Have you ever wondered why some online ads you see are targeted to your tastes and interests? Or how websites remember your preferences from visit-to-visit or device-to-device?

The answer may be in the “cookies”---or in other online tracking methods, like “device fingerprinting” or “cross-device tracking.”

Here are specific answers provided by Amy Hebert, Consumer Education Specialist, Federal Trade Commission, to some commonly asked questions about online tracking—how it works and how you can control it.

**UNDERSTANDING COOKIES**

- **What is a cookie?**
  A cookie is information saved by your personal web browser, the software program you use to visit the web. When you visit a website, the site might store a cookie so it can recognize your device in the future. Later if you return to that site, it can read that cookie to remember you from your last visit. By keeping track of you over time, cookies can be used to customize your personal browsing experience, or to deliver ads targeted to you.

- **Who places cookies on the web?**
  First-party cookies are placed by the site that you visit. They can make your experience on the web more efficient. For example, they help sites remember:
  - Items in your shopping cart;
  - Your log-in name;
  - Your preferences, like always showing the weather in your home town; and
  - Your high game scores.

  Third-party cookies are placed by someone other than the site you are on. For example, the website may partner with an advertising network to deliver some of the ads you see. Or they may partner with an analytics company to help understand how people use their site. These “third-party” companies also may place cookies in your personal browser to monitor your behavior over time.

  Over time, these companies may develop a detailed history of the types of sites you frequent, and they may use this information to deliver ads tailored to your interests. For example, if an advertising company notices that you read a lot of articles about running, it may show you ads about running shoes---even on an unrelated site you’re visiting for the first time.
UNDERSTANDING OTHER ONLINE TRACKING

• What are Flash cookies?
A Flash cookie is a small file stored on your personal computer by a website that uses Adobe’s Flash player technology. Flash cookies use Adobe’s Flash player to store information about your online personal browsing activities. Flash cookies can be used to replace cookies used for tracking and advertising, because they also can store your settings and preferences. Similarly, companies can place unique HTML5 cookies within a browser’s local storage to identify a user over time. When you delete or clear cookies from your personal browser, you will not necessarily delete the Flash cookies stored on your personal computer.

• What is device fingerprinting?
Device fingerprinting can track devices over time, based on your personal browser’s configurations and settings. Because each browser is unique, device fingerprinting can identify your personal device, without using cookies. Since device fingerprinting uses the characteristics of your browser configuration to track you, deleting cookies won’t help.

Device fingerprinting technologies are evolving and can be used to track you on all kinds of internet-connected devices that have browsers, such as smart phones, tablets, and laptop and desktop computers.

• How does tracking in mobile apps occur?
When you access mobile applications, companies don’t have access to traditional browser cookies to track you over time. Instead, third-party advertising and analytics companies use device identifiers—such as Apple iOS’s Identifiers for Advertisers (IDFA) and Google Android’s Advertising ID—to monitor the different applications used on a particular device.

• Does tracking of other “smart devices” occur?
Yes. More and more, consumer devices, in addition to phones, are capable of being connected online. For example, smart entertainment systems often provide new ways for you to watch TV shows and movies, and also may use technology to monitor what you watch. Look to the settings on your devices to investigate whether you can reset identifiers on the devices or use web interfaces on another device to limit ad tracking.

CONTROLLING ONLINE TRACKING

• How can I control cookies?
Various browsers have different ways to let you delete cookies or limit the kinds of cookies that can be placed on your personal computer. When you choose a browser, consider which suits your privacy preferences best.

To check out the settings in a browser, use the “Help” tab or look under “Tools” for settings like “Options” or “Privacy.” From there, you may be able to delete cookies, or control when they can be placed. Some browsers allow add-on software tools to block, delete, or control cookies. And security software often includes options to make cookie control easier. If you delete cookies, companies may not be able to associate you with your past browsing activity. However, they may be able to track you in the future with a new cookie.
If you block cookies entirely, you may limit your personal browsing experience. For example, you may need to enter information repeatedly, or you might not get personalized content that is meaningful to you. Most browsers’ settings will allow you to block third-party cookies without also disabling first-party cookies.

