

TechCentral AT CLEVELAND PUBLIC LIBRARY

DIGITAL FOOTPRINTS

In today's world, everyone has an internet presence. Everything from property records to press releases can be made available on the web. At the same time, people handle more personal affairs online: shopping, social networking, banking, and more. In this way, the internet has increased convenience and broadened opportunities, but it has also increased the need for personal responsibility. More than ever, it is important to understand what information about you may be available online, how this information is created and stored, and what you can do to control it.

Before we learn more about managing our information online, we should take a moment to discover what information might be publicly available about us online. This is sometimes called ego-surfing or vanity searching. One quick way to do this is to use a search engine like Google to search ourselves.

EXERCISE

- Open Internet Explorer
- Go to google.com
- Search yourself. (You can try each search with and without quotes.) For each search, check the specialized results as well (images, videos, news, etc).
 - Type in your first and last name: "Joe Schmoe" or "Joseph Schmoe"
 - Type in your first, middle, and last name: : "Joseph Theobald Schmoe"
 - Type in your last name, then a comma, then your first name: "Schmoe, Joe"
 - Type in your street address (with and without city and state): "123 Library Lane"
 - Type in your phone number (with and without dashes): "2169876543"
 - Type in your email address: "superfanceleveland@gmail.com"
- Evaluate your results
 - How many results did you find about yourself?
 - What kind of information is out there about you?
 - What, if anything, would you like to change?

Other people searches:

Whitepages.com

This is the world's largest online phone book. Virtually anyone who is "listed" in the phonebook can be found in this database. This database is searchable by name, address, and phone number. You can even search an address and get the names of people living in a neighborhood.

Pipl.com; Spokeo.com; Peekyou.com

These are a few examples of people search sites. These sites often will provide basic public information about people, like their name, age, address, and phone number. Often, they will offer to provide a more detailed report for a fee. Sometimes they will link you to other pay services, such as intelius.com or beenverified.com that provide person reports or background checks.

EXERCISE

- Go to whitepages.com
 - Search your name
 - Search your phone number
 - Search your address
- Try searching for yourself on one or more of these websites:
 - pipl.com
 - spokeo.com
 - peekyou.com

Google Alerts

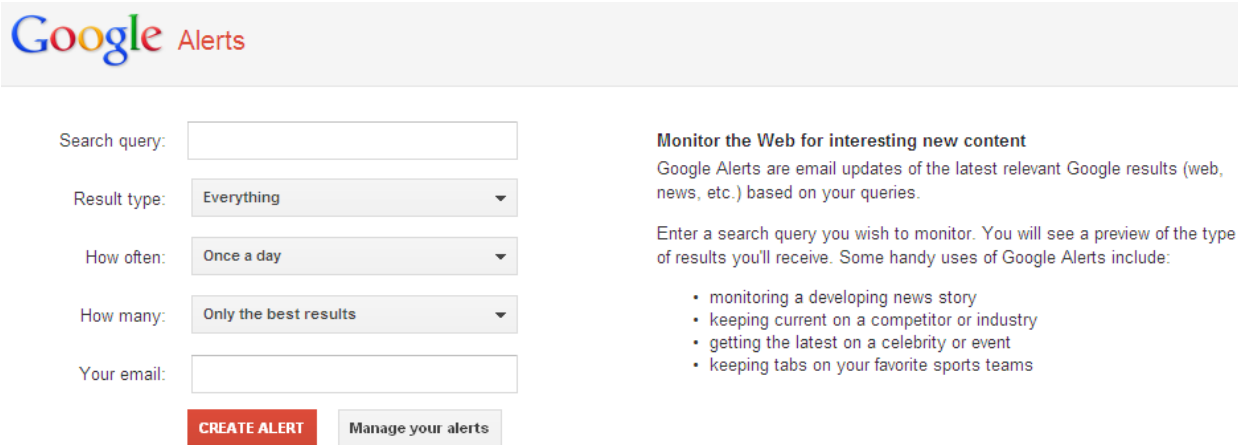
If you are interested in keeping tabs on your online reputation, setting up a Google Alert is great way to get started. A Google Alert is a notice sent to your email from Google when Google has found a new instance of any keywords you have setup to monitor. So, for example, Google can let you know when new information associated with your name shows up in a Google search. You do not need a Google account (such as a Gmail address) to use Google alerts; you can have this notice sent to any email address.

