

Protecting Your

PRIVACY



**How to safeguard your
personal information**

**Maryland Attorney
General's Office**

J. Joseph Curran Jr., Attorney General

**J. Joseph Curran,
Jr.
Attorney General**



Almost every time you make a purchase, use the Internet, or have a prescription filled, a record of the event is entered into a database. That information can be, and often is, sold and traded to marketing companies, and is vulnerable to being accessed by those with criminal intent.

This availability of your personal information can result in your being inundated with telemarketing calls, direct mailings, and unwanted e-mail. Exposure of your financial information can lead to identity theft and credit fraud. Of even greater concern, your children's privacy can be invaded as they surf the Internet, which can result in their being targeted by marketers or, worse, sexual predators.

While it's not possible to keep your personal information entirely private, there are ways you can limit who has access to it. This brochure contains a variety of practical steps you can take to protect your privacy and that of your family.

A handwritten signature in black ink, which reads "J. Joseph Curran, Jr." The signature is written in a cursive, flowing style.

Protecting Your **PRIVACY**

Inside

Protecting Your Privacy: Practical Steps..... 4

Limit the information you give out in everyday transactions

Using Caution on the Internet..... 9

Reduce the information that is collected about you online

Avoiding Identity Theft..... 13

Be protective of your financial information

Safeguarding Your Children Online..... 18

The law, filtering tools, monitoring, and talking with your kids

Resources..... 24

Where to find help

Protecting Your Privacy: Practical Steps

Be assertive in guarding your personal information. Here are ways to do that on an everyday basis:

Limit the personal information you give out. When filling out forms or making a purchase, only give the information that is absolutely necessary. If you don't understand why the information is needed, question it. Also ask if the information will be shared with third parties.

Protect your Social Security number. Don't carry your Social Security card in your wallet. Don't print the number on your checks. Give your Social Security number only when absolutely necessary—ask to use other types of identification when possible.

Don't leave personal information where others can see it. At home, be cautious about where you leave personal information such as bank statements, particularly if you have roommates, employees in the home, or are having service work done to your home.

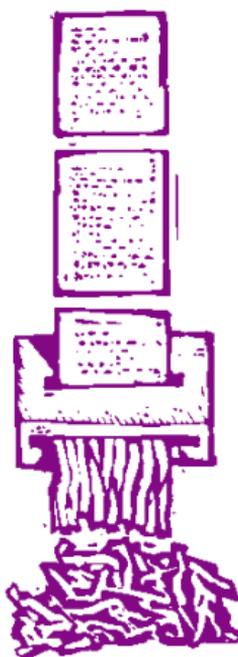


Speak up if you see sloppy handling of personal information in the workplace, at the doctor's office, at stores or your pharmacy. For example, ask that staff not leave forms with personal information on counters where they can be easily seen by anyone walking by or waiting to be served.

Be careful with your mail. If you're expecting new checks, call the bank if they don't arrive when expected. Mailbox thieves can steal new checks that arrive in your mailbox. Thieves can also steal credit card offers mailed to you, which they apply for in your name. Consider getting a locking mailbox. Be aware that thieves can also steal outgoing mail you leave for the postal carrier, in order to find out your Social Security number or other personal information that may be on bill payments. Consider putting your outgoing mail into a U.S. Mail box or taking it to the post office.

Shred sensitive trash.

Identity thieves go through trash to find personal information they can use to apply for credit in other people's names. Tear up or shred items you are discarding that have personal information on them, such as credit card receipts, bank statements or credit card offers.



Don't disclose any information about yourself to strangers on the phone.

Many scams involve callers who say they represent your bank or credit card issuer and need to verify your account information. Even "research surveys" that ask for personal information can be a scam.

Ask your local phone company not to publish your address. Mailing list companies compile names and addresses from residential phone book listings. Consider having an unlisted number, or ask your local phone company to publish just your name and telephone number. Ask the phone company to remove your listing from its street address directory.



Get off national mailing lists. Register with the Direct Marketing Association's Mail Preference Service. You can

get off many national mailing lists this way. Your name will remain on this "delete file" for five years. Send your name and address to: DMA Mail Preference Service, P.O. Box 9008, Farmingdale, NY 11735-9008, or visit www.the-dma.org/consumers/offmailinglists.html.

Tell the credit reporting agencies that you don't want to receive pre-approved offers of credit. Those credit card offers that come in the mail are from companies who get your name and address

from one of the credit reporting agencies. You can tell all three of the major credit reporting agencies—Equifax, Experian and TransUnion—to remove your name from these lists by calling one toll-free number, 1-888-5-OPT-OUT.

Tell magazines and charities that you don't want them to share your name and address with other businesses or charities. Request the same from mail order companies.

