



A KIWI GUIDE TO OPTING OUT OF SURVEILLANCE CAPITALISM

# Take Back *Your Data*

Every time you scroll, click, or swipe, your data is harvested, then sold by digital data brokers to advertisers, insurers, political campaigns, and more. In Aotearoa, we're not immune. Our personal details appear on offshore databases, scraped and commodified without consent.

But you're not powerless. This guide offers everyday Kiwis a path to reclaiming privacy, resisting surveillance capitalism, and shifting power away from the tech billionaires profiting off our lives.

Haere tonu, let's go and get you safer online.

# 01 Free your data from AI tools

## Free your data from ChatGPT

- 1 Log into ChatGPT.
- 2 Go to **Profile** → **Settings** → **Data Controls** → turn off "**Improve the model for everyone.**"

This only stops future conversations from training the model. It doesn't touch what's already in your history — for that, go to **Settings** → **General** → **Delete all chats**.

Thinking of using Temporary Chat instead? It skips your history and isn't used for training or memory, but OpenAI still holds onto it behind the scenes for up to 30 days for safety and abuse monitoring. Not quite the vanishing act the name suggests.

While you're in Data Controls, you'll also find:

- ◆ **Export your data** — get a copy before you delete anything
- ◆ **Delete your account**
- ◆ **Manage Memory** — what ChatGPT remembers about you between chats
- ◆ **Privacy Portal** — for formal data requests

### BEFORE YOU PASTE ANYTHING IN

Don't upload sensitive personal, health, employment or client information to any AI tool just to get it summarised. Even with training switched off, most providers still keep what you send them for a while — for safety review, abuse prevention and legal reasons. Turning off training isn't the same as nothing ever touching their servers.

### MYTH TO RETIRE

"AI incognito" isn't one universal setting you flip once, covering every AI tool. ChatGPT, Claude, Gemini and the rest each have their own controls, their own definition of "temporary," and their own retention window behind that definition. Check each one on its own terms.

## Why some Kiwis are looking at Claude instead

If you're weighing up ChatGPT against Anthropic's Claude, here's the honest comparison rather than the sales pitch:

- ◆ Both now default new users into a choice, not a free pass. ChatGPT's "Improve the model for everyone" and Claude's "Help Improve Claude" are both toggles you have to actively manage.
- ◆ Both have a genuine incognito/temporary mode, and on both, that mode is excluded from training even if your main account setting says yes.
- ◆ Anthropic states that, by default, staff can't access your individual conversations without your consent or a safety flag on the content — a more explicit access restriction than OpenAI publishes.
- ◆ Retention shapes are similar: opt into training on either platform and your data can be kept for years. Opt out or delete, and both still keep a shorter backend copy (roughly 30 days) for safety and fraud checks first.
- ◆ For business and API accounts, both companies say they don't train on customer data by default, so this mostly matters for personal, free-tier use.

Bottom line: switching to Claude isn't a shortcut to zero data collection. Run the same audit either way — training off in Privacy Settings, Incognito for anything sensitive.

# 02Data removal services

Prices below are labelled by check date rather than stated as fixed, since they drift.

## Free tools (unchanged — all confirmed working in NZ Jul 26)

| Service                                | Coverage                | Works in NZ?      | Best for                                  |
|----------------------------------------|-------------------------|-------------------|-------------------------------------------|
| Manual Opt-Out                         | Broker-specific         | Yes               | DIYers                                    |
| SimpleOptOut.com                       | 150+ brokers            | Yes               | Tech-savvy Kiwis                          |
| DuckDuckGo Privacy Tools               | Trackers, ads           | Yes               | Everyday browsing                         |
| Firefox (Enhanced Tracking Protection) | Web privacy             | Yes               | General web use                           |
| uBlock Origin — full version           | Ads, trackers           | Yes, Firefox only | Advanced users willing to switch browsers |
| uBlock Origin Lite — Chrome/Edge       | Ads, trackers (reduced) | Limited filtering | Chrome/Edge users who can't switch        |

## Paid data removal services (pricing checked July 2026)

| Service | Price               | Works in NZ?        | Notes                                                                                                                                         |
|---------|---------------------|---------------------|-----------------------------------------------------------------------------------------------------------------------------------------------|
| Optery  | NZD, Free—~\$300/yr | Yes                 | Officially launched for NZ residents in 2026 with its own NZD pricing page — currently the only paid service here confirming NZ availability. |
| Kanary  | USD                 | Check before paying | Targets US-based people-search sites; some sources note early UK expansion. Confirm current coverage on Kanary's own site.                    |

### BEFORE YOU HAND OVER YOUR DETAILS

These services need you to give another company your sensitive identifying information — full legal name, addresses, sometimes ID — so it can act on your behalf. Read what each one does with that data first, and treat a "free scan" result as a sales funnel, not a neutral audit.