You can set what areas of the internet you wish to monitor. You can choose to have a comprehensive report covering all instances throughout the web, or only monitor news articles, blogs, videos, or groups.

You can set the frequency that you receive your Google alert. The alert can be sent when Google finds the phrase, once each day, or once a week.

In one session you are allowed to create up to ten unique alerts. Once you confirm your alerts, you are allowed to create more. The maximum number of alerts you are allowed per email address is 1000.

Create a Google Alert



The screenshot shows the Google Alerts creation interface. On the left, there are five input fields: 'Search query' (a text box), 'Result type' (a dropdown menu with 'Everything' selected), 'How often' (a dropdown menu with 'Once a day' selected), 'How many' (a dropdown menu with 'Only the best results' selected), and 'Your email' (a text box). Below these fields are two buttons: a red 'CREATE ALERT' button and a grey 'Manage your alerts' button. On the right, there is a section titled 'Monitor the Web for interesting new content' with a brief description of Google Alerts and a list of examples: monitoring a developing news story, keeping current on a competitor or industry, getting the latest on a celebrity or event, and keeping tabs on favorite sports teams.

1. Go to the Google Alerts home page (www.google.com/alerts).
2. In the top text box, type in the terms you want Google to track for you. In addition to being alerted about new instances of your name, you can choose to monitor anything else you want: people, events, products, interests, etc.
3. Use the Type drop-down allows you to select the kinds of alerts you want.
 - Everything
 - News
 - Blogs
 - Video
 - Discussions
 - Books

Most of the time, you will want to choose “Everything.”

4. Use the *How often* drop-down to choose the frequency of alerts you will receive.
 - As-it-happens – Receive an alert as soon as Google finds an instance of your alert.
 - Once a day – Receive a Google alert email once a day.
 - Once a week –Receive your Google alert email once a week.

If you want to keep right on top of when your phrase is found, select as-it-happens.

5. Use the *How many* drop-down to choose delimit the results included in the alert.
 - Only the best results
 - All results

6. Finally, in the *Your email* text box, type in the email address you would like to receive the alert.

7. When you are sure of all of your selections, click “Create Alert.”

8. Google will send an email to you asking you to click a link to confirm that you would like to receive the alerts. Once you do, you will begin receiving Google Alerts.

Now that you've seen the kind of personal information that might be available about you online and how to find this information, it is time to discuss the traces you leave behind when you use the internet.

Digital Footprints

In everyday life, your identity and actions are documented by paper records such as your birth certificate, vehicle registration, pay stubs, and receipts. Similarly, your digital identity and digital actions are documented by digital records. These records form your digital footprint, a sort of "digital paper trail" you leave when you use the internet or other digital services like mobile phones and television.

A digital footprint can include a record of such activities as logging in and out of services, browsing history, accessing or creating files, purchasing history, or emailing and chatting. Information shared on social media sites (Facebook, Twitter, YouTube, etc.) also contributes to your digital footprint. Information, pictures, and videos that others post about yourself are part of your digital footprint as well. When you use a mobile device, your digital footprint can include data about your location and the people with you. All of these records can be collected and stored in databases where interested parties may be able to access the data.

Active digital footprints

An active digital footprint is created any time you intentionally share information online. This includes data from email messages, blogs and comments, and social networks, as well as from information you provide during online registrations, surveys, and purchases. This data may or may not be made available to other entities, so it is important to read privacy agreements for every online service you use. You can control whether your email, chat, and social networking profiles are public or private, so take the time to review and set your privacy settings.

What can I do to control my active footprint?

The most effective way to control your active digital footprint is to be careful about the information you share (personal information, opinions, pictures, etc.), where you share information (a web forum, an email, a social network), and who you share information with (the public, friends and family, an individual, etc.). Be particularly careful about publicly sharing:

- Full name
- Social security number
- Address (past or present)
- Date of birth
- Telephone number
- Workplace / School

Social Networking

Social networking is a way to share online with other internet users. Many different types of websites are now interactive and social, and users share information, pictures, videos, documents, and more.

Social networking sites like Facebook, Twitter, and LinkedIn are thriving like never before, and many people have become comfortable communicating online. However, before you relax too much into this new way of interacting, you may need to take a closer look at issues regarding safety and privacy in order to protect yourself both on and offline.

Keep in mind that much of the following information may apply to many different kinds of web services (email, online shopping sites, online games, etc.), not just social networking sites.

