earthfood Freedom with nitrifying living soil microbes

EXIT THE DIGITAL ID MATRIX: A HUMAN SURVIVAL GUIDE

For Earthfood Community & All People Who Refuse the Collar of Control

This is the booklet they hope you never find.

Because once you see how the system is built and who it serves you can never unsee it.

This is not a conspiracy. Its reality millions are waking up to. And it's time to reclaim your place in a future worth living for.

Why This Booklet Matters

On December 25th, 2025, a new frontier of surveillance begins.

This isn't just about digital convenience. It's about control. A sweeping rollout of biometric identification systems, AI-based verification, and centralised data tracking will soon become mandatory across many digital and physical services in Australia and beyond.

They say it is for your security. But we say it is a system that hands your sovereignty, your autonomy, and even your identity to algorithms controlled by corporate-government alliances.

The Earthfood Community exists not just to heal the soil, but to protect humanity. This guide is the beginning of a multi-stage strategy to unplug from invasive systems, transition into ethical digital and community-based alternatives, and reclaim our lives under God-given rights.

A Note on Integrity and Fair Exchange

If you've been gifted or passed a copy of this booklet and are not a member of the Earthfood Community, we ask that you honour the spirit in which this was created.

This booklet represents countless hours of deep research, spiritual reflection, and hard-earned insight. It was written not by a corporation, but by a small family-run Australian business with a mission to future-proof our nation, protect our rights, and restore the balance between people and the natural world.

We ask for a humble contribution of **$18.88 AUD**, not as a fee, but as a fair exchange. By supporting this work, you're helping us continue to offer truthful, grounded resources to those who need it most. If you don't, you're not just ripping us off, you're quietly reinforcing the very system this booklet warns against.

Support the mission, be fair.

SECTION 1: UNDERSTANDING THE SYSTEM YOU'RE TRAPPED IN

Digital ID is not just a username and password. It is:

- Your facial scan
- Your fingerprint

- Your keystroke habits
- Your eye movement patterns
- Your health data
- Your vaccine status
- Your spending behaviour
- Your location history
- Your browser activity
- **Your whole living experience - your movements, purchases, emotions, and even your silence - is being harvested for verification, tracing, and what the system calls "predictive behaviour".**

This is not some distant possibility. It is now embedded in global AI contracts and biometric

systems designed to anticipate what you will think, do, or say, then categorise you accordingly. These are tools of control, not convenience. The goal is not your safety, but your predictability.

  - *"They devise evil plans in their hearts; they continually gather together for war. They sharpen their tongues like swords and aim cruel words like deadly arrows."* Psalm 64:6–7

- Through force, fines, censorship, and social scoring, you will be nudged into obedience or digitally exiled. This is the beast system creeping in—not with fangs, but with QR codes and consent forms.

  - *"And that no man might buy or sell, save he that had the mark..."*
    Revelation 13:17

These identifiers are assigned to you, tracked in real-time, and managed by third-party servers that you do not control.

AUSTRAC, MyGovID / MYID, [Centrelink, Medicare, ATO, Superannuation companies], banks, tolls, supermarkets, and even phone access will soon be locked behind these systems.

If not compliant, you may be excluded—digitally blacklisted, denied access to services, flagged for review, or nudged via algorithmic coercion.

These tools are already embedded in global banking (via AUSTRAC, the World Bank's Digital ID4D program), Big Tech (Meta, Google, Microsoft), and AI-backed surveillance firms like *Palantir, Thales Group,* and *Accenture*.

See: World Economic Forum's "Framework for Digital ID" (2023), Australian Financial Review coverage on AUSTRAC's biometric mandates (2024), and the Palantir-NHS predictive health contract in the UK (2022). https://www.weforum.org/publications/reimagining-digital-id/

And this: as quoted from the Australian Government Digital Id System PDF*: "All Australians will have the opportunity to provide input on how a voluntary, inclusive Digital ID system can protect their personal information. Digital ID is one of the ways the Government is responding to the increase in third party data breaches, alongside the National Strategy on Identity Resilience, funding for the ACCC's National Anti-scam Centre, the introduction of the Identity Verification Services Bill, continued reforms to the Privacy Act and the Government's Cyber Security Strategy 2023-2030".*

https://www.digitalidsystem.gov.au/sites/default/files/2023-09/australiadigitalidsystem_roadmap_18092023.pdf

Digital ID Act 2024 – Section 74 Creating and using a digital ID is voluntary

In China, this is overt social credit scoring.

