



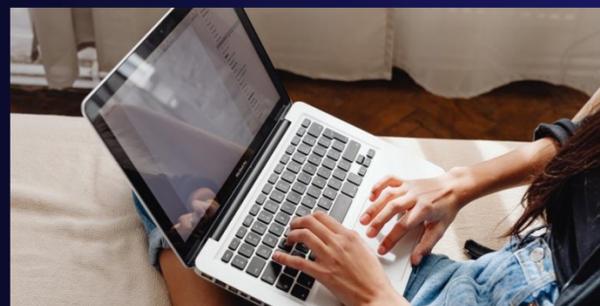
**DEXIT**



# Who is watching?

**How Your Everyday Devices Are Collecting  
Data — And What You Can Do About It**

# EVERYDAY DEVICES THAT SPY ON YOU



# YOUR PHONE KNOWS EVERYTHING



**Location Tracking**



**Microphone Access**



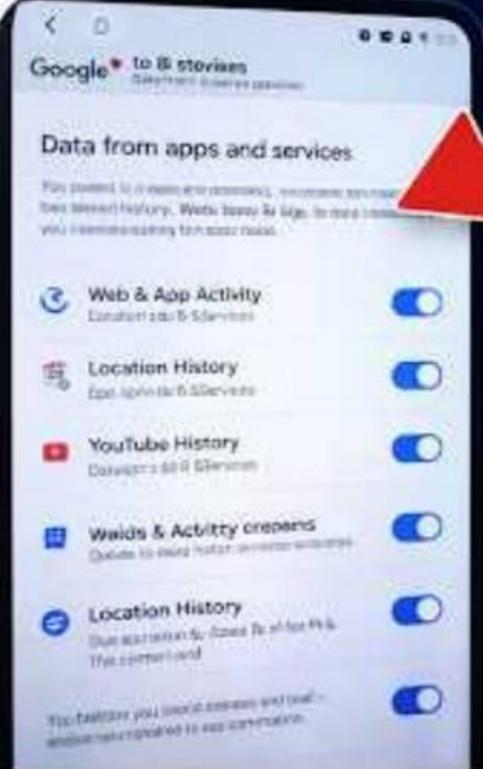
**App Data Collection**



**Advertising ID**

**There is data on your phone you cannot see, cannot delete, and that may be sold to companies you have never heard of.**

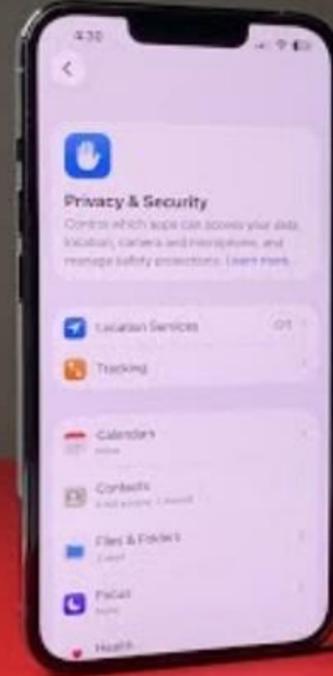
# IPHONE AND ANDROID PHONES SHARING DATA



**YOUR ANDROID PHONE IS SHARING THIS DATA**  
— HERE'S HOW TO STOP IT



The image shows a screenshot of an Android phone's Google account settings page. The page is titled "Data from apps and services" and lists several tracking options with toggle switches: "Web & App Activity", "Location History", "YouTube History", "Waits & Activity trends", and "Location History". A red arrow points from the text "YOUR ANDROID PHONE IS SHARING THIS DATA" to the "Data from apps and services" section. A red play button icon is overlaid on the text, and a red toggle switch is shown below it.



**Your iPhone is Tracking You!**  
CHANGE THESE SETTINGS NOW!



The image shows a screenshot of an iPhone's "Privacy & Security" settings page. The page lists several tracking options with toggle switches: "Location Services", "Tracking", "Calendar", "Contacts", "Files & Folders", "Facial", and "Health". A red play button icon is overlaid on the text, and a grey gear icon is shown below it.

# SMART SPEAKERS THAT ARE ALWAYS

Amazon Echo, Google Nest, and Apple HomePod are convenient — but their microphones **LISTENING** never fully switch off.



**WAKE WORD MONITORING**



**ACCIDENTAL RECORDING**



**CLOUD STORAGE**





# THE TV THAT WATCHES YOU BACK

**ACR TECHNOLOGY**

**MICROPHONES IN TVS**

**WHAT GETS TRACKED**





# YOUR CAR MAY BE TRACKING YOU

**⚠️ WATCH OUT:** When you sell, trade in, or return a rental car, factory reset it first. Your location history and phone contacts go with it.



