Focus On...

How Companies Are Tracking Your Data

Businesses and others are regularly gathering information about you — whether you're at the store, in your car or at home.

Understanding how your data gets collected can help you take more control of your privacy. Here's a look at situations in daily life in which you may be sharing personal information without realizing it.

Browsing the Internet
That search engine you're using to find websites or information tracks your browsing activity. It then analyzes this behavior to target ads to you.

Listening to Music
When you activate an Amazon Echo or Google Home speaker with your voice, those companies record what you utter. Doc Searls, editor in chief at the Linux Journal, calls smart speakers "a personal data fire hose squirting from your house."

Shopping Online
Amazon and other online retailers have made it an art form to track not only your purchasing patterns but also what items you viewed so that they can recommend more products that align with your interests and needs.

Watching TV
Some smart TVs can collect your viewing data and other information. New models typically ask your permission first, but it's not always easy to understand what you're agreeing to. If you have an older set, it may be tracking you by default — and you'd have to opt out.

Cooking a Meal

Many new models of kitchen appliances, thermostats, light bulbs, light switches, door locks and more can be controlled from a phone or remote device, presenting new privacy and data security challenges. Transmitted data can even indicate whether you are home.

Researching Your Genealogy
Businesses like 23andMe and Ancestry promise to reveal your genetic relatives based on the DNA from a saliva sample. But who's able to peek at that data? Recent criminal cases reveal that police are working with such services to gather information for investigations.

Visiting Your Doctor
Pacemakers, defibrillators and other medical devices are now often connected to your doctor or hospital, transmitting medical information.

Surfing the Web at a Coffeehouse
Beware of eavesdroppers on free Wi-Fi networks. The person next to you could be using a tool called a packet sniffer to see what data you're sending to the websites you visit.

Shopping at a Store
Those cards that get you discounts at stores and restaurants and other businesses are used to track your name, address and what you buy.

Getting Your Computer Fixed
Got a problem with your computer? The repair team at that big-box store can help. But recent reports revealed that employees at Best Buy were paid by the FBI to notify them of possible illegal content on customers' computers.

Driving
E-ZPass and other toll transponders create a log of your locations. Also, speed or red-light cameras at key locations snap license plate numbers, along with the date, time and location. And some auto insurance companies may want to track your driving with a device installed in your car that transmits data.

Doing Research at the Library
If you go to the library, and use a public internet kiosk there and forget to log out, the data you saved and the websites you visited will be available to the next person. Be sure to clear your history, logins and other information before leaving.

Exercising
The fitness tracker on your wrist collects data on your workouts, exercise routines and location. That information is shared with the manufacturers and can be synced with your social media accounts.

Renting a Car
Connecting your phone to the onboard electronics in a rental car could be risky. Anyone who uses the car afterward may be able to go through the car's menus and see what calls you made, and they may even be able to find out your contact list.

Taking a Walk
Your phone's location service tracks you and may share that data with certain apps. Also, surveillance cameras are increasingly used in public places to aid police investigations or to monitor for suspicious activity.

How to Protect Yourself
Use a VPN. Virtual Private Networks are secure data "tunnels" that protect online activity from prying eyes.
Change web browsers. A few, such as Tor or Epic Privacy Browser, prevent snoopers from seeing the sites you visit and stop websites from tracking you.
Search anonymously. Search engines such as DuckDuckGo and StartPage block ad trackers and keep your search history private.
Be wary when using apps. Many ask for access to your contacts, photos and other information. Decline first and see how the app runs without sharing that info.
Don't share your location. "If you go for a walk that your fitness app tracked, don't post your path on Facebook.

Source: Lance Whitney, AARP Bulletin, October 3, 2018

AWARENESS

Focus Audits, LLC
11301 N. US Hwy. 301
Ste. 105
Thonotosassa, FL 33592
(813) 638-8565
www.FocusAudits.com