# 03 Passwords that actually pass

## The order that protects you, 2026

- 1 Passkey, wherever the service offers one.
- 2 No passkey? A unique password generated and stored by a password manager.
- 3 Phishing-resistant MFA or a physical security key, where offered.
- 4 An authenticator app (TOTP codes), if no security key option exists.
- 5 SMS codes — only as a last resort. Better than nothing, easiest of these to intercept.

## Why length beats cleverness

US NIST, the standards body most password guidance leans on, has shifted its advice: password managers and phishing-resistant authentication now matter more than symbol rules. A single-factor password should be at least 15 characters. A genuinely random four-word passphrase beats a clever eight-character substitution — length is what actually slows a brute-force attack, and a password manager means you never have to remember either.

### PERSONAL PASSWORD SYSTEM DEEMED TOO WEAK

The "make your own system" advice and the BuyMyGoatGumboots2025! example are gone. Predictable transformations and reused patterns are exactly what current guidance says to avoid — they feel clever but crack fast.

## Password managers for Kiwis, 2026

| Service                 | Price              | Free? | Standout                          | Best for                        |
|-------------------------|--------------------|-------|-----------------------------------|---------------------------------|
| Bitwarden               | Free–US\$19.80/yr  | Yes   | Open source, audited              | Budget-conscious, privacy-first |
| 1Password               | ~US\$36–45/yr      | No    | Family plans, Travel Mode         | Families, Apple users           |
| Dashlane                | From ~US\$50/yr    | No    | Built-in VPN, dark web monitoring | All-in-one bundle               |
| Apple Passwords         | Free with Apple ID | Yes   | Native app, cross-device autofill | Apple ecosystem                 |
| Google Password Manager | Free               | Yes   | Built into Chrome/Android         | Basic users, Google ecosystem   |

Note: Apple now presents this as its own Passwords app rather than folding it entirely into Settings — the underlying iCloud Keychain sync is the same.

## 04 It's break-up time

### Should you ditch "Sign in with Google/Apple"?

Not necessarily. "Switch back to email and password because it's more secure" isn't generally true. Signing in with Google or Apple avoids creating another reusable password, and it usually grants the app a defined, visible set of permissions rather than blanket access.

The better move isn't abandoning it wholesale — it's auditing it:

- ◆ Review exactly what permissions each connected app has requested.
- ◆ Remove anything old, unused, or unrecognised.
- ◆ Protect the identity-provider account itself with a passkey or strong MFA — it's now the single key to everything connected to it.
- ◆ Remember: revoking access stops future data flow, it doesn't delete what the other service already copied. Contact that service directly for that.

#### UPDATED GOOGLE STEPS

Google's current path is **Google Account** → **Security** → **"Third-party apps with account access"** (also shown as "Your connections to third-party apps & services"), rather than a separate "Manage third-party access" page. Direct link: [myaccount.google.com/connections](https://myaccount.google.com/connections)

#### IF YOU USE SIGN IN WITH APPLE

On iPhone or iPad: **Settings** → **[your name]** → **Sign-In & Security** → **Apps Using Apple Account**. On Mac: **System Settings** → **[your name]** → **Sign-In & Security**. Or go straight to [account.apple.com](https://account.apple.com) → **Sign-In & Security** → **Sign in with Apple** from any browser.

## 05 Phone & browser settings

### Android

The old "Opt out of Ads Personalisation" path is being phased out on newer versions. Current path: **Settings** → **Privacy** → **Ads** → **Delete advertising ID** — this removes the identifier itself rather than just opting out of its use. Also check your Privacy Dashboard and My Ad Center for what's actually been inferred about you.

