RESIST KIT

GUIDE

TRAVEL PRIVACY TIPS:

HOW TO REDUCE DIGITAL & BIOMETRIC EXPOSURE WHEN YOU TRAVEL

Modern travel involves layers of digital tracking. From biometric border checks to airline apps, hotel systems, airport Wi-Fi, SIM cards, financial transactions, and behavioural data. You cannot avoid all of it, but you can massively reduce what you hand over.
This guide provides clear steps to protect your privacy while still travelling normally.

Travel Privacy – The Spice Guide

We've grouped practical steps into three "spice levels" so you can choose what suits your comfort, values, and travel style. **You're in control. Pick your privacy spice level.**

🌶 Bare minimum - Low effort · High impact · Everyday traveller

🌶🌶 You're getting serious - More intentional · Fewer data trails · Still practical

🌶🌶🌶 Defcon 5! - Maximum privacy · Minimal digital footprint · Advanced

In Summary: The Big Six for Travel Privacy

If you do nothing else:

1. Avoid SmartGates - line up, choose manual passport checks.
2. Withdraw cash early and use cash wherever possible.
3. Avoid airport and hotel Wi-Fi for sensitive tasks.
4. Minimise apps - use paper boarding passes.
5. Limit SIM registration - use roaming or travel eSIMs.
6. Turn off Bluetooth, Wi-Fi and location when not required.

1. Before You Travel

A. Minimise your digital footprint 🌶

- Delete unused apps, especially those with location or microphone access.
- Turn off "ad personalisation," "analytics," and "app tracking" in your phone settings.
- Remove saved boarding passes from airline apps once you land.
- Disable cloud syncing for sensitive photos and ID documents.

B. Prepare a "travel phone" (optional but ideal) 🌶🌶🌶

Some frequent travellers use a simple smartphone with:

- no social media
- no banking apps
- minimal permissions

It dramatically reduces exposure.

C. Check your passport photo & biometric use 🌶🌶

- A biometric photo is mandatory for an Australian passport.
- You can reduce additional biometrics by choosing manual border processing (see section 2).
- Review DFAT's privacy policy before you travel.

D. Download maps & key documents offline 🌶🌶🌶

Some frequent travellers use a simple smartphone with:

- Offline maps
- Hotel booking confirmations
- Airline Vouchers
- Attraction tickets

This avoids unnecessary log-ins and network tracking

2. At the Airport or Border Control

A. Skip SmartGates if you want to avoid extra biometrics 🌶🌶

SmartGates perform:

- a live facial recognition scan
- a biometric match
- a linked travel-history verification record
- SmartGate activity tracking

To avoid this:

- Use the manual passport line
- Tell staff you prefer a manual check

CCTV remains, but no biometric matching occurs.

Get more resources & kit here: www.MyResistKit.com

ALIGNED COUNCIL OF AUSTRALIA

RCR .media

TRAVEL PRIVACY TIPS
Continued

GUIDE

You may politely refuse SmartGates
Simply say:
"I prefer a manual passport check, thank you."

B. Avoid airport Wi-Fi 🌶️
Airport Wi-Fi often captures:
- device identifiers
- browsing activity
- behavioural analytics

If you must use it:
- connect via a VPN
- avoid sensitive activities (email, banking, government log-ins)

C. Boarding passes: use paper where possible 🌶️
Airline apps track:
- device information
- location
- user behaviour

A paper pass avoids these digital analytics.

D. CCTV is still present
Airport and border CCTV record the environment but it is generally not matched to your passport unless a security reason exists.

3. During Flights

A. Avoid airline apps 🌶️🌶️
They often log:
- what you click
- which movies you watch
- device IDs
- seat number

B. Turn off Bluetooth & Wi-Fi when not needed 🌶️
Planes use:
- Bluetooth beacons
- Wi-Fi analytics
- device scanning

Minimise this by switching them off.

4. At Your Destination

A. Hotels: provide the minimum required 🌶️
Hotels increasingly:
- scan passports
- store ID in cloud systems
- use lobby CCTV with analytics
- track Wi-Fi usage

Privacy tips:
- Decline copies of documents where possible
- Request a manual check-in instead of app-based check-in
- Avoid hotel Wi-Fi for sensitive tasks
- Use cash for deposits if the hotel allows

B. Taxis & rideshare 🌶️
Rideshare apps collect:
- live location
- travel patterns
- payment identifiers
- behavioural data

Reduce exposure by:
- using taxis and pay cash where possible
- turning off location permissions after each rideshare trip

5. SIM Cards & Telecommunications

A. SIM cards 🌶️🌶️
Many countries require SIM registration with:
- passport details
- full name
- sometimes a photo

To reduce this:
- use roaming on your existing SIM/eSIM
- choose airport kiosks that require fewer details
- disable unused network services

B. Turn off location services 🌶️🌶️
Unless required:
- disable GPS
- disable "high accuracy" modes
- turn off Bluetooth scanning
- turn off "nearby devices"

These are major data collectors.

6. Money & Payments

A. Withdraw local currency soon after arrival 🌶️
- ATMs allow you to convert a single digital transaction into days or weeks of private, untracked spending.
- Withdraw larger amounts less often to reduce the number of logged transactions.
- Use reputable bank ATMs rather than hotel or convenience-store ATMs (which often harvest extra metadata).

TRAVEL PRIVACY TIPS
Continued

GUIDE

B. Use cash wherever possible 🌶️
Cash prevents:
- movement profiling
- commercial tracking
- location logs created through card transactions
- backend data-sharing between banks, apps, and merchants

C. If you can't use cash 🌶️🌶️
Choose privacy-friendlier options:
- prepaid travel cards
- debit cards not linked to your main accounts
- digital wallets that reduce merchant visibility

7. Public Transport 🌶️🌶️

Systems can track:
- tap-on/tap-off times
- journey routes
- device signals

To minimise:
- use paper tickets where available
- turn off Wi-Fi and Bluetooth
- avoid linking travel cards to your name

8. Apps, Maps & Messaging 🌶️🌶️

A. Maps
Use:
- offline maps
- no location history
- apps with minimal data-sharing

B. Messaging
Better for privacy:
- Signal
- Telegram

More heavily logged:
- WhatsApp
- Messenger
- SMS

C. Social media
Avoid posting in real time — it reveals:
- precise location
- travel patterns
- hotel details
- time stamps

Post after leaving a place.

9. Returning Home 🌶️🌶️

A. Clean your device
- uninstall hotel and airline apps
- remove foreign SIM/eSIM profiles
- clear browser data
- delete temporary QR apps
- reset advertising IDs

B. Review your privacy settings
Some apps silently reactivate tracking permissions.