Understanding Online Privacy Policies

Carefully review a site's privacy policy. It is best to thoroughly review the privacy policy of any site that you join in order to understand how your information is being displayed and used. If the privacy policy is overwhelming and confusing, then conduct some research and see what kind of advice or tutorials are offered. Let's take the time to find and review the privacy policies of some popular websites.

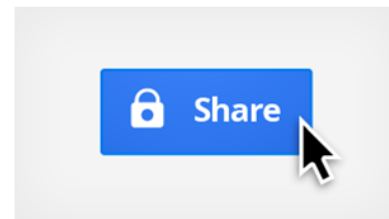
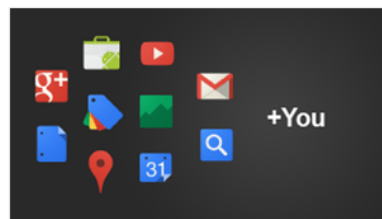
The Google privacy policy center can be found at: <http://www.google.com/intl/en/policies/>



One policy, one Google experience

On March 1, 2012, we changed our Privacy Policy and Terms of Service. We got rid of over 60 different privacy policies across Google and replaced them with one that's a lot shorter and easier to read. The new policy and terms cover multiple products and features, reflecting our desire to create one beautifully simple and intuitive experience across Google.

This stuff matters, so please take a few minutes to read our updated Google [Privacy Policy](#) and [Terms of Service](#), and visit our [FAQ](#) to read more about the changes.



The Facebook privacy policy can be found here: <http://www.facebook.com/about/privacy/>

Data Use Policy

Last updated: September 23, 2011

Information we receive and how it is used

Learn about the types of information we receive, and how that information is used.

Sharing and finding you on Facebook

Get to know the privacy settings that help you control your information on facebook.com.

Sharing with other websites and applications

Find out about the ways your information is shared with the games, applications and websites you and your friends use off Facebook.

How advertising works

See how ads are served without sharing your information with advertisers, and understand how we pair ads with social context, such as newsfeed-style stories.

Minors and Safety

Find out how Facebook protects minors, and what you can do to protect yourself and others online.

Some other things you need to know

Learn how we make changes to this policy and more.



If you have questions or complaints regarding our privacy policy or practices, please contact us by mail at 1601 Willow Road, Menlo Park, CA 94025 or through this [help page](#).

More resources

Interactive Tools

[View the complete Data Use Policy](#)

More Privacy Policy Examples:

Yahoo: yahoo.com/privacy

Twitter: twitter.com/privacy

Amazon: amazon.com/privacy

Most privacy policies can be found from a website's homepage. Let's practice finding and reviewing the privacy policies from a few of the most popular websites.

EXERCISE

Explore various privacy policies.

- Open Internet Explorer
- Go to google.com
 - Click on *Privacy & Terms* at the bottom of the page
 - Review Google's privacy policy and terms of service
- Go to facebook.com
 - Click on *Privacy* at the bottom of the page
 - Review Facebook's privacy policy
- Find and review Yahoo's privacy policy
- Find and review Twitter's privacy policy
- Find and review Amazon's privacy policy

Privacy Settings

You can use social networking sites to keep in touch with friends and family, make new friends or business contacts, or share opinions. These sites allow you to share personal information, opinions and videos or photos. It is important to remember, however, that any information you post on a site could be public and may be seen by other entities.

Most sites allow you to control how public or private your information is: these controls are usually called 'privacy settings' or 'privacy controls'. While some sites set privacy settings automatically at their most "private" level, on others all your information could be available to anyone unless you change the privacy settings. If you don't understand what a particular setting means in practice, don't post any information until you have found out.

Here are a few things you should consider before posting information or images on social networking sites:

- Find out how the available privacy settings can limit access to your personal information.
- Adjust your privacy settings so that information about your family and children is shared only with those you know well.
- Don't include any personal information that could make you vulnerable to identity fraud.
- Think carefully before posting. Think about whether you would want your employer or potential employer to see a particular post, picture, or video.
- Review your information regularly. Something that may have seemed like a good idea at the time may not seem so great a few months or years later.
- Get people's consent before you post their pictures or personal information.
- Use strong passwords to prevent your account being misused.