### iPhone

- ◆ **App Privacy Report** (Settings → Privacy & Security → App Privacy Report) shows exactly what each app has accessed, and when.
- ◆ **Safety Check** (Settings → Privacy & Security → Safety Check) quickly cuts off everyone and everything with access to your device and accounts.

#### IF YOU'RE USING SAFETY CHECK BECAUSE OF A PARTNER OR EX

Safety Check is genuinely useful here, but changing settings on a shared device can tip that person off before you're ready. Have a quick safety plan first — a backup device, a trusted contact, a sense of timing. Netsafe and NZ Police both have guidance for this exact situation.

### Browser: uBlock Origin

Full uBlock Origin no longer works properly on Chrome — Google's Manifest V3 changes removed the capability it relies on. If ad and tracker blocking is a priority, install full uBlock Origin on **Firefox**. Staying on Chrome or Edge, install **uBlock Origin Lite** instead — real, but reduced filtering power. Get either from the developer's own site or your browser's official extension store, not a generic promotional domain.

## 06 Your rights as a Kiwi

Here's what New Zealanders can actually ask for, and what changed in 2026.

### What you can ask for under the Privacy Act

- ◆ Ask any organisation what personal information they hold about you. They generally have 20 working days to respond.
- ◆ Ask them to correct it — including asking them to delete it — though NZ doesn't have a broad GDPR-style "right to be forgotten." These are requests you can make, not guarantees you'll get.
- ◆ If they refuse to correct something, ask them to attach a statement of correction so your version sits alongside theirs.
- ◆ Not getting anywhere? Contact the organisation's privacy officer, then escalate to the Office of the Privacy Commissioner.

| *"The latest developments to protect Kiwis' rights online:"*

### IPP 3A — in force from 1 May 2026

Organisations generally now have to tell you when they've collected personal information about you from someone other than you — a data broker, another company, a public register — unless a specific exception applies.

### The Biometric Processing Privacy Code

Covers face, voice, fingerprint and other biometric data. In force for new systems since November 2025; organisations already using biometrics before then have until **3 August 2026** to comply.

### A few more worth knowing

- ◆ Marketing emails and texts: businesses must generally act on your unsubscribe request within five working days.
- ◆ Stalking and harassment: from 26 May 2026, NZ has a stand-alone stalking offence covering digital tracking, spyware and doxxing, not just physical following.
- ◆ Doxxing, intimate-image abuse and AI-generated deepfakes: Netsafe has dedicated guidance on doxxing and image-based abuse, including deepfakes. NZ Police's Harmful Digital Communications guidance covers the criminal side. Screenshot first, with the date and URL visible, then reach out.

## 07 Getting content off Google

You have more say over what shows up about you on Google than most people realise, it just depends which lever you pull. Here are the three that actually exist:

- 1 **Remove it at the source.** Contact whoever runs the site or platform and ask them to take it down. The only option that removes the content itself.
- 2 **Remove it from Google Search.** Google can delist certain categories of personal information (phone number, home address, ID numbers) from search results — the original page is still live if someone goes there directly.
- 3 **Refresh outdated content.** For pages already updated or taken down at the source, where an old cached version is still showing. Only use once the live page has actually changed or gone.

## 08 Take back my data checklist

The main moves from this guide, in one place. Work through them at your own pace — even three or four of these puts you ahead of most people online.

- ☐ Turn off model training in ChatGPT and Claude, and use Temporary Chat or Incognito for anything sensitive.
- ☐ Run a free scan with Optery to see what data brokers already hold on you.
- ☐ Get a password manager and switch on passkeys wherever a service offers one.
- ☐ Audit your "Sign in with Google/Apple" connections and remove anything old or unrecognised.
- ☐ Turn off ad tracking on your phone — delete your Android advertising ID or check Apple's App Privacy Report.
- ☐ Install uBlock Origin (Firefox) or uBlock Origin Lite (Chrome/Edge) to cut down tracking as you browse.
- ☐ Know your Privacy Act rights — you can request, correct, or complain about how an organisation uses your data.
- ☐ If something's already online, contact the source directly or use Google's removal tools to limit its reach.



## Ngā mihi nui

This guide is a project of Big Picture Thinking — narrative strategy and systems change for Aotearoa. Better narratives, bigger change, more impact.

**[bigpicturethinking.nz](https://bigpicturethinking.nz)**

Take Back Your Data — checked July 2026