In Australia, it's emerging as **myID**, **eSafety Commissioner mandates**, and **banking restrictions tied to behavioural data**. Globally, the United Nations' **2030 Agenda** promotes interoperable digital ID linked to financial inclusion and "sustainability goals"- a soft form of control with hard consequences.

The goal is not your safety, but your predictability. You become a dataset, and your worth is measured by compliance. You will be told you have no choice. But you do. Systems are illusions. Man -made structures that only work if you believe in their power. There are parallel systems you can choose.

The System Illusion – How to Navigate Without Getting Caught

If you've ever felt like something was off, like you're playing in a game where the rules shift without notice: you're right!

What we call *"the system"* is actually a tightly woven **network of different systems**, some visible, others entirely hidden, each with their own laws, permissions, and methods of enforcement.

You've been trained to think there's only one lawful path: birth certificate, school, tax file number, job, superannuation, mortgage, aged care, grave. But **this isn't nature's law. It's a manufactured flow chart**.

It's time to understand how these systems work — and how to exit them.

System Layers You May Be Caught In

- **Fiat Currency System**: You earn AUD, pay tax, get taxed again on savings, then are locked out if the bank suspects "suspicious activity."
- **Digital ID System**: Linked health records, banking access, facial recognition, voice imprinting, Medicare tracking: all under the illusion of convenience.
- **Biometric Surveillance System**: You're scanned at airports, cameras log your gait, and phone towers track your precise movements.
- **Corporate Credit Grid**: All your purchases, subscriptions, payment habits, and online behaviour are used to model your future actions.
- **Superannuation Scheme**: You pay into it your whole life but can't touch it unless you're dying or old. Meanwhile, corporations build housing and profits from it, then rent it back to you.
- **Predictive Behaviour Model**: Your digital exhaust — every search, voice query, transaction, loyalty card swipe — is used to train AI models that don't just guess what you'll buy...
  They aim to control what you'll do, say, and eventually believe.
  When you resist?
  You're managed through restrictions, fees, financial pressure, cancelled services, or "compliance" threats.

Real-World Footnote: How Deep Does It Go?

- **Mastercard's AI division works with behavioural surveillance models** to detect "risk factors". Not for crime, but for consumer deviation.
- **AUSTRAC monitors every transaction over $10,000 and every international transfer over $1,000**. Regardless of legality.
- **Woolworths' Everyday Rewards** collects data on your eating, drinking, and pharmacy habits, then sells it to health insurers and third parties.

- **The ATO cross-checks your social media with reported income**. They don't even need a warrant.
- **Digital licenses (now in rollout)** will allow real-time revocation of driver's access, tied to insurance, fines, or medical compliance.

The "System of Systems" and Where You Get Caught

What most people don't realise is: these systems don't naturally interact with each other. They only touch **because you link them.**

For example:

- You can operate in **blockchain** without banks unless you cash out to fiat without privacy protocols.
- You can **homeschool your children privately** unless you register with the state for "compliance" and funding.
- You can barter, grow food, trade seeds, and run a **Private Association** unless you voluntarily register as a public-facing entity, in which case you must comply with every government mandate.
- You can store money offshore legally but if you move it to an Australian bank without a "compliant" story, **AUSTRAC freezes it instantly**.
- You can **own land** but if it's mortgaged, zoned, or under council title, **you're leasing it from the system**, not stewarding it as sovereign.

Everyday Scenario: The Superannuation Trap

You're a small business. You've worked yourself sick to keep it afloat. You've been forced to contribute thousands into super for staff.

You:

- Can't access it yourself.
- Can't use it to build your own housing.
- Can't apply for a release without a death certificate or financial collapse.

Meanwhile:

- Large corporations use pooled super funds to build housing developments.
- Those are bought and sold amongst other corporate entities.
- You pay rent on homes funded by your own money.
- And you're told to be grateful your super is "investing in growth."

It Gets Worse: Predictive Human Modelling

The most dangerous system is the **predictive behavioural grid**.
This is where your:

- Purchases
- App usage
- Smart device interactions
- Travel patterns
- Voice samples
- Face scans
- DNA test kits
- Medical records
- Social media posts
- Keyboard cadence and spelling patterns

… are **fed into predictive AI models that map what you'll do, say, believe and how to manipulate you**.

This isn't future fiction. It's active now.