Most popular websites have learning or help centers to assist you in understanding your privacy options. Be sure to use these resources to discover how to adjust your sharing to your preferred settings. Here are some examples:

<https://www.google.com/dashboard/>

<http://www.facebook.com/help/privacy>

<http://learn.linkedin.com/settings/>

Username

Many services on the web require you to create a user account. Usually this involves at minimum choosing a username and a password.

The username (sometimes referred to as a screen name, login name, or handle), is a pseudonym that can allow you to control the visibility of your identity. A username is often used for instant messengers, forums, and chat rooms. It is the name that you are known by online. You can choose a username that keeps your identity private if you wish (e.g. GuitarPro53). Alternatively, if you want to build an internet reputation for personal or professional reasons, you can choose a username that makes your identity public (e.g. JoeSchmoeGuitarPro).

In many cases your email address may double as a screen name for other services, so it is often useful to have both private and public email accounts. For help in choosing a safe username, you can refer to websites like the following:

http://www.ehow.com/how_2343046_choose-safe-screen-name.html

Passive digital footprints

A passive digital footprint is created when data about your online activities are collected without your consent or knowledge. Essentially, any explicit action on the internet can be captured and stored: any click, keystroke, or mouse movement has the potential to be recorded as data. Some implicit data (sometimes called meta data) can be recorded as well, such as IP address, ISP, location, and context. Here are some examples:

Server logs:

Servers at most websites automatically record the page requests you make. These logs typically include your web request, Internet Protocol address, browser type, browser language, the date and time of your request and one or more cookies that may uniquely identify your browser. This data is not usually accessible to general Internet users. Here is an example of a Google log entry where the search is for “cars”, followed by a breakdown of each piece:

```
123.45.67.89 - 29/Feb/2012 10:15:32 -  
http://www.google.com/search?q=cars -  
Firefox 3.1.6; Windows Vista SP3 - 740654ce2143e969
```

- 123.45.67.89 is the IP address of the computer making the request;
- 29/Feb/2012 10:15:32 is the date and time of the query;
- `http://www.google.com/search?q=cars` is the requested URL, including the search query;
- `Firefox 10.0.2; Windows Vista SP3` is the browser and operating system being used;
- `740654ce2143a969` is the unique cookie ID assigned to this particular computer

Cookies:

A cookie is a small file that is sent to your computer when you visit a website. When you return to the website, the cookie allows that site to recognize your browser. Cookies may store user preferences and other information. You can reset your browser to refuse all cookies or to indicate when a cookie is being sent. However, some website features or services may not function properly without cookies.

Web bugs:

A web bug (also known as a “tracking bug” or a “pixel tag”) is a type of technology placed on a website or within an email for the purpose of tracking activity. It is often used in combination with cookies.

Browser history:

A web browser is a program used to access and interact with information resources on the internet. Some examples are Microsoft Internet Explorer, Mozilla Firefox, and Google Chrome. These programs can store information about the websites you visit, and sometimes send this information to the company that created the program (e.g. Microsoft).

Why is this data collected?

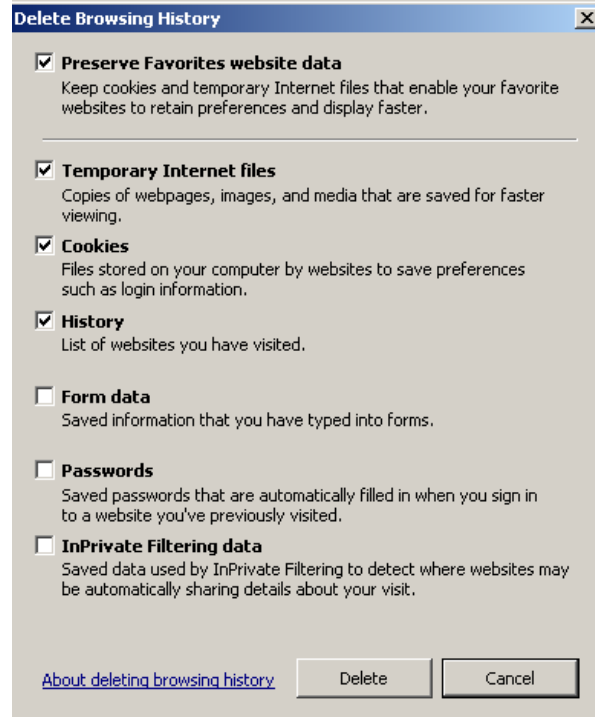
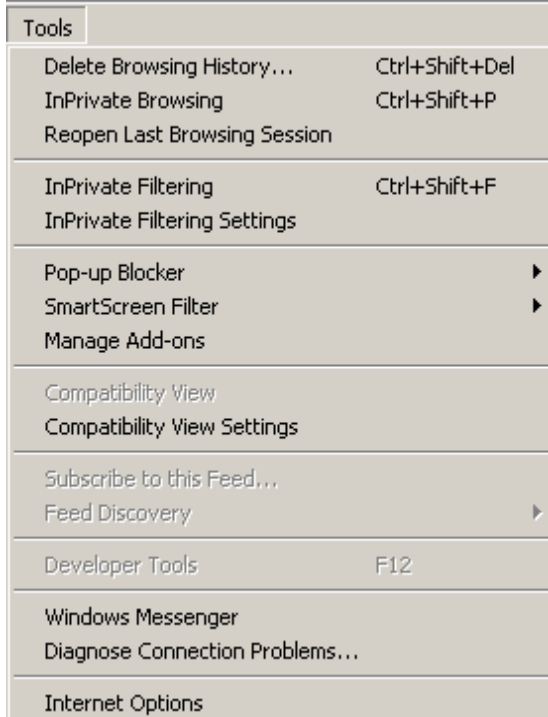
The digital information you leave behind can be extremely valuable to companies for a variety of purposes. Often, data collected from you (the user) is used to build a profile that a company can use to learn what services you would be most likely to use or purchase, to discover your interests in order to determine how to most effectively advertise to you, or simply to improve or personalize how you experience their services. Sometimes this information is depersonalized and converted into statistical information to provide companies with data to improve general marketing and advertising strategy.

What can I do to control my passive footprint?

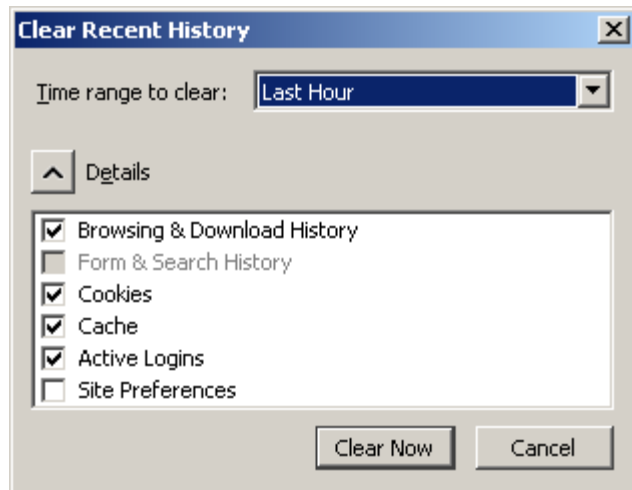
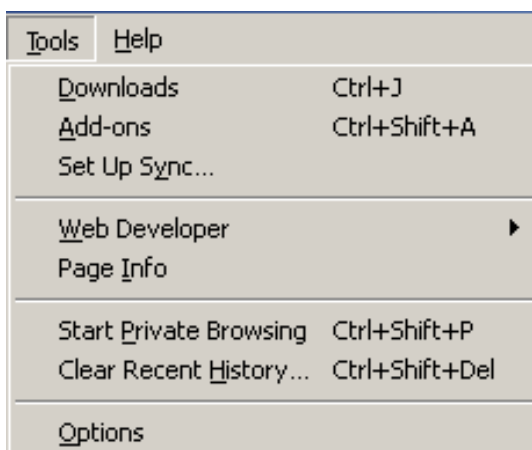
Although you cannot often prevent websites from recording server logs, sending cookies, or implementing web bugs, you can take some steps to protect your privacy. Most importantly, be smart about the websites you visit and the emails that you choose to open. Evaluate links and messages before you decide to click on them, and avoid suspicious or untrustworthy websites.

Browsing and Internet History

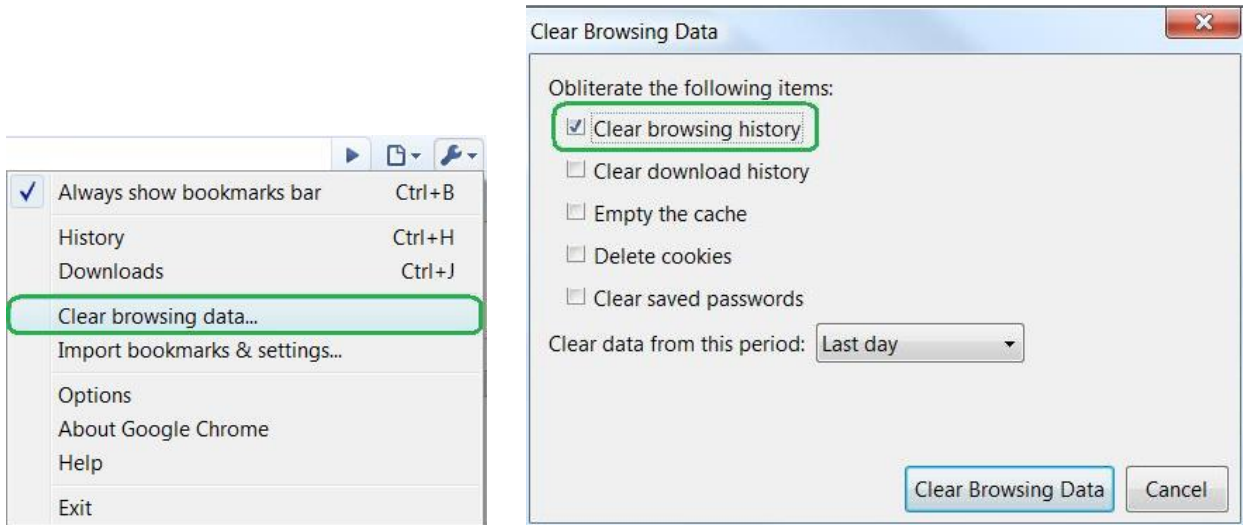
In Internet Explorer, you can clear your browsing history by clicking on Tools in the Menu Bar, and selecting Delete Browsing History from the menu. You can choose whether to delete temporary internet files, cookies, history, and more.



In Mozilla Firefox, you can clear your browsing history by clicking on Tools in the Menu Bar, and selecting Clear Recent History from the menu. You can choose how far back you would like to clear and whether to clear history, cookies, cache, and more.



In Google Chrome, you can clear your browsing history by clicking on the wrench in the upper right corner of the browser and selecting Clear Browsing Data.



Private Browsing

Most browsers will also have an option in the Tools menu for private browsing sessions. This is called *InPrivate Browsing* in Internet Explorer, *Private Browsing* in Mozilla Firefox, and *Incognito* in Google Chrome. Here is how private browsing is explained in Google Chrome:

You've gone incognito. Pages you view in this window won't appear in your browser history or search history, and they won't leave other traces, like cookies, on your computer after you close the incognito window. Any files you download or bookmarks you create will be preserved, however.

Going incognito doesn't affect the behavior of other people, servers, or software. Be wary of:

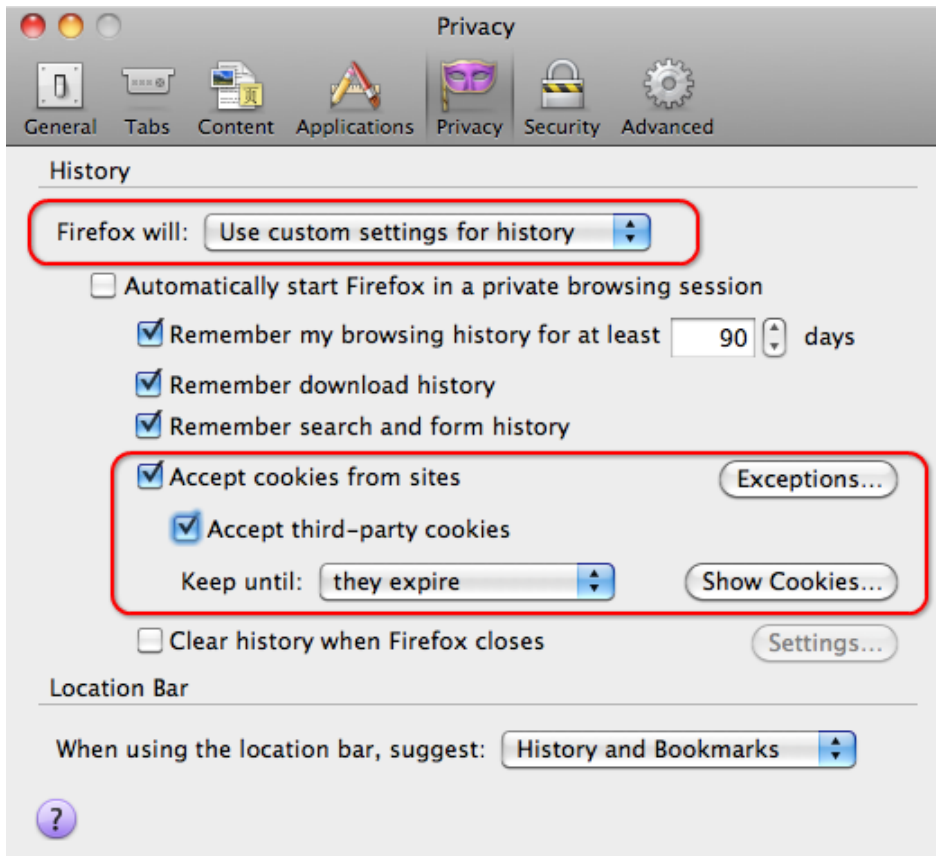
- Websites that collect or share information about you
- Internet service providers or employers that track the pages you visit
- Malicious software that tracks your keystrokes in exchange for free smileys
- Surveillance by secret agents
- People standing behind you

[Learn more](#) about incognito browsing.

Cookie Settings

You can also adjust your cookie settings in your browser. In general you will find these settings in the Tools menu, under Internet Options: you can choose whether to accept cookies automatically, after prompting, or not at all; you can block cookies from certain websites; you can decide whether to keep cookies or have them deleted when you close the browser.

Remember that cookies store information about your computer, but they can also improve and customize your experience on your favorite websites, and some services will not work at all without cookies enabled. On the next page is a picture of the cookies settings in Mozilla Firefox:



Browser Extensions

Browsers extensions (sometimes called plug-ins or add-ons) are programs that perform additional or complimentary functions for your browser. Some of them, like Adobe Flash Player, can greatly enrich your online experience. However, be aware that these programs may store information about your online activities. Be careful to consider this before installing toolbars or plug-ins.

Other Passive Footprints

Passive digital footprints can also include digital records about you that have nothing to do with your own actions on the internet: ID photos, prescription medicines, driver's license records, college transcripts, organization memberships, and tax and bank records. These records—usually stored securely in organization or government databases—are usually not available to the public, but they still constitute part of your digital footprint. Here are two examples:

Political contributions you make are public actions and can be found online:

fundrace.huffingtonpost.com

Property ownership records are public and can be found online:

fiscalofficer.cuyahogacounty.us/en-US/REPI.aspx

Your Online “Brand” / Online Reputation Management

When you hear the word “brand” you probably think of products like Coca-Cola, Budweiser, Ford, or Apple, but individuals can have brands too. Your online brand is basically the public information on the internet from which people can form an opinion about you. You can use your brand as a way to market yourself to others by creating public profiles that emphasize your interests, skills, and accomplishments. Alternatively, you can try to avoid having a brand by controlling the privacy of all of your personal information.

How you formulate your brand is completely up to you. We all know that celebrities and their agents love to use online branding to increase their popularity and fame. They may create Facebook, Twitter, and YouTube accounts using their real names and build large followings. Even if you aren’t a celebrity or public figure, you can build a brand to promote your knowledge in your profession or make people aware of your business or enterprise.

Here are some links to help you go about creating your own brand. There are many resources out there; these are just a few:

Steps you can take to lower your Google profile:

<http://www.wikihow.com/Ungoogling-Yourself>

<http://www.youtube.com/watch?v=3vFr3dt8ZHM>

Building a personal brand online:

<http://www.readwriteweb.com/start/2011/10/how-do-you-manage-your-online.php>

<http://publicspeaker.quickanddirtytips.com/how-to-Manage-Your-Online-Presence.aspx>

Internet Privacy Resources

Great online tutorial about internet safety:

<http://www.gcflearnfree.org/internetsafety/1>

U.S. Government website on internet security:

<http://onguardonline.gov/>

Online privacy protection information:

<http://www.privacyrights.org/Online-Privacy-and-Technology>

Google Privacy YouTube account:

<http://www.youtube.com/user/googleprivacy>

Video tutorial for using the Google dashboard:

http://www.youtube.com/watch?v=ZPaJPxhPq_g