Exercise your "opt-out" rights in the privacy policies of your credit cards and banks. By opting out, you can tell the bank not to share your personal information with other companies. The bank may still be allowed to share your information with "affiliate" companies with which it has a relationship. A financial institution must mail you a copy of its privacy policy each year; you can also contact the company to request a copy at any time.

Know your privacy rights when paying by check or credit card.

Maryland law limits the information a merchant can ask of you when making a purchase.



- ▲ When you are paying by check, the merchant can ask to see a credit card for purposes of identification or to

verify credit worthiness, but may not record your credit card account number on the check. The merchant can record the type of card and the issuer.

- ▲ When you are paying by credit card, the store may not record your address or telephone number on the credit card transaction form, unless the store needs the information for shipping or delivery.

Avoid entering drawings and sweepstakes. The purpose of most of these contests is to compile names and addresses for marketing purposes.

Don't fill out warranty or product registration cards. Most cards are used to compile information on consumers that is sold to companies for marketing purposes. Your receipt will ensure that you are covered by the product warranty if the item turns out to be defective. If you decide to send in the card, don't fill out "lifestyle" information, such as your income or hobbies.



Pay with cash. If you don't want to create a database record of your purchases, pay with cash rather than a credit card, and don't use "frequent shopper" or "savings club" cards.

Using Caution on the Internet

Every time you use the Internet, a record is created somewhere in cyberspace. You may not be able to control the type of information that is collected, but you should be aware that it is happening.



Think of e-mail as a postcard rather than a sealed letter. E-mail can be intercepted, either intentionally or unintentionally, so be cautious about including sensitive personal informa-

tion. At work, realize that employers generally have the right to monitor any e-mail messages sent from computers in the workplace.

Exercise caution when visiting chat rooms, bulletin boards and newsgroups.

Since these are open forums, it's not a good idea to reveal your address, financial information or other personal information.

Choose carefully what you reveal in personal or family Web sites. Because you don't know who might access your personal or family Web site, be cautious about posting your telephone number, address, photos, or information such as the names of your children and where they go to school.

Know that your Web site visits are not entirely private. Many people mistakenly think that when they visit Web sites they are doing so anonymously. In fact, the Web sites you visit can gather information about you, including your screen-name, information about your computer, your Internet service provider and more.

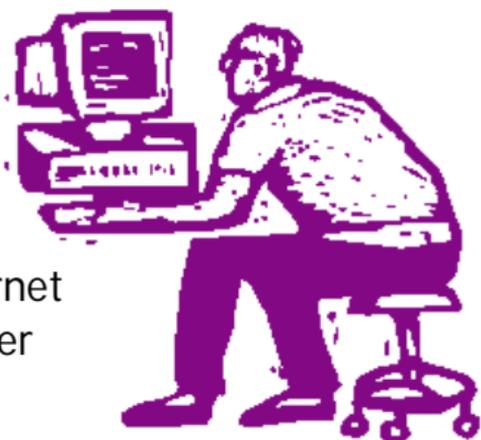


In addition, some Web sites ask you for information. If you provide it, it can be added to a database for future use by that company or be sold to other companies.

Also, Internet service providers and Internet browsers can collect information about your Web visits and may sell that information.

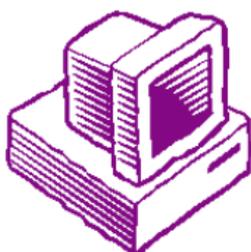
- ▲ To protect your anonymity when you visit a Web site, try using "The Anonymizer" at www.anonymizer.com. It will assign you an anonymous identity that is revealed in place of your real identity when you visit other sites. www.junkbusters.com has other helpful tools and suggestions for protecting your privacy online.
- ▲ You can block "cookies" from being placed on your computer. Cookies are small files placed on your computer by Web sites you've visited. If you revisit the site, the cookie file lets the site

identify you as a return guest and offer you products tailored to what your last visit revealed about you. Cookies can also reveal to Web sites where else you have traveled in cyberspace and allow them to build a data file about you. Go to the Help section of your Internet browser program, such as Netscape or Explorer, to learn how to block cookies. You can also choose to require that your permission must be given before any cookie is placed on your computer. Know that if you disable cookie files, some Web sites at which you've registered will no longer recognize you and you may find it difficult to access certain sites.



- ▲ Ask your Internet service provider what kind of information it collects about you, how it uses the information and whether it sells the information.

Protect your computer from being hacked. If you have a high-speed connect to the Internet via digital subscriber line or cable, you could be at risk of a hacker accessing your computer's hard drive. You should install a firewall.



Another solution is to disable file and printer sharing. Information on how to do that can be found at <http://www.grc.com/su-bondage.htm>.

Only give your credit card or bank account numbers to Web sites that offer secure, encrypted transactions. Never give personal information—such as your Social Security number, credit card number, bank account numbers or address—to unknown companies. Remember that you don't know who is really at the other end. You might also consider new, single-use credit card numbers for Internet purchases that are being offered by some credit card companies.

