Online Privacy—How to Protect Yourself and Your Family

We all have concerns regarding our online privacy. Chief among those concerns are:

- Potential identity theft
- Disclosure or misuse of personal or private information
- Denial of employment, insurance, or medical coverage
- Governmental intrusions on our liberty and autonomy

At the same time, we know that most information and services on the Internet are essentially free because website owners make money by selling ads and providing user information to advertisers. In effect, websites ask us to give up some privacy to give us a better user experience.

We each need to make decisions about how much privacy to give up in exchange for a better and more vibrant web experience. What is the right balance for you? For your family? Whatever you choose, your decision will be better if it is informed.

This paper will help you make an informed decision about this balance between privacy and personalization, a topic that is very much a part of enabling the Human Network.

This paper covers:

- Why websites want to collect information about you
- What information websites collect
- How they do it
- How to give or deny permission for websites to collect your information
- How you can browse the Internet anonymously
- Resources and information that explain how to protect your and your children's privacy, to protect your identity against theft, to fight spam, and more

Why do websites collect information about you?

The first thing to understand is why anyone wants information about you. **Why** a website wants information about you affects both **what** information they collect and **how** they collect it. These factors may affect your privacy and the steps you take to protect your personal information.

Generally, websites gather information about you for four main purposes:

- To improve the website to bring you a better user experience
- To facilitate your online transactions, payment processing, and package delivery tracking
- To be attractive to advertisers that provide revenue to the websites
- To share information about you with others such as partners, affiliates, and advertisers

What information do websites collect from your computer?

Websites collect technical information about your computer, such as the size of your screen or type of browser you use. This information helps web designers format websites in a way that is compatible with your computer.

© 2009 Cisco Systems, Inc. All rights reserved.

Websites also collect information related to your activity on the web, such as your Internet Protocol (IP) address, the time you clicked on a link, how much time you spent on a particular web page before moving on to the next one, and the web page you were reading prior to clicking the link. This information, when aggregated with similar information about other users, is extremely valuable to advertisers.

Some websites may also collect Personally Identifiable Information (PII) such as your name, email address, or phone number.

How do websites collect information?

Every computer on the Internet has a unique identification number called an IP address. This address is usually assigned by your Internet service provider to identify your specific computer or router, and it can be used to show your general physical location. When you connect to a website, that site collects your IP address. If you are concerned about allowing a website to have this information, you can hide your IP address (see Additional Resources at the end of this document for information on how to hide your IP address).

Websites use other technologies to let them know you have visited their sites. Prominent among these are four technologies that websites store on your computer and use to collect information about your activity:

- Browser cookies
- Flash cookies (or local shared objects)
- Web beacons
- Google Analytics

Browser Cookies

The vast majority of websites store small data files, called cookies, on your computer when you access or browse a website. After your first visit to a website, its cookie allows that website to recognize your computer when you return to that site. Cookies also record your previous activity on that site.

Cookies offer several benefits to you:

- Automatic login: Cookies remember your username and password so you don’t have to re-enter these when you return to a website.
- Optimized, personalized information: Based on your previous activity on the site, the website can show you information you may find interesting.
- Location memory: Cookies record where you stopped accessing a site. This makes it possible for you to re-enter a site and pick up exactly where you left off. For example, if you were in the middle of making a purchase, you won’t have to reselect your purchases or re-enter certain information. Note that as a general business practice, most sites do not store confidential information, such as credit card numbers, in the cookie for redisplay.

Cookies benefit websites in several ways:

- Site understanding: Cookies record how you interact with the site, which helps the owner develop sites that better utilize your time.

© 2009 Cisco Systems, Inc. All rights reserved.

- Market understanding: Cookies help websites learn which offerings interest the majority of visitors. This, in turn, can help the owners supplement their sites with complementary information from other websites.
- Customer understanding: Cookies help websites infer what interests you in particular. This allows them to present you with information, products, or services that might interest you.
- Metrics: Cookies collect data such as the number of unique visitors that have viewed a particular ad or visited a particular web page. This allows the owner to track the effectiveness of the site.

Cookies are stored on your computer by your browser. To control cookies, you can do the following:

- Disallow some or all cookies from being stored
- Delete some or all cookies already stored
- Install software that notifies you when a cookie is being stored

If you would like to exercise control over your cookies, see the Additional Resources section at the end of this paper. Keep in mind that cookies reside on a specific computer, with specific login and browser combinations; if you change computers, users or browsers, or use multiple computers or browsers, you will need to control your cookies on each computer and browser you use. Also note that disallowing cookies may limit your access to some websites.

