CONSUMER INFORMATION SHEET 6
September 2012

How to Read a Privacy Policy

One way to protect your privacy is to learn how an organization will use your personal information *before* you give it out. Today most financial institutions, insurance companies, heath care providers, government agencies, and e-commerce Web sites give their customers and visitors information on their privacy practices.[i] California law requires commercial Web sites that collect personal information on California consumers to post a privacy policy and to comply with it. The law also applies to "online services," such as AOL or Yahoo![ii]

Before you fill out an application for credit in a store or bank, or type your credit card number into an online order form, ask to see a copy of the organization's privacy policy. If you are not happy with the policy's terms—or if you are told there is no written privacy policy—STOP. Consider looking for another company that respects its customers enough to explain how it handles and protects their personal information. A privacy policy should answer at least the following basic questions.

☑ What personal information is collected?

What kinds of personal information does the organization collect from you? Personal information that businesses and government agencies ask you for may include the following: your name and home address, your home phone number, your email address, your Social Security number, your driver's license number, your financial information, such as credit card numbers, bank account numbers, and household income, your medical information, such as your health insurance plan, diseases or physical conditions, and prescription drugs used, your education and work experience, and other details of your personal life, such as your date of birth, the names and ages of your spouse or children, and your hobbies.

The privacy policy of a commercial Web site or online service that collects personal information on California consumers must list the categories of personal information collected.[iii]

☑ How is the information collected?

In addition to asking you to provide personal information on a paper or online form, an organization may collect information "automatically" through its Web site. One way to do this is through the use of "cookies." Internet cookies are small text files placed on your computer by a

Web site you visit. A cookie contains information on you that your browser saves and sends back to a Web site when you visit it again.

Web sites can use cookies to track your purchases and the different pages you visited or ads that you clicked on. Such information can be used to create a more detailed profile on you that may be sold to marketers.

Look for a description of the site's use of cookies or other tracking technology in its privacy policy. For more information on cookies and how to manage them, see the Electronic Privacy Information Center's cookie page at www.epic.org/privacy/internet/cookies/.

☑ Why is the information collected?

Does the personal information asked for seem appropriate to the transaction? For example, your name, home address, phone number, and credit card number may be necessary for making and shipping your purchase. Your household income and hobbies are not. Pay attention if a business or Web site asks for information beyond what is needed for the transaction. The purpose for the extra information should be clearly stated. Look for an opportunity to opt out of, or say no to, giving the extra information. Consider going somewhere else if you can't complete the transaction without giving up personal information you think is unnecessary.

☑ How is the information used?

A privacy policy should explain how the organization collecting the personal information intends to use it. Will it be used just to complete the transaction you requested? If additional uses are intended, you should be given the opportunity to opt out of them. For example, if a merchant plans to use your information to market to you, you should be given an easy way to say no to this. You should get this opportunity right up front, before you receive any unwanted email ads, telemarketing calls, or mail offers.

☑ Who will have access to the information?

Does the company or Web site share customer information with other companies? Does it share information with its affiliates or companies in the same "corporate family"?

The privacy policy of a commercial Web site or online service that collects personal information on California consumers must list the categories of third-party persons or entities with whom that personal information may be shared.[iv]

☑ What choices do you have?

Look for opportunities to opt out of the use of your information for marketing and the sharing of your information with others. There should be an easy way to opt out, such as calling a toll-free phone number or sending an email.

The Center for Democracy and Technology has created Operation Opt-Out to help you get off marketing lists and limit the sharing or sale of your personal information.[v] Their Web site contains forms you can print out and mail or send online to opt out of information sharing by many Web portals, data aggregators, and businesses.

According to Consumer Reports' E-Ratings, the better companies and Web sites do not share personal customer information with other unrelated companies unless the customer consents in advance.[vi]

☑ Can you review or correct your personal information?

An organization may give you the opportunity to review or request changes to the personal information that it has collected on you. Look for instructions on how to do this.