Internet technology changes all the time. Therefore, you will need to stay alert to both new risks to your privacy and new tools or strategies you can use to defend your privacy.

Avoiding Identity Theft

Identity theft is when someone else uses your name, Social Security number, bank account number, credit card number or other personal identifying information without your knowledge to commit fraud. The imposter may open credit accounts, get a driver's license or rent an apartment in your name, and create havoc with your finances. Identity thieves can even rack up criminal charges or declare bankruptcy in your name.



Identity theft is a crime that can be prosecuted, but the thief is often difficult to track. Even if the thief is caught and stopped, it can take months or years for the victim to clear up the incorrect information. In the meantime, the victim may not be able to get a car loan, a mortgage or refinancing, may be charged criminally, or may be harassed by debt collectors.

By following the practices listed under "Protect Your Privacy: Practical Steps," you can reduce the chances of becoming the victim of identity theft.

Other things you should do on a regular basis include:



- ▲ Obtain a copy of your credit report each year to be sure it is accurate and reflects only credit actions you've authorized. Call the three major credit reporting agencies: Equifax at 1-800-685-1111; Experian at 1-888-397-3742; and Trans Union at 1-800-888-4213. Maryland residents are entitled to one free copy of their report each year.
- ▲ Check credit card statements and bills for unauthorized charges.
- ▲ Pay attention to your billing cycles. Follow up with creditors if bills don't arrive on time. An identity thief can change your address or steal bills from your mailbox.

If it turns out that someone is using your identity fraudulently, act immediately. Your first three steps should be:

1. Contact the fraud units of each of the three major credit reporting agencies.

Ask that your file be flagged with a fraud alert, and add a victim's statement to your report, such as "My ID has been used to apply for credit fraudulently. Contact me at (your telephone number) to verify all applications." Ask the credit reporting agency about its procedures for investigating and removing incorrect information from your report.



Fraud Unit Numbers:

Equifax: 1-800-525-6285

Experian: 1-888-397-3742

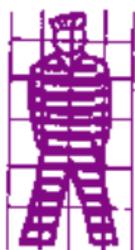
TransUnion: 1-800-680-7289

2. Immediately contact all creditors with whom your name has been used fraudulently, by phone and in writing.

You may be asked by banks and credit grantors to fill out and notarize fraud affidavits. Get replacement credit cards with new account numbers for accounts that have been used fraudulently. Carefully monitor your mail and credit card bills for evidence of new fraudulent activity. Report it immediately to credit grantors.

3. Report the fraudulent activity to your local police or sheriff's department. Get a copy of your police report. Keep the phone number of your fraud investigator handy and give it to creditors and others who require verification of your case. Credit card companies and banks may require you to show the report in order to verify the crime. Some police departments have been known to refuse to write reports on such crimes. Be persistent!

A Maryland law effective October 1, 1999 makes it a crime to assume another person's identity in order to obtain any benefit or thing of value, to avoid the payment of a debt, or to avoid prosecution for a crime. A person convicted of this crime is subject to a fine up to \$5,000 or up to one year in prison or both. The court may also order the person to make restitution to the victim for reasonable costs incurred, including attorney's fees for clearing the victim's credit history or as the result of any civil proceeding that arose because of the crime.



For more steps you should take, see the Attorney General's pamphlet *Identity Theft: What to Do If It Happens to You* by visiting our Web site at www.oag.state.md.us and visit the Web site of the Privacy Rights Clearinghouse, www.privacyrights.org and the Federal Trade Commission's Identity Theft Web site: www.consumer.gov/idtheft.



Warning signs of identity theft:

- ▲ You get a letter from a bank or creditor confirming your recent change of address—and you haven't moved.
- ▲ You get calls or letters stating that you have been approved or denied credit by a creditor to which you never applied.
- ▲ You receive credit card, utility or telephone statements in your name and address for which you never applied.
- ▲ A collection agency says it is trying to collect on a defaulted account in your name, but you never opened the account.



Safeguarding Your Children Online

The Internet is a wonderful tool for children to learn about the world and communicate with others. Unfortunately, it can also be a way that the world can learn about your child. Dangers to children online include:

- ▲ that the child will be exposed to materials you find inappropriate, such as pornographic, racist or violent material;
- ▲ that strangers might locate and physically harm your child, for example by befriending the child through e-mail and luring them to meet “in the real world”; and
- ▲ that companies may try to obtain personal information from your child for marketing purposes.

To protect your child from these hazards you will have to be vigilant. Here are steps you can take:

Keep the computer in a public room in your house. Choose the family room, living room or kitchen, where you can keep an eye on your child as he uses it. Don't let young children “surf the Net” alone.