Flash Cookies

Flash cookies (or local shared objects) are similar to browser cookies but are stored on your computer when you use Adobe Flash to play movies from websites. These cookies may contain some of the following information:

- An identifier that allows a website to track movies you have watched from that site
- Any information you provide to that site
- Your computer’s configuration

If you would like to exercise control over your Flash cookies, you can use Adobe’s FlashPlayer Settings Manager to disable or allow new Flash cookies on a site-by-site basis and delete all or some existing Flash cookies. As some Flash applications may request access to your camera and microphone, this tool enables you to respond to those requests with “always deny” or “always ask.” See Additional Resources for a link to Adobe’s FlashPlayer help page.

Web Beacons

Web beacons are objects that are embedded into web pages or email messages; they may also be referred to as web bugs, tracking bugs, tracking pixels, pixel tags, 1×1 gifs, single-pixel gifs, pixel tags, smart tags, action tags, tracers, cookie anchors, or clear gifs. Many websites and applications that deliver email use these objects, often invisible, to prompt your browser or email program to send them information. Information may include your computer’s IP address, the time the content was requested, your browser type, and the existence of cookies previously set by that server. Your email address also may be collected when you open an email message.

Websites use web beacons to count unique and repeat visitors, track how each page of their websites is used, and track how users entered the site. Websites use this information to improve and personalize user experience. Web beacons can also be used to deliver cookies or downloadable applications.

Web beacons are used by those sending email to identify which recipients open a message, whether they act on the message, and what action they took in response. Web beacons tell senders how many times a message is forwarded, which links were followed, and what was done on the destination website. If you open a spam message with an embedded beacon, the spammer can capture your email address. Web beacons can also be used in conjunction with cookies.

Exercising control over web beacons is more difficult than controlling cookies. However, web page filtering, which disallows many web beacons, is available by using web proxies. These rewrite web pages and serve them to you while filtering out web beacons.

Also, many email programs allow you to manage how you receive pictures from the Internet. You can disallow requests for pictures or displaying pictures from the Internet, or be prompted to allow or disallow each request. You can also turn off pictures completely and display messages only using text. Either of these methods prevents tracking or validating your email by web beacons. When using a laptop or handheld device, you can prevent web beacon communication by disabling the network connection when you open and read messages. This simple action prevents all pictures from being retrieved from a website. However, you must repeat that procedure every time you open the message.

Privacy policies often include notices about the use of web beacons. If web beacons are used to transfer PII to a third party, you should be given a choice to opt in or opt out of these beacons.

Google Analytics

Website owners use visitor information to improve their websites and to tell potential advertisers how many visitors they get, where those visitors are located, and which other sites they visited previously. Google Analytics is a free service that reduces the amount and complexity of this raw data into a meaningful report. It is widely used by websites, which send their raw data to Google and receive an analysis in return that includes the following types of information:

- Type of user agent (browser) used, software manufacturer, and version number
- Type of operating system
- Network location and IP address: Can include country, city, or any other geographic data as well as the hostname and your bandwidth (connection speed)
- Time of visit
- Pages visited
- Time spent on each page of the website
- Referring site statistics: Can include the website you came through to reach this website and the search-engine query that brought you there

Some websites include a statement about their use of Google Analytics on their privacy pages, but this information is generally harder to find than information about the use of cookies. Opting out of cookies has no effect on Google Analytics. Nevertheless, you can exercise some control over Google Analytics reporting by using a browser add-on like Adblock plus to filter out reporting to Google Analytics or by turning off Javascript (see Additional Resources for more information).

How can you give or deny permission to collect information about you?

When you use a website, it is generally assumed that you accept the terms and conditions of that website. If you want to know what these are, look for a link labeled “privacy” or “privacy policy.” Some sites allow you to control how information about you is used. Control usually takes the form of either opt-in or opt-out consent. Opt-in email is a term applying to email that recipients have previously requested by signing up on a website or through a special ad banner. If you opt out of these messages, the website operator is prohibited from sending you promotional emails. Many websites assume that you give your consent unless you opt out of certain uses of your data. You can opt out of certain services offered at a single website by usually linking to that site's privacy page. There are also other special websites that allow you to opt out of many individual websites. One of these is the Network Advertising Initiative (NAI). http://www.networkadvertising.org/.