Many organizations allow a customer to review and request changes in the customer's own personal information. A commercial Web site or online service that collects personal information on California consumers must describe its process for giving consumers' access to their own personal information, if it has such a process, in the privacy policy posted on the site.[vii]

☑ What security measures are used to protect your personal information?

The privacy policy should give a general description of the security measures the organization uses to keep customers' and visitors' personal information safe. It should also cover security safeguards that the organization requires its business partners and vendors to use.

Web sites requesting personal information should use Secure Socket Layers (SSL), the industry standard for protecting private information sent over the Internet. The information is encrypted, or scrambled, into a code. This means that your information can't be read during transmission. Look for signs of security on Web pages where you enter personal information. Look for "https," rather than the usual "http," in the address window. Look for a closed lock icon in the lower right or left corner of your screen. These signs mean the connection is secure. You should remain in this secure zone for the entire checkout process.

Good security also means using strong security measures, such as encryption, to protect personal information when it's stored on company computers. It includes technology and procedures to limit access to customers' personal information to only those who need it to perform their duties.

☑ How long will the organization honor its privacy policy?

What is the effective date of the privacy policy? Does the policy state that the organization will honor its current policy in the future? Does it say that if they do change the policy, they will notify customers and site visitors? Does it say they will give customers and visitors a chance to opt out of having their information used according to the terms of the new policy?

The privacy policy of a commercial Web site or online service that collects personal information on California consumers must include a policy effective date and information on how consumers will be notified of changes.[viii]

☑ Who is accountable for the organization's privacy practices?

Someone in the organization should be responsible for its privacy policy and practices. Does the policy give you someone to contact with questions or concerns? Is there an easy way to contact the right person—by email or by a toll-free phone number?

A Web site may offer assistance with consumer complaints through a "privacy seal" program. The two major programs, TRUSTe and the BBBOnline Reliability Program, both require seal holders to follow certain privacy practice guidelines.[ix] Click on the seal logo for information and assistance on privacy issues.

☑ More Information on Privacy Policies

Center for Democracy and Technology, "Getting Started: Website Privacy Policies," at http://www.cdt.org/privacy/guide/start/privpolicy.php.

Privacy Rights Clearinghouse, "Financial Privacy: How to Read Your 'Opt-Out' Notices," at www.privacyrights.org/fs/fs24a-optout.htm.

GetNetWise, "How to Read a Privacy Policy," at http://privacy.getnetwise.org/shopping/policy.

Notes

[i] The federal Financial Services Modernization Act requires financial institutions and insurance companies to send a privacy notice to customers every year. See the Financial Privacy page on the California Department of Justice Web site for more information. The federal Health Insurance Portability and Accountability Act requires health care providers, health plans, and health insurers to provide patients with notice of the patient's privacy rights and the privacy practices of the covered entity. More information is available from the federal Office of Civil Rights at www.hhs.gov/ocr/hipaa/ and from the Health Privacy Project at www.healthprivacy.org/.

[ii] The California Online Privacy Protection Act of 2003, Business and Professions Code §§ 22575-22579, requires operators of commercial Web sites that collect "personally identifiable" information on California consumers to "conspicuously post" its privacy policy on its Web site and to comply with the policy's provisions. The Act also applies to operators of "online services" that collect personal information on California consumers.

[iii] Business and Professions Code § 22575(b)(1).

[iv] Business and Professions Code § 22575(b)(1).

[v] The Center for Democracy and Technology (CDT) is a non-profit policy organization that works to promote democratic values and constitutional liberties in the digital age. Their Web site is at www.cdt.org. Operation Opt-Out is at http://opt-out.cdt.org/.

[vi] See Consumer Reports, *E-Ratings: A Guide to Online Shopping, Services, and Information*, available at www.consumerreports.org/ (visited June 2004).

[vii] Business and Professions Code § 22575(b)(2).

[viii] Business and Professions Code §§ 22575(b)(3) and 22575(b)(4).

[ix] Information on TRUSTe's programs can be found at www.truste.org/consumers and on the BBBOnline Reliability Seal at www.bbbonline.org/reliability/Rel_EN.asp.