Don't let a child use his or her last name or age in an onscreen name. Limit the amount of personal information the child fills out on his or her profile page.

Establish ground rules for Internet usage. Just as you teach your child rules about dealing with strangers outside the home, you should provide rules for communicating online.

- ▲ Tell your child not to give out any personal information, such as name, address or telephone number, without your permission. Explain



that even if a familiar cartoon character asks for the information, or the information is required to play a game or enter a contest, he or she should ask you first.

- ▲ Tell your child never to respond to email or chat messages that makes him or her feel uncomfortable, and to report such messages to you.
- ▲ Tell your child to ask you before agreeing to meet anyone he's met online.
- ▲ Encourage your child to share their online experiences with you.

Read the privacy policies of Web sites your child visits. Under the federal Children's Online Privacy Protection Act, Web sites that are directed to children under age 13 must post a notice about the types of information they collect from children, how the information is used, whether it is shared with others, and who to contact at the Web site about children's privacy. In many cases, Web sites directed to children under age 13 must obtain consent from parents before collecting, using, or disclosing personal information about a child.

If you don't like what the policy says, or a privacy policy is not posted, tell your children the site is off-limits.

For more information about the Children's Online Privacy Protection Act, or to report a suspected violation, contact the Federal Trade Commission's Consumer Response Center toll free at 1-877-FTC-HELP or online: www.ftc.gov.

Learn about "parental control tools." Your Internet Service Provider and the Web browser you use may offer a range of parental control tools, or you can purchase special software on your computer. These methods are not perfect. They cannot block everything you might not want your child to see, and they may block information that is helpful.



- ▲ **Filtering tools** may: limit access to a specific list of Web sites that have been classified as inappropriate; limit access to Web sites that fall into certain categories, such as containing explicit language, sexual content or violence; block Web sites, e-mail or newsgroups that feature certain “keywords” (such as “sex” or “breast”). The tools vary in how much parents can customize them and override them when appropriate. Some filtering tools will also allow you to block the outgoing transmission of children’s personally identifying information, such as names, addresses and telephone numbers.
- ▲ **Monitoring tools** can record the addresses of Web sites that a child has visited, and provide a warning message to a child if he or she visits an inappropriate site. Monitoring tools can be used with or without the knowledge of the child.

- ▲ **Browsers for kids** work like the widely used Internet Explorer or Netscape Navigator browsers, except that they filter sexual or otherwise inappropriate words or images.
- ▲ **Kid-oriented search engines** only search within a certain group of pre-approved sites, or will search the entire Web while withholding search results that are inappropriate.

Don't give your child your credit card information. If your child wants to make a purchase over the Internet, handle the transaction yourself. Giving your children your credit card information may give them access to adult sites with pornography or gambling, many of which ask for credit card information as a proof that the visitor is at least 18 years old.



Resources

Privacy Rights Clearinghouse

619-298-3396

www.privacyrights.org

Many fact sheets on privacy, Internet privacy, financial privacy and opt-out notices, and identity theft

The Federal Trade Commission

www.ftc.gov

Publications on privacy, identity theft and children and the Internet

Center for Democracy and Technology's Guide to Online Privacy

www.cdt.org/privacy/guide

Explains laws covering privacy, lists privacy-enhancing software tools.

EPIC (Electronic Privacy Information Center) 202-544-9240

www.epic.org

List of privacy-enhancing software tools.

Junkbusters.com

<http://internet.junkbusters.com>

Offers free software that blocks unwanted Internet banner ads and deletes unauthorized cookies.

Sites with helpful information for parents and kids about safety on the Internet:

FTC's Kidz Privacy Web site:

Follow link from www.ftc.gov

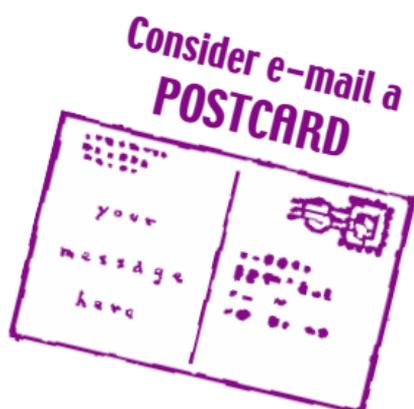
American Library Association's "Librarian's Guide to Cyberspace for Parents & Kids":

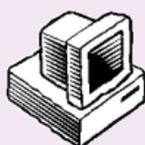
www.ala.org/parentspage/greatsites/guide.html

www.yahooligans.com

www.familyclick.com

www.getnetwise.org





**Visit our website for late-breaking
consumer news and helpful
publications, as well as other
important legal information.**

www.oag.state.md.us

About the Office

What's New

News Releases

Criminal
Investigations

Consumer
Protection

Legal Opinions

Securities

Health Advocacy