Once you're profiled, your experience online and offline is **tuned to that profile**. You get different prices, different news, different medical options, different banking access all under the illusion of "personalisation."

Some Systems You Can Choose to Exit

- **Corporate supermarkets** → Start your own food club or trade through a private community – Your Earthfood Community. Yourearthfood.com

- **AUSTRAC-banked wallets** → Move to Monero, cold wallets, or cash communities.
- **Digital licenses** → Use your right to travel freely under natural law.
- **Behavioural tracking apps** → Delete them. Use de-Googled phones. Use open-source software. (refer to back section for phone scramming)
- **ID-linked marketplace platforms** → Trade on Gumtree, Locanto, or within private bartering communities.
- **Mainstream media** → Build your own knowledge base. Follow sources that don't serve corporate/government narratives.

This section is in more details with HOW-TO's in Booklet 2: EXIT THE AU MATRIX

Released October 18th in our private community – to JOIN OUR COMMUNITY go to yourearthfood.com

What the Research / Public Records Tell Us

What's true and already happening:

1. **Higher Taxes on Large Super Balances**
   From 1 July 2025 the Australian government announced that superannuation earnings on balances over $3 million will be taxed at 30%, double the previous rate for high balances. Morningstar
2. **Warning Scenario: What Might Happen**

   If current trends accelerate, by 2030 we could see superannuation transformed into something very different.

   Imagine a system where:

   - Large balances are heavily taxed or stripped of concessions.
   - Access to your super could depend on digital identity or biometric verification.
   - Programmable constraints force your super to be used only for approved expenses or certain approved providers, in other words please explain on what you are using the funds.

- Failure to comply with identity, behaviour, or health mandates results in restricted access or even freezing of your super.
- These aren't wild guesses, they're already part of government debate, fintech proposals, and global finance frameworks.
- If we accept current regulation creep without resistance, one day super might still exist but heavily conditional, surveilled, and controlled. In other words, no rights and could be excluded from accessing the money in time.

- There is a growing push to reshape superannuation (note: Australia for sure, but other commonwealth countries I didn't research). Already, balances over $3 million will be taxed at 30% from mid-2025. Discussions are ongoing about limiting tax concessions, increasing oversight, and linking super access with identity verification and compliance with system rules.
- Think about what *could* happen by 2030: what if your super funds become programmable? What if you must verify your digital identity, your behaviour, or your health status to access them?
- It's possible that super won't disappear, but it may become a digital collar, with rules, conditions, and restrictions built in. We must treat this not as speculation, but as a rising risk.

3. **Capping Tax Concessions / Limits on Super**
   There are proposals (like those from the Greens) and discussions around limiting tax concessions for high super balances beyond certain caps. This shows intent to reduce benefits for the wealthiest in the system. pbo.gov.au

4. **Digital / Data Innovation in Superannuation**
   Super funds are increasingly adopting AI, data analytics, and digital tools which could allow more oversight, control, and linkage of super balances with identity systems. JPMorgan Chase

5. **Programmable Money Discussions**
   There are global and local conversations about money that operates with "code" or conditions (e.g. spending limits, perhaps even restrictions) through digital currencies, fintech, or government-controlled ledger systems. Federal Reserve+2Netbul+2

What is speculative / unconfirmed:

- No government has publicly declared that superannuation will be eliminated by 2030. However, current legislative shifts and digital infrastructure reforms strongly suggest that the system is being reshaped from a retirement buffer into a controlled, programmable asset pool. Historically, we've seen such shifts before.

- After WWII, Australia's Labor government rolled parts of the national retirement scheme into consolidated revenue, reabsorbing what workers believed was theirs.
- In 1933, the U.S. government ordered all citizens to hand over privately held gold under Executive Order 6102 criminalising noncompliance and centralising wealth "for the greater good."
- Superannuation, today, remains a tempting honeypot. With over $3.5 trillion AUD in managed funds, it sits ripe for future repurposing especially under regimes driven by carbon targets, programmable central bank digital currencies (CBDCs), and sustainability scoring. It is no stretch to imagine future limitations placed on what retirees *can* access based on compliance metrics, health status, or spending behaviour.
- The real question is not whether they've announced the end of superannuation it's whether you're watching closely enough to see the chessboard being set.
- No law yet mandates super be replaced by a programmable or entirely digital system that you can't access.