**LOCATION HISTORY**



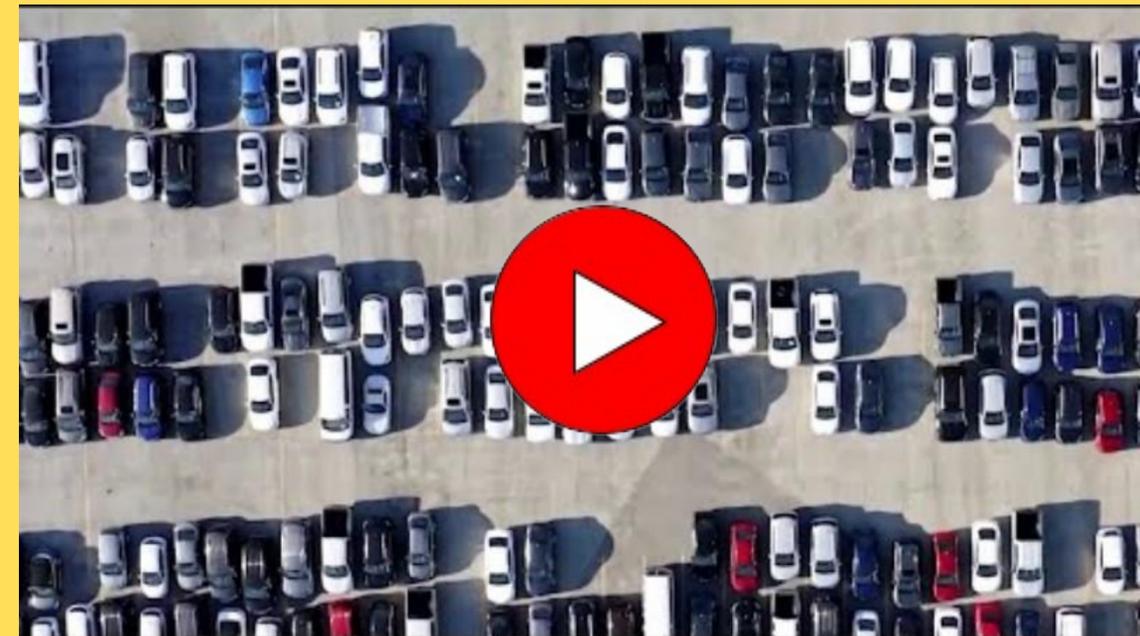
**DRIVING BEHAVIOR**



**YOUR PHONE GETS COPIED**



**WORST PRIVACY RECORD**





# DOORBELLS AND SECURITY

✓ **TIP: You can turn off Community Requests in your Ring app and enable End-to-End Encryption to prevent Ring from accessing your footage.**

## CAMERAS



**Police can request your footage**



**Familiar Faces Facial Recognition**



**What Ring Shares When You Respond**



**FTC Fined Ring \$5.8 Million**



# FITNESS WATCHES AND HEALTH TRACKERS

**⚠️ WATCH OUT:** Wearable health data is not medical-grade protected. It can be subpoenaed in court and used in insurance decisions legally.



