P. 42 VIOLINIST OVERCOMES VISION LOSS
P. 44 Q&A: ERIC IDLE

HOW THEY TRACK YOU

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

BY LANCE WHITNEY

You can assume that most tasks you perform on a phone or computer—pay a bill, send a photo, share a joke or buy a gift—are recorded by some business or organization. But the tracking of your information doesn't end there. Your phone might be silently transmitting your location. Your debit or credit card swipes will mark what you bought and where you bought it. Your alarm system keeps records of when you lock your doors.

Most of this is done legally, and with good intentions. As companies collect more data about you and your preferences, they presumably can deliver more personalized information and experiences. Some data collection is merely a function of a product itself; a fitness tracker that can't locate you can't record how many miles you ran today, for example.

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.

Lance Whitney has written for Time, *CNET and* PC Magazine. *He's also the author of tech books.*

Illustrations by CHRIS O'RILEY

RESEARCHING YOUR GENEALOGY

Businesses like 23andMe and Ancestry .com 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," says Ray Klump, professor and chair of computer science and mathematics at Lewis University.

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.

OUT AND ABOUT

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.

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," Klump says.

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," Klump says. Browsers offer a setting through which you can clear your history, logins and other info.

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.

TAKING A WALK

Your phone's location service tracks you and may share that data with certain apps. Says Jeff Wilbur, technical director of the Online Trust Alliance: "We love the benefit of our smartphones as GPS or to utilize ride-sharing or similar location-based services, but by default those apps track and log a tremendous amount about your location history." Also, surveillance cameras are increasingly used in public places, to aid police investigations or 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. Search "VPN" on the web to find services; most charge a small monthly fee.

Change web browsers. A few, like 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, even for bragging rights, because then people see very clearly where you live and when you're away," says Ray Klump, professor of computer science and mathematics at Lewis University.