call 888-5-OPTOUT (888-567-8688). Doing this will stop most offers from credit card companies and other lenders.

Another way to remove your name from some lists is to contact the Direct Marketing Association (DMA) to opt out of its members' direct mail and e-mail marketing solicitations. This also keeps member companies from selling your name to third parties. Go to DMA Choice (www.dmachoice.org) to learn more.

- To stop some junk mail, send your name and address to DMA Mail Preference Service, P.O. Box 9008, Farmingdale, NY 11735 or register online at www.dmachoice.org.
- To remove your e-mail address from DMA members' e-mail lists, go to its special e-mail opt-out page (www.ims-dm.com/cgi/optoutemps.php).

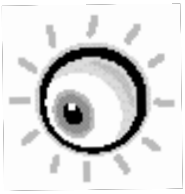
To stop telemarketing calls, add your phone numbers (landline and cell) to the National Do Not Call Registry (www.donotcall.gov).

You can sue telemarketers in small claims court if they call you before 8 a.m. or after 9 p.m. or after you have asked to be on their do not call lists. For each violation, you can sue for $500. For more information, you can purchase Private Citizen's guide, "So You Want to Sue a Telemarketer" (http://privatecitizen.com; 800-CUT-JUNK).

Unsolicited sales communications sent by fax must by law contain a toll-free number you can call to have your name removed from future fax broadcasts.

If you are concerned about having your number in the phone book, your phone company will remove it from the directory for a small fee. On the Internet, check online directories such Anywho.com, Switchboard.com, Whitepages.com, ReversePhoneDirectory.com, Phonenumber.com and Smartpages.com and "people finder" links on search engines such as Google.com and Yahoo.com. (If you have an unlisted number, it won't be there.) Many sites allow you to remove your number—check the privacy policy or help section. Removing your phonebook listing from one site, such as Google, will not remove your personal information from other web sites.

The law allows financial institutions to share information about you with businesses they own or have a share in, with government agencies and with other firms that provide services such as preparing and mailing your monthly statement. You can ask financial institutions not to share your information for marketing purposes. You can ask other companies you do business with to do the same, but there is no guarantee that they will honor your request unless they are members of the Direct Marketing Association.



Federal law gives credit reporting agencies (CRAs) the right to keep information about your credit history on file. Only companies with your permission or a permissible purpose—usually credit, employment, tenant-related or insurance—may access your credit file.

Government and law enforcement agencies may legally keep information on file about you. In some cases, this is "public information" and marketers have access to it. With a subpoena or court order, law enforcement agencies may obtain search warrants to search your person, home, office or car. In some cases, law enforcement needs only a "probable cause"—often a subjective belief or even a hunch on the part of a police officer—to perform a search.

Should you restrict your information?

It's your choice whether or not to buy things online, disable cookie files and opt out of marketing programs. Retailers and marketers often point out the "drawbacks" of opting out: you will miss out on good deals, "freebies," sales and offers of personal interest. Some people like browsing the retail catalogs that clog our mail boxes; others find them annoying; others point to the overall waste of paper. (Catalog Choice—www.catalogchoice.org—is a new service to help you opt out.)

Even if you are dedicated to opting out of every marketing program possible, of asking every magazine you subscribe to not to sell your name and surfing the web through an anonymizer program, chances are you can't stem the tide of databank technology. Every time you use your credit card or pay your property taxes, another bit of information about you gets added to a databank somewhere, and under current law there's nothing you can do to stop it.

For information and assistance

Government agencies

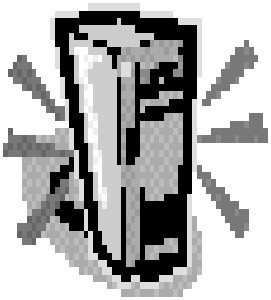
The Federal Trade Commission (www.ftc.gov) has law enforcement responsibilities under the Fair Credit Reporting Act, which provides certain privacy protections for consumers by limiting access to consumers' credit reports. Under the agency's mission to protect consumers from deceptive marketing, it monitors data collection disclosure practices on the Internet. It also provides help for victims of identity theft. (www.ftc.gov; (877) FTC-HELP)

Consumer advocacy organizations

Most of these organizations prefer to provide information to consumers over the Internet. Your local library probably offers Internet access if you don't have it at home.

American Civil Liberties Union (www.aclu.org). Provides a wealth of privacy-related information on "cyberliberties," workplace rights, data collection and wiretapping.

Center for Democracy & Technology (www.cdt.org). Works to promote democratic values and constitutional liberties in the digital age. Its Opt-Out site (http://opt-out.cdt.org) lets you create personalized letters to print and mail.



Consumer Action (www.consumer-action.org). Provides nonlegal advice and referrals on consumer problems if you leave a message at (415) 777-9635 or (213) 624-8327; TTY answering machine: (415) 777-9456. Chinese, English and Spanish are spoken. For advice and referrals via e-mail, write to: hotline@consumer-action.org.

Electronic Frontier Foundation (www.eff.org). Works to raise public awareness about civil liberties issues, including privacy, centering on computer-based communications media.

Electronic Privacy Information Center (www.epic.org). Maintains an extensive list of privacy resources, including state privacy laws, pointers to privacy resources on and offline, tips for surfing anonymously and using encryption programs and anonymous remailers.

Junkbusters (www.junkbusters.com). Promotes consumer education and methods "to free the world from junk communications."

Privacy Rights Clearinghouse (www.privacyrights.org). Works to raise consumer awareness of how technology affects personal privacy, offers tips on privacy protection, responds to specific privacy-related complaints from consumers and, when appropriate, refers them to the proper organizations for further assistance.

National Fraud Information Center (www.fraud.org). Advice and referrals about scams and many forms of fraud from the National Consumers League (NCL).

Industry alliances

Better Business Bureau (www.bbb.org). Local chapters of the Better Business Bureau provide consumer reports on businesses and charity organizations, resolve consumer disputes and promote voluntary ethical business standards and self-regulation by member businesses.

Direct Marketing Association (www.the-dma.org). A trade association for database marketers, it allows companies to display its logo only if they honor consumer requests to opt out of marketing programs through its mail, telephone and e-mail preference services.

TRUSTe (www.truste.org). Web sites that are allowed to display the TRUSTe seal must have a privacy policy that meets TRUSTe guidelines and agree to settle any disputes with customers using TRUSTe's alternative dispute resolution process.

VeriSign SecureSite (www.verisign.com). Users can click on the seal to verify a web site before submitting confidential information.

About this publication

This publication was created by Consumer Action and has been revised and updated with funding from Consumer Action's Privacy Information Project.

This publication is available in Chinese, English and Spanish. Community-based organizations may order free bulk copies. For more information, visit our web site, and click on "Publications," or e-mail us at info@consumer-action.org.

Consumer Action

www.consumer-action.org

221 Main St., Suite 480

San Francisco, CA 94105

(415) 777-9635

523 W. Sixth St., Suite 1105

Los Angeles, CA 90014

(213) 624-8327

e-mail: info@consumer-action.org