• **How can I control Flash cookies and device fingerprinting?**
The latest versions of Google Chrome, Mozilla Firefox, and Microsoft Internet Explorer let you control or delete Flash cookies through the browser’s settings. If you use an older version of one of these browsers, upgrade to the most recent version, and set it to update automatically.

If you use a browser that doesn’t let you delete Flash cookies, look at Adobe’s Website Storage Settings panel. There, you can view and delete Flash cookies, and control whether you’ll allow them on your personal computer.

Like regular cookies, deleting Flash cookies gets rid of the ones on your personal computer at that moment. Flash cookies can be placed on your computer the next time you visit a website or view an ad unless you block Flash cookies altogether.

• **How can I control tracking in or across mobile apps?**
You can reset the identifiers on your personal device in the device settings. iOS users can do this by following Settings > Privacy > Advertising > Reset Advertising Identifier. For Android, the path is Google settings > Ads > Reset advertising ID. This control works much like deleting cookies in a browser—the device is harder to associate with past activity, but tracking can start anew using the new advertising identifier.

You also can limit the use of identifiers for ad targeting on your personal devices. If you turn on this setting, apps are not permitted to use the advertising identifier to serve consumers’ targeted ads. For iOS, the controls are available through Settings > Privacy > Advertising > Limit Ad Tracking. For Android, Google Settings > Ads > Opt Out of Interest-Based Ads. Although this tool will limit the use of tracking data for targeting ads, companies may still be able to monitor your app usage for other purposes, such as research, measurement, and fraud prevention.

Mobile browsers work much like traditional web browsers, and the tracking technologies and user controls are much the same as for ordinary web browsers, described above.

Mobile applications also may collect your geolocation to share with advertising companies. The latest versions of iOS and Android allow you to limit which particular applications can access your location information.

• **What is “private browsing?”**
Many browsers offer private browsing settings that are meant to let you keep your personal web activities hidden from other people who use the same computer. With private browsing turned on, your personal browser won’t retain cookies, your browsing history, search records, or the files you downloaded. Privacy modes aren’t uniform, though; it’s a good idea to check your browser to see what types of data it stores.

But note that cookies used during the private browsing session still can communicate information about your personal browsing behavior to third parties. So, private browsing may not be effective in stopping third parties from using techniques, such as fingerprinting, to track your web activity.
• **What are “opt-out” cookies?**
Some websites and advertising networks allow you to set cookies that tell them not to use information about what sites you visit to target ads to you. For example, the Network Advertising Initiative (NAI) and the Digital Advertising Alliance (DAA) offer tools for opting out of targeted advertising—often by placing opt-out cookies. If you delete all cookies, you’ll also delete the cookies that indicate your preference to opt out of targeted ads.

Cookies are used for many purposes—for example, to limit the number of times you’re shown a particular ad. So even if you opt out of targeted advertising, a company may still use cookies for other purposes.

• **What is “Do Not Track?”**
“Do Not Track” is a setting in most internet browsers that allows you to express your preference not to be tracked across the web. Turning on “Do Not Track” through your personal web browser sends a signal to every website you visit that you don’t want to be tracked from site to site. Companies then know your preference. If they have committed to respect your “Do Not Track” preference, they are legally required to do so. However, most tracking companies today have not committed to honoring users’ “Do Not Track” preferences.

• **Can I block online tracking?**
Consumers can learn about tracker-blocking browser plugins, which block the flow of information from a computer to tracking companies and allow consumers to block ads. They prevent companies from using cookies or fingerprinting to track your personal internet behavior.

To find tracker-blocking plugins, type “tracker blocker” in your search engine. Then, compare features to decide which tracker blocker is best for you. For example, some of them block tracking by default, while others require you to customize when you’ll block tracking.

Remember that websites that rely on third-party tracking companies for measurement or advertising revenue may prevent you from using their site if you have blocking software installed. However, you can still open those sites in a separate browser that doesn’t have blocking enabled, or you can disable blocking on those sites.

***************

For more information or to file a complaint, contact Pinellas County Consumer Protection at (727) 464-6200 or visit www.pinellascounty.org/consumer.