Many websites are members of ad networks, organized groups of network advertising companies that manage and provide advertising for numerous unrelated websites. Member websites share summaries (not PII) of what they know about you with the ad network and other members. These members use that information to target more relevant ads to you, independent of the website you are visiting. For example, if you regularly visit a website for new mothers, Procter & Gamble might be interested in sending you advertising for diapers. Many members of ad networks are also members of the NAI, which recommends best practices for its members that make it simple and easy to opt out of this type of analysis and advertising presentation.

Other similar arrangements exist among websites to help provide you with a better experience. For example, the social network LinkedIn provides a list of the interests voluntarily made available by its members to the *New York Times*, which then serves customized headlines based upon those interests to LinkedIn users.

When you opt out of a website, the information is recorded on a cookie. When you visit a website from which you have opted out, it recognizes that you have opted out and treats you as though you had never been there before (there is no customization, for example). If you opt out from an ad network, all of its member websites recognize that you have opted out. Keep in mind that the opt-out cookies are stored in your browser. If you delete them, neither the websites you visit nor ad networks will recognize that you have previously opted out.

What about your offline data?

It is important to understand that information gathered about you online also can be linked to publicly available data about you that is gathered offline.

Offline information about you may include:

- Telephone calling patterns
- Home ownership and rental history
- Legal history
- Purchase history
- Family relationships
- Medical history
- Late bill payments
- Education history
- Employment history
- Memberships

Some of this information is closely held (for example, your medical history), much of it is for sale by those that collect it, and some is a matter of public record. You can use online services, such as

© 2009 Cisco Systems, Inc. All rights reserved.

http://www.peoplefinders.com or http://www.people.yahoo.com, to find out what information about you is freely available. Simply search on your name or phone number to get a report.

As technology progresses, websites will have more ways to identify you online. For example, facial recognition may be used to match images online and offline, so that your online image may become PII. As data mining software becomes more intelligent, disparate snippets of online information could be combined with various nontraditional data sources to identify you. For example, fragments of information about you in blogs, chatrooms, and friends' postings may be combined with information from links to how-to sites to identify not only who you are but what you are trying to accomplish.

How can you browse anonymously?

For many years there have been ways to browse the internet anonymously, using special sites that act on your behalf. These proxy sites take you where you want to go while hiding information about your computer such as its location and address.

Today, there are simpler ways to surf anonymously using newer versions of the browser you may already use.

Firefox 3.1 has integrated "Private Browsing," which ensures that data such as cookies or browsing history is not stored on your computer. By selecting "Private Browsing" from the Tools menu then "Start Private Browsing," you pause your normal browsing session and open a private session in a new window. When you finish browsing privately, open the Tools menu and deselect "Private Browsing." At that point, any cookies and history related to your private browsing session are deleted and your normal browsing session resumes.

Internet Explorer 8 has integrated "InPrivate Browsing," which ensures that data such as browsing history, temporary Internet files, form data, cookies, usernames, and passwords are not stored. To start a new private browser session, either open a new tab and select "Start InPrivate Browsing" or "InPrivate Browsing" from the Safety button. When you finish browsing, simply close the browser window. Internet Explorer 8 also provides enhanced cookie deletion control that gives you more control of which cookies to delete.

Safari 3 offers private browsing, which ensures that searches, cookies, browsing history, or form data are not stored. Go to edit and select "Private Browsing." When you turn off private browsing, Safari resumes its normal operation. Safari also has a one-click Privacy Reset to delete all stored browsing information.

Using these browsers may help protect your information, but remember that sharing a computer with others may expose your browsing information.

Also, if you choose to use a proxy, you should know that the proxy may see logins, passwords, and credit card information that you may not want shared. Read up on the security techniques of the proxies and use them only if you are comfortable with their policies.

What can you do to protect your children's privacy online?

With an increasing number of children spending time online, it is important that both parents and children are aware of the potential risks. A number of free educational resources for teens and parents are available at this website: http://www.webwisekids.org.

In addition to your own protections, the U.S. Federal Trade Commission regulates certain websites that collect personal information about children under the age of 13. Under the Children's Online

© 2009 Cisco Systems, Inc. All rights reserved.

Privacy Protection Act, anyone operating a website that is designed for or directed to children, or who otherwise knows that it is collecting children's personal information:

- Must clearly disclose who is collecting the information, the kind of information that is being collected, how the information is being used, and any third parties with whom the information is being shared
- Must not require a child to disclose more information than is reasonably necessary as a condition to participate
- Must obtain verifiable parental consent from the child's parent (with certain exceptions)
- Must allow parents the option to prevent the sharing of information with third parties
- Must provide parents the opportunity to review, delete, and refuse any further collection or use of child's information

More information can be found at http://ftc.gov/privacy/privacyinitiatives/childrens.html.