**What They Collect**



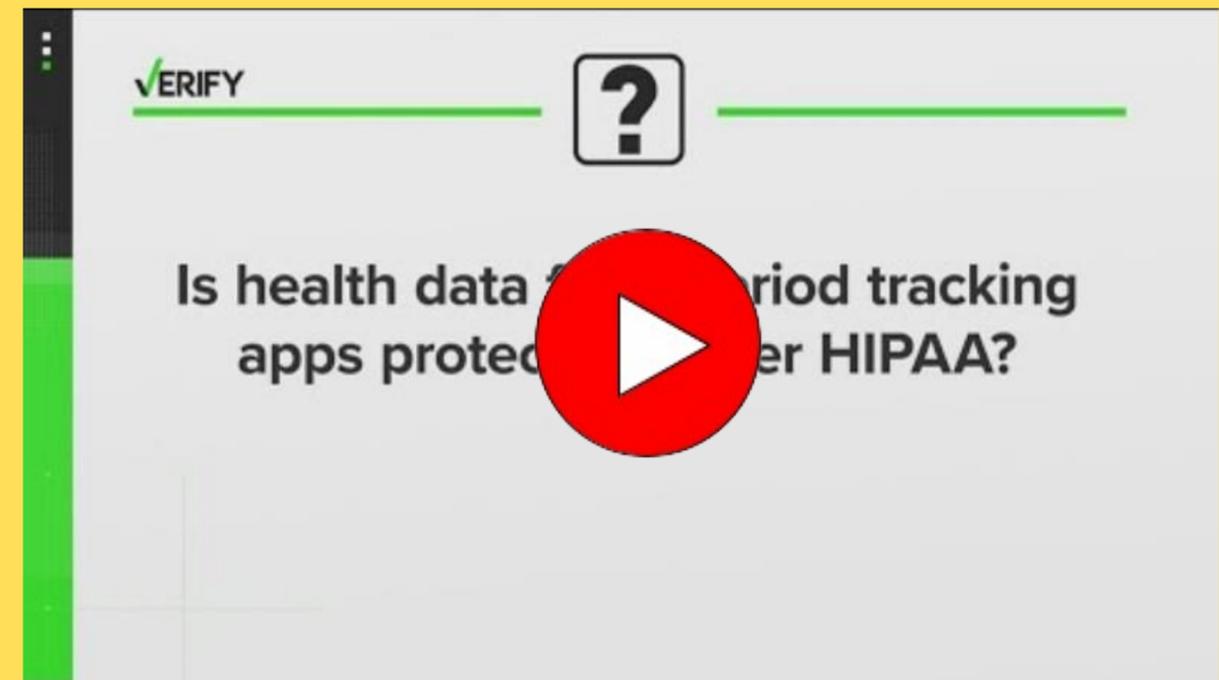
**Not Covered by HIPAA**



**Insurance and Legal Risk**



**Google Bought Fitbit**



*Your Fitbit, Apple Watch, or Garmin knows more about your body than most doctors — and it is not covered by medical privacy law.*



# SMART HOME DEVICES

*Your thermostat, smart lights, and refrigerator are all sending data about your daily life to servers around the world.*



**Smart Thermostats**



**Smart Refrigerators**



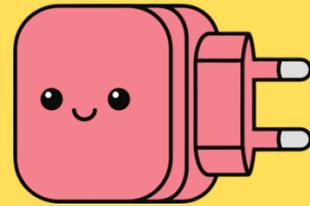
**⚠WATCH OUT:** The average U.S. home now has 25 connected devices. Each one is both a data source and a potential security door left open.



# HIDDEN CAMERAS IN ORDINARY OBJECTS



**Alarm Clocks**



**Phone chargers**



**Picture frames**



**Water Bottles**

***Hidden cameras are sold legally online for under \$30, disguised as chargers, clocks, smoke detectors, and pens.***

**Ordinary objects placed at unusual angles.**

**The FTC has issued consumer warnings specifically about hidden cameras in Airbnbs and vacation rentals.**



# WiFi Routers and Internet Providers



**IPS Monitoring**



**Router Logs**



**DNS Tracking**



**Public WiFi Risk**

***Your internet provider can see every website you visit — and since 2017, U.S. law allows them to sell that information.***

# APPS THAT KNOW MORE THAN YOU THINK

*The apps on your phone are among the most aggressive data collectors — and the least transparent about what they take.*



**Free Apps = You Pay with Data**



**What Gets Collected**



**Third-Party Trackers**



**Ask This Question**



**WATCH OUT:** Deleting an app from your phone does **NOT** delete the data it already collected. That data may be stored indefinitely by the company.



# TOYS AND BABY MONITORS

**Internet-connected toys and baby monitors have microphones and cameras and some have been hacked or used to collect children's data illegally.**

**✓TIP: Before buying a connected toy as a gift, check whether it collects voice or video data. The packaging often does not make this obvious.**



# ONLINE SHOPPING AND LOYALTY

Every purchase, every search, every click **PROGRAMS** being recorded – and built into a permanent profile of your habits and preferences.

✓**TIP:** Use private/incognito browsing when shopping online – it clears tracking cookies between sessions and can result in lower prices.

**amazon**



**Amazon Tracks Everything**

**Grocery Loyalty Cards**

**You May Pay Different Prices**

**Email Receipts Track You**

# WHAT WE DID NOT COVER, BUT YOU SHOULD KNOW

 **Email Providers (Gmail, Outlook)**

 **Social Media (Facebook, Instagram)**

 **Health and Medication Apps**

 **Data Brokers Have a File on You**

 **Your Bank Sells Data Too**

 **[Your Digital Life Needs a Plan \(DEXITPLAN\)](#)**



**THANK YOU**

**[WWW.DEXITPLAN.COM](http://WWW.DEXITPLAN.COM)**