Your data is the product.

Shops, apps and phones quietly collect a lot about you. Here is how to take some control back.

LOYALTY CARDS: POINTS FOR YOUR DATA

Every time you scan a loyalty card, the program records what you bought, when and where. Over months that builds a detailed picture of your household. Consumer group CHOICE calls these programs a "data goldmine", used for targeted marketing and personalised pricing, and warns the data may be shared with insurers or data brokers.

Sydney Morning Herald, 2013: Woolworths said it had "overlaid" its insurer's car-crash database with Everyday Rewards data to find the best customers to target for insurance. The retailers say the data is de-identified, but a privacy lawyer warned it can often be re-identified.

TRACKING IN STORES

Your phone's signals

CHOICE: "If you have Wi-Fi or Bluetooth enabled on your phone, many retailers can use it to track your movements."

"Free" Wi-Fi

Joining can hand over your details and browsing activity. The price of free Wi-Fi is often your data.

Watching cameras

Some digital billboards have hidden cameras that estimate a viewer's age and gender before choosing which ad to show.

FACES AT THE DOOR

Australia's privacy regulator found two big retailers scanned shoppers' faces unlawfully.

Bunnings: faces of hundreds of thousands of customers analysed in 62 stores (2018 to 2021). Found to have breached the Privacy Act in 2024; Bunnings has said it will seek a review.

Kmart: facial recognition used in 28 stores, collecting sensitive biometric data without notice or consent. Found to have breached the Privacy Act in 2025.

SMALL STEPS YOU CAN TAKE TODAY

1. **Switch off Wi-Fi and Bluetooth** when you're out, and skip "free" Wi-Fi sign-ups.
2. **Join loyalty programs sparingly.** Give only what's needed and opt out of data sharing.
3. **Ask what they hold.** You can ask any company for the personal information it keeps on you.

Sources: CHOICE, "How retail stores are tracking you" (2023) · iTnews and the OAIC on the Bunnings determination (Nov 2024) · CHOICE on the OAIC Kmart determination (Sept 2025) · Sydney Morning Herald, "Supermarket spies: big retail has you in its sights" (16 Sept 2013) · oaic.gov.au, Australian Privacy Principles.

APCSC is an independent business and is not affiliated with the Australian Government or the Australian Cyber Security Centre.

ABN 13 262 392 536 · © 2026

Big companies slip up too.

Even large organisations have misled customers or lost their data, so you can't count on them to protect your privacy for you. The less you hand over, the less there is to lose.

RECENT AUSTRALIAN EXAMPLES

Google · 2022
$60 MILLION PENALTY

The Federal Court found Google misled Android users. Turning off "Location History" did not stop location data being collected through another setting that was on by default.

Meta (Facebook) · 2024
$50 MILLION SETTLEMENT

Personal information of some Australian users was disclosed to a quiz app, exposing it to the risk of reaching Cambridge Analytica and being used for political profiling.

Medibank · 2022
9.7 MILLION CUSTOMERS

Hackers stole and released customers' data, including sensitive medical information. The privacy regulator has taken Medibank to court, alleging it failed to protect it.

TURN DOWN THE TRACKING · 15 MINUTES

1. **Google:** in your Google Account under Data & privacy, set Web & App Activity and Location History to off or auto-delete, and turn off ad personalisation.
2. **Facebook and Instagram:** in Meta's Accounts Center, review your ad preferences and the activity other businesses share with Meta, and limit what you can.
3. **Your phone:** delete the advertising ID (the number apps use to follow you between apps), and set each app's location to "only while using" or "never".
4. **Your smart TV:** many identify what you watch. Look in the privacy settings for "viewing information" or "content recognition" and switch it off.

Settings menus change often and are not always easy to find. If you would like a hand going through them, ask us at your home audit.

Sources: ACCC media release, "Google LLC to pay $60 million for misleading representations" (accc.gov.au, Aug 2022) · Office of the Australian Information Commissioner (oaic.gov.au): Meta settlement (Dec 2024) and Medibank proceedings (Information Age, June 2024).

APCSC is an independent business and is not affiliated with the Australian Government or the Australian Cyber Security Centre.

ABN 13 262 392 536 · © 2026

Go further, step by step.

Once the quick wins are done, these changes make the biggest difference over time. You do not need to do them all at once.

NEXT LEVEL

1. **Switch browser and search engine.** Firefox or Brave with the uBlock Origin ad blocker, and DuckDuckGo or Brave Search. This blocks much of the tracking that follows you around the web.
2. **Use a different email address for each shop and service.** Alias services such as SimpleLogin or addy.io do this (Bitwarden can create the aliases for you). If an address leaks, switch it off without losing your real inbox.
3. **Message with Signal.** Conversations are end-to-end encrypted, and the app collects almost nothing about you.
4. **Block trackers across the whole house.** A DNS filter such as NextDNS or AdGuard Home, or the filtering built into your router, covers every device, including smart TVs. We can set this up for you.
5. **Post less, and check who can see it.** Think before sharing photos, your location or your children's details.

Beware of quick fixes. A VPN moves your trust from your internet provider to the VPN company. It helps on public Wi-Fi, but it does not stop Google or Meta tracking you while you are signed in. Private or incognito mode only hides your history from other people using the same device.

WE RECOMMEND

GrapheneOS

A free, open-source, privacy-focused operating system for Google Pixel phones. You decide what each app can reach: switch off an app's network access or sensors, keep banking and shopping in separate profiles, and optionally run Google Play sandboxed so most apps still work. Updates arrive automatically.

Good to know: it needs a supported Pixel (see the list on the website), Google Wallet tap-to-pay isn't supported, and a few apps may not work. Test your must-have apps first. We can help you choose, set up and test.

grapheneos.org

Scan to visit

Sources: GrapheneOS features (grapheneos.org/features). Other products named are examples of the kinds of tools available.

APCSC is an independent business and is not affiliated with the Australian Government or the Australian Cyber Security Centre.

ABN 13 262 392 536 · © 2026