- "Programmable money" is being explored, but its real-world implementations are still in early phases and have significant resistance. This gives us time and a warning to get cracking – we show you this in *"EXIT THE AU MATRIX"*

What the research now tells us about the Vietnamese government's handling of its currency, the dong (VND), adds a vivid warning. The State Bank of Vietnam has allowed the dong to depreciate gradually, nearly 5% in some periods, amid growing pressure from rising US dollar strength, global inflation, and domestic economic headwinds.VnEconomy+2The Shiv+2

While a weaker dong may help Vietnam's export industries by making its goods more competitive abroad, it also drives up prices for essential imports, squeezes household savings, and increases dependency on foreign currency.vietnamnews.vn+1

For those holding dong (or similar currencies), this means you are exposed in two ways:

1. your saving value erodes as your currency loses strength.
2. your ability to convert, spend, or use those funds is vulnerable, especially when moving from one system to another (e.g. from foreign currency into ID-tied or surveillance-tied banking systems).
3. In short: what is nominally a currency holding can become a liability in a regime that demands verification, biometrics, proof of identity, digital identity links for banking or access.
4. It shows how even money you think you own can be immobilised if you are forced into systems that see your identity as the gateway to financial freedom.

"The borrower is servant to the lender." Proverbs 22:7

> This verse cuts to the heart of debt, control, and ownership perfect for highlighting the reality that governments or systems that "manage" our wealth also own the levers that limit our freedom.
>
> If we allow others to manage our future those with zero care factor for our wellbeing, yet total obsession with shareholder profits and CEO bonuses often funnelled offshore into corporate cartels—then we must wake up to the rot. It is not just bad policy. It is theft dressed in a suit.

And the longer we tolerate it, the more we become complicit in the erosion of our own freedom.

"Woe to those who make unjust laws, to those who issue oppressive decrees, to deprive the poor of their rights..." *Isaiah 10:1–2*

A Message from Bronwyn Holm

Founder of Earthfood, Farmers' Voice, Growers Guidance and Minister of Agriculture & Soil, Great Southern Accord; under Royal Tribal Administration, Owner of the Earthfood Project.

Why am I putting this out?

Because I'm an Australian by 6 generations and as a Southeast Queenslander. And being an Aussie once meant something.

It meant **standing up when you're told to sit down**.
It meant **fair go for all**, not surveillance, not silence, not submission.
It meant we stood shoulder to shoulder—from the **Eureka Stockade** to the **trenches of Tobruk**, from the **Wool Classers' sheds** to the **bushfire frontline**—we weren't afraid to say:
"No. Not on our land. Not to our people."

But now, we're being digitised. Codified. Barcoded like cattle.

I'm putting this out because I believe in our country—**not the version run by overseas banks, bureaucrats, and unelected committees**, but the one that still breathes beneath the surface and catching on to the ground swell behind closed doors of suburbia.

My voice has always said FEAR NOT and true to my word.
The one where **mateship means everything**,
where you can still trust a handshake,
where **your name is your bond**,
and **the land still means home**.

This booklet isn't just about exiting the Digital ID system.
It's about **reclaiming who we are before it's too late**.

It's about your kids and grandkids not needing to scan their face to buy bread. It's about pulling your money, your food, your health, and your identity out of their system and planting it firmly back in yours.

Because I'm not just writing this for me. I'm writing it for the cane cutters who swung machetes through North Queensland heat, the opal miners in Lightning Ridge who dug with their bare hands, and the old fellas who still keep bees out the back of Bourke because they trust the land more than they trust the labels.

For the single mums in Bendigo growing veggies in bathtubs, and the families out west who've taught their kids to butcher, bake, and build because no one's coming to save them.

For the drought-hardened graziers who've buried more stock than they've sold, and the fishermen who still read the tide by the moon, not by an app.

For the cattlemen in Cape York who never asked permission, and the CWA women holding the line with seed libraries, wood stoves, and quiet courage.

For the Eureka rebels who bled for the right to choose their future, and the Anzacs who never checked in with a QR code into battle. For the retired diggers who still salute the flag even when no one's watching.

For the shearers who walked off the job in 1891 and said, "We deserve better." For the everyday Aussies who are waking up and realising… "If we don't draw a line in the red dirt now we'll be programmed out of existence."

So here it is. The line. Join me. Join Our Community.

We are the people.

We are the Mud Army.

We are Bushfire Brigade.

We are the custodians of our seed, our soil, our future.

We don't need a barcode to prove we exist.

We never outsourced our common sense.

We stand on land that remembers who we are.

We are not property. We are not programs.

We are not waiting for permission. We are it. And we are girt by sea - so no one is coming.

Let's grow food that nourishes, not poisons.

Let's build systems that free us, not trap us.

Let's honour the spirit of Eureka and light that Southern Cross once more.

Join me. Stand up. Get out of their matrix.

We are it. Here's how we do it: step by step.

SECTION 2: VOLUNTARY BUT MANDATORY - HOW THEY MAKE YOU COMPLY (For Beginners)

You've heard it all before:

"It's completely voluntary… but you can't go to work, access services, or travel without it."

Sound familiar?

It's the same playbook Australia used during the COVID-19 injection rollout. The government claimed the medical procedure was optional. But in practice, it was enforced through economic coercion:

- No jab? No job.
- No jab? No home loan.
- No jab? No travel, no freedom, no access.

This wasn't done by direct government legislation. Instead, private corporations were deputised to enforce it. Businesses, banks, employers, and even hospitals carried out the mandates — many of them with no legal standing under threat of withdrawal of funding, insurance issues, or regulatory pressure.

The Illusion of Choice

The Australian government repeatedly shielded itself by saying these decisions were made "independently" by corporations. But those corporations had little choice — and the people even less.

The genius (and the horror) of this tactic lies in legal immunity. When the mandates went wrong when people were injured, fired, or segregated the government avoided liability, claiming it never "forced" anything.

Instead, mandates were implemented via policy, not law, making it nearly impossible to litigate against those truly responsible.

Now the Tide Turns: Mandates on Trial

In 2024, a quiet shift began. The very corporations that enforced the mandates are now being exposed. Legal actions are underway globally, and Australian law firms are cautiously exploring coercion liability. Some workers' compensation claims have been successful. In the US and UK, courts are now hearing major cases on wrongful termination and health injury linked to mandated medical products.

Australia's government has already introduced new legislation to further shield itself and agencies. But cracks are forming and the legal dam is leaking.

The Next Round: Digital ID as a "Voluntary Mandate"

This same coercive strategy is being repackaged for the new frontier: Digital ID.

They say:

- "You don't have to get the Digital ID…"
  But:
- You won't be able to access Medicare rebates without it.
- You'll be denied entry to government portals.
- Centrelink, MyGov, and even tax returns will "require verification."
- Your online banking will begin to phase it in "for your protection."

And guess who will enforce it?
Not the government but your bank, your employer, your accountant, your local council. Just like before.

This is not a conspiracy theory. This is the same mechanism used repeatedly, masked as convenience and "security."

Say no. Do not hand over your:

- Fingerprint
- Facial scan
- Voice scan
- Real-time location tracking
- Biometric passport or driver's licence scan

Why? Because the Act of Legislation Digital ID is Voluntary for individuals and Directors of Companies. (some may be surprised!) Refer: Section 74 or the Act.

In the near future there is a price for giving up this information in it permanently ties you to a global database that feeds AI systems capable of real-time social control. Once it's in, you can't take it back.

Australia has already trialled biometric entry at airports. Woolworths tested facial recognition. Banks are pushing biometric logins. The deadline is here.

THIS IS PREDICTIVE CONTROL - NOT SECURITY

This isn't about protecting your identity. It's about **predicting your behaviour** and shaping your decisions.

Governments and corporations already deploy:

- **Predictive policing** (as seen in Victoria and NSW since 2019)
- **Behavioural nudging** (used during COVID-19, via the Behavioural Economics Unit)
- **Credit scoring models based on social data**
- **Pre-emptive censorship algorithms**

Once your data is centralised, through Digital ID, the next step is **programmable consequences**:

- Fines deducted automatically.
- Travel blocked for "non-compliance."
- Purchases denied at checkout based on profile flags.
- Health treatments restricted to "approved" patients only.

IT'S LEGAL, BUT IT'S NOT LAWFUL

- These programs are rolled out **via policy, not law.** You will not find a single Act of Parliament that says:
- "Australians must submit biometric data to access the internet, healthcare, or banking."
- Instead, you'll find *partnerships*, *regulatory frameworks*, *pilot programs*, and *private-sector enforcement*.
- These are testbeds - voluntary at first, **coerced by design** later.

- It starts as a convenience.

  It becomes an expectation.

  It ends as a requirement

SECTION 3: PLATFORMS, TOOLS, AND STRATEGIES FOR LIVING DIGITALLY INDEPENDENT

1. Communications

- Encrypted messaging apps that don't require ID
- Decentralised social networks
- Local mesh networks and walkie-talkie apps for emergencies

2. Financial Freedom

- Offshore fintech accounts (non-AUSTRAC aligned)
- Cold wallet crypto storage (Bitcoin, Monero, etc.)
- Gift economy systems and parallel bartering channels

3. Privacy Browsing + Devices

- Alternative browsers and privacy search engines
- Burner phones / de-Googled phones
- Linux-based operating systems
- Tracking blockers and browser hardening tools

4. Identity & Authentication

- Avoiding biometric submission
- Anonymous email + phone number tools
- Paper-based and wet-signature ID templates
- Facial recognition blockers (IR glasses, spoof masks)

5. Hosting & Cloud Storage

- Decentralised data storage options
- Encrypted file lockers

- Web hosts outside 5 Eyes jurisdiction

6. Marketplace & Online Trade

- Local buy/sell networks with no ID requirement
- Open-source community exchange platforms
- Food, goods, and service sharing apps that avoid data scraping

7. Knowledge & Community

- Forums and channels to stay updated (without censorship)
- Alternative news aggregators
- Earthfood Community et al and parallel community infrastructure

8. Exiting Surveillance Infrastructure

- How to leave MyGov, Medicare, and linked-ID services
- Reclaiming seed, land, and water rights from digital mapping tools
- Creating a parallel record of your existence: private ledgers, affidavits

9. Education for the Next Generation

- Offline, open-source homeschooling and digital detox programs
- Earthfood-aligned nature and soil literacy curricula (Now available for RTO standards within High Schools education assessments if required).
- Teaching children how systems work – not just how to follow them

10. Spiritual and Legal Autonomy

- Natural law foundations and Bible-affirmed living with no judgements
- How to reject digital jurisdiction without declaring yourself a 'SovCit'
- Setting up lawful private contracts, declarations, and private structures

Messaging:

- Signal: End-to-end encrypted
- Session: Australian, decentralised, anonymous
- Element (Matrix): Encrypted, open-source

Social Media:

- Mastodon: Decentralised Twitter alternative

- Friendica: Facebook-style networking without surveillance
- Pixelfed: Instagram-style, privacy-based

Video/Streaming:

- PeerTube: YouTube alternative, no ads
- Odysee: Blockchain-based
- BitChute: Censorship-resistant

Web Browsing:

- Brave: Blocks trackers, fast and safe
- Tor Browser: Complete anonymity online

3.1 COMMUNICATIONS

Secure your voice, your data, and your digital presence

In a world where predictive behaviour and digital surveillance shape not only what you *see* online but also what you *say*, it's vital to start here: **communication is no longer private unless you make it so.**

Your Digital Trail: Who's Watching?

A vital starting point for any digital sovereignty journey is awareness. One of the simplest yet most powerful tools is:

HaveIBeenPwned.com

This free online tool checks if your email or phone number has been part of a **data breach**, a cyberattack in which usernames, passwords, and other private info are leaked.

This website emerged after one of the largest breaches in history (Adobe), where millions of customer records were exposed. It now tracks over 12 billion breached accounts globally.

Why it matters:

- Hackers reuse breached logins across multiple platforms.
- Many people still use the same password across platforms, multiplying the risk.
- Your personal identity may already be circulating on dark web marketplaces.

Step 1: Check your email(s) and change passwords immediately if you're compromised.
Use unique passwords and a secure password manager going forward.

Messaging Without Eyes on You

Mainstream apps like **WhatsApp**, **Messenger**, and **Telegram** are increasingly integrated with phone numbers, device metadata, and even **facial recognition or government IDs** in some countries. While some claim to be "encrypted," their metadata is still trackable.

Instead, switch to:

1. Signal (https://signal.group/#CjQKIErgsMOIQBx6jR6W39eK_oPZAOCTsMHvsgfdCsPTE53YEhBz6aUgQN1JcPGE4-RAmaAO find us @YourEarthfood)

- End-to-end encrypted
- Open-source, funded by donations
- Minimal metadata retained
- *Known for integrity and auditability*
- *TO find us here @YourEarthfood*

2. Session

- Created by Loki Foundation in Australia
- No phone number required
- Onion routing (similar to Tor) hides your location
- Great for anonymous or activist communication
- Find us @YourEarthfood

3. Element (Matrix)

- Secure, decentralised chat system
- Supports bridges to other networks (like Slack, Discord, etc.)
- Good for group collaboration or private family channels
- Find us @yourearthfood @yourearthfood:matrix.org

Pair these with a de-Googled phone or a Linux device to limit tracking.

Emergency Comms: Off-Grid and Decentralised

4. Briar

- Peer-to-peer messaging
- Works without internet: can use Bluetooth or Wi-Fi direct
- Ideal for local organising or blackouts

5. Zello

- Push-to-talk walkie-talkie app
- Can be used in disasters or bushfires
- Needs mobile data but limited footprint

Consider creating a basic comms hub with a burner phone, offline maps, and these apps installed in case of natural disaster, censorship events, or future cyber lockdowns.

Guidance for Beginners and Older Users

For those less tech-savvy or 50+:

- **Write down passwords by hand** and store securely.
- **Use email aliases** to separate high-security logins from social or shopping platforms.
- **Avoid linking accounts** (Google/Facebook logins to other sites).
- **Install Signal with help from a trusted family member or technician.**

We are not here to be *invisible*.
We are here to be **untrackable by default**, **findable only by choice**, and **digitally independent**.

SIDE NOTE OF COMPARISON OF SIGNAL AND TELEGRAM

Telegram: The Pros and Cons

What Telegram Gets Right

1. **Secret Chats for End-to-End Encryption**
   Telegram offers a "Secret Chat" option that is truly end-to-end encrypted: only you and the other person can read it; Telegram's servers don't hold the keys.
   Telegram+2OneRep+2

2. **Client-side Code Open Source (partially)**
   The app's client-side code is open source. This means users can inspect what is happening in the app interfaces. SafetyDetectives+1

3. **Self-destruction & Privacy Settings**
   You can set messages to self-destruct, control who sees your profile details, disable contact syncing, etc. Some good control features are there. Telegram+1

4. **Feature Rich & Broad Reach**
   Telegram has wide adoption, large group capacity, media sharing, channels, large storage via cloud chats, etc. That makes it useful if you need reach, to build community, or share publicfacing content. OneRep+2Tom's Guide+2

Weaknesses & Risks You Must Know

1. **Default Chats Are Not End-to-End Encrypted**
   Regular, cloud chats are encrypted in transit and at rest on Telegram's servers—but Telegram holds the decryption keys. That means those chats are accessible (or vulnerable) if Telegram's servers are compelled by law or breached. Only Secret Chats are fully private. Tom's Guide+2Telegram+2

2. **Server Storage = Possible Exposure**
   Because many chats are stored on their server, if those servers are accessed (legally or otherwise), your messages could be exposed. Also, cloud backups might sync metadata. Telegram+1

3. **Policy Shifts & Cooperation With Authorities**
   After legal or regulatory pressure, Telegram has made changes. It may share metadata (IP addresses, phone numbers) with authorities when presented with legal requests. Following the arrest of CEO Pavel Durov, concern has increased about how Telegram handles such requests. CyberSecurityCue+2Cointelegraph+2

4. **Features That Compromise Privacy**
   Tools like "People Nearby" expose location in less secure ways; public channels are visible to many people; channels can be scraped; group memberships expose connections. Any public group is less private. arXiv+2Tom's Guide+2

5. **Large Platform = Visibility = Target**
   Because so many people use Telegram, big userbase = more attention from governments, surveillance efforts, moderation, legal pressures. The more it's used, the more likely it will be compelled by laws to comply with requests. Reuters+2CyberSecurityCue+2

Where Telegram Might Fit in Your Strategy

If your bar for security is moderate—if you want more privacy and less tracking than WhatsApp, Messenger, or SMS—it can be useful **with caution**. But if you're aiming for maximum privacy & minimal exposure, then you should pair it with other tools or use alternatives.

Here are how you might use Telegram, if chosen:

- Use **Secret Chats** only, for sensitive/private conversations. Never for public or group sharing of private info.
- Turn off contact sync; don't expose your phone number if you can avoid it.
- Put all high-sensitivity communications on more hardened apps (Signal, Session, Element).
- Use Telegram for less sensitive group/community messaging, announcements, public channels.
- Avoid using optional features that reveal your location or metadata.
- Always assume that law enforcement or state actors *could* request data, so don't put anything permanently risky there.

Recommendation (Expert View)

You can say: "Telegram is okay for everyday community connection or semi-public communication, but not good enough as a fully private vault." For the Earthfood Community and *Exit the Matrix* audience, you'll want to emphasise safer alternatives (Signal, Session, Element) for truly sensitive areas of your life.

If you're stepping away from corporate surveillance, **Telegram** can seem appealing—but it's only partially secure. Its regular chats are not end-to-end encrypted and are stored on Telegram's servers, meaning they could be accessed or subpoenaed. If you use Telegram, *only ever use Secret Chats*, turn off contact syncing, and avoid public groups. **Signal** is more secure for one-on-one communication, backed by audited encryption and no cloud storage. **Session** goes further, needing no phone number or email—it's decentralised and anonymous. **Element (Matrix)** is ideal for decentralised communities and encrypted group chats. If privacy is critical, choose Session or Signal. If reach and ease are needed, use Telegram cautiously and strategically.

Lets dive in:

- https://haveibeenpwned.com/ this is the website to get in to see who has been tracking tracing you. This site came about after what was, at the time, the largest ever single breach of customer accounts: Adobe The creators of this software did a deep dive to

find the same accounts exposed over and over again, often with the same passwords which then put the victims at further risk of their other accounts being compromised.

This site serves two primary purposes for me: firstly, it obviously provides a service to the public. Data breaches are rampant, and many people don't appreciate the scale or frequency with which they occur. By aggregating the data here I hope that it not only helps victims learn of compromises of their accounts but also highlights the severity of the risks of online attacks on today's internet.

SECTION 3.2 BROWSING & SEARCH: ESCAPE THE EYES OF BIG TECH

The Problem with Traditional Browsers and Search Engines

When you use Google Chrome or Safari, every site you visit, search term you enter, and link you click is monitored. This information is sold to advertisers, used to profile you, and can be subpoenaed or flagged. You've effectively become a product in someone else's system.

Many browsers also preload surveillance tools like:

- Fingerprinting scripts that track you even in incognito mode.
- Real-time location and microphone access.
- Auto-fill data harvesting.
- AI learning models that use your behaviour to train surveillance algorithms.

Safe Browsers to Use Instead

Brave

- Based on Chromium but strips out Google's trackers.
- Built-in ad-blocker, script-blocker, and tracker-buster.
- Can use Tor mode for anonymous browsing.

Tor Browser

- The most private option, routes traffic through multiple encrypted relays.
- Extremely slow, but highly anonymous.
- Blocks scripts and plug-ins by default to reduce attack surfaces.

Mull (Android Only)

- Hardened version of Firefox, open source.
- Often used in privacy-focused mobile setups.
- Works great with custom DNS and VPNs.

Librewolf (Desktop Only)

- Fork of Firefox, privacy-enhanced with no telemetry or auto-updates.
- Ships with hardened settings out of the box.
- Minimal exposure, maximum control.

Search Engines That Don't Sell You Out

Startpage.com

- Uses Google search results but strips your IP and personal data first.
- Excellent for transitioners who still want good results.

Mojeek

- Built its own independent crawler—no Google, no Bing.
- No profiling, no personalisation.
- Clean, transparent, and based in the UK.

Qwant (Europe)

- French engine complies with EU data privacy laws.
- Mostly independent, although results may still blend in Bing indexes.
- No tracking or ads based on behaviour.

DuckDuckGo

- Formerly popular, but its reputation has taken a hit after it allowed Microsoft trackers.
- Still okay for light use but not ideal for high privacy.

Browser Add-ons to Harden Your Surfing

- **uBlock Origin** – best-in-class ad and tracker blocker
- **Privacy Badger** – learns and blocks invisible trackers
- **ClearURLs** – strips out tracking parameters from links
- **HTTPS Everywhere** – forces encrypted connections where possible
- **Cookie AutoDelete** – wipes cookies after you leave a site

SECTION 3.3 – EMAILS & DIGITAL IDENTITY: RECLAIM YOUR ONLINE IDENTITY

Why Email is the Weakest Link

Your email address is your digital passport. If compromised, it becomes the master key to your online life—bank accounts, utilities, social media, and even identity verification. And most people are using Gmail, Outlook, Yahoo, or Big Tech-owned services that:

- Track your location and metadata
- Scan contents to train AI and sell ad space
- Log keystrokes and device IPs
- Create behavioural profiles for algorithmic enforcement

Once linked to a digital ID system, your email may become part of a unified profile that can be suspended, geo-fenced, or restricted—especially in crisis or "compliance" events.

What You Can Do Instead