How do you know who to trust online?

Websites gain your trust by providing the information that you need and by using your private information in ways that help you. Most websites strive to be trustworthy, and many participate in organizations and processes that validate their trustworthiness. One indication that a website is trustworthy is a Privacy Seal, obtained by complying with certain standard practices prescribed by a certifying organization. TRUSTe and Entertainment Software Rating Board (ESRB) are two well-known certification organizations. The ESRB, primarily used for rating gaming sites, uses a rating system similar to the Motion Picture Association's film ratings. Click here to find out more information about these organizations:

ESRB: http://www.esrb.org/index-js.jsp

TRUSTe: http://www.truste.org/consumers/index.php

If a site bears a Privacy Seal, you can file with the certifying organizations if you have a complaint or dispute with that site. While a Privacy Seal may give some assurances that the websites take user privacy seriously, the lack of a Privacy Seal does not mean a site disregards those concerns. The best way to protect yourself is to take the time to read a site's privacy policy.

Additional resources

The following links provide more resources and information about how to protect yourself online:

- **Cookies:** Control your computer's cookies: http://www.aboutcookies.org/Default.aspx?page=1
- **Flash cookies:** Control your Flash cookies (Adobe's Flash Player help page): http://www.macromedia.com/support/documentation/en/flashplayer/help/settings_manager06.html
- **Opt-out:** NAI ad network members opt-out: http://www.networkadvertising.org/managing/opt_out.asp
- **Personal information online:** Find out what information about you is available online: http://www.peoplefinders.com
- **Anonymous browsing:** Find out more about anonymous browsing: http://www.wired.com/science/discoveries/news/2006/01/70051?currentPage=all
- **IP address:** What location does your IP address show? http://whatismyipaddress.com

© 2009 Cisco Systems, Inc. All rights reserved.

- **Javascript:** Turn off Javascript: http://www.cert.org/tech_tips/home_networks.html#III-B-6
- **Google Analytics:** Block reporting to Google Analytics: http://www.veign.com/blog/2007/01/how-to-block-yourself-from-google.html
- **Spam:** Fight against spam: http://www.ftc.gov/spam/
- **Children online:** Protection act for children: http://www.coppa.org
- **Identity theft:** Fight identity theft: http://www.ftc.gov/bcp/edu/pubs/consumer/idtheft/idt04.shtm
- **General information on privacy protection:** http://www.futureofprivacy.org/2008/11/26/where-does-your-data-go-before-you-even-click

There are more actions you can take to protect your computer systems at home; the following are recommended by the CERT Coordination Center. For further information on each of these points, see the CERT Coordination Center website: http://www.cert.org/tech_tips/home_networks.html.

- Consult your system support personnel if you work from home
- Use virus protection software
- Use a firewall
- Don't open unknown email attachments
- Don't run programs of unknown origin
- Disable hidden filename extensions
- Keep all applications (including your operating system) patched
- Turn off your computer or disconnect from the network when not in use
- Disable Java, JavaScript, and ActiveX if possible
- Disable scripting features in email programs
- Make regular backups of critical data
- Make a boot disk in case your computer is damaged or compromised

Americas Headquarters
Cisco Systems, Inc.
San Jose, CA

Asia Pacific Headquarters
Cisco Systems (USA) Pte. Ltd.
Singapore

Europe Headquarters
Cisco Systems International BV
Amsterdam, The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at www.cisco.com/go/offices.

CCDE, CCENT, Cisco Eos, Cisco HealthPresence, the Cisco logo, Cisco Lumin, Cisco Nexus, Cisco StadiumVision, Cisco TelePresence, Cisco WebEx, DCE, and Welcome to the Human Network are trademarks; Changing the Way We Work, Live, Play, and Learn and Cisco Store are service marks; and Access Registrar, Aironet, AsyncOS, Bringing the Meeting To You, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, CCVP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Collaboration Without Limitation, EtherFast, EtherSwitch, Event Center, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, iQuick Study, IronPort, the IronPort logo, LightStream, Linksys, MediaTone, MeetingPlace, MeetingPlace Chime Sound, MGX, Networkers, Networking Academy, Network Registrar, PCNow, PIX, PowerPanels, ProConnect, ScriptShare, SenderBase, SMARTnet, Spectrum Expert, StackWise, The Fastest Way to Increase Your Internet Quotient, TransPath, WebEx, and the WebEx logo are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (0812R)

Printed in USA C11-519232-00 01/09

© 2009 Cisco Systems, Inc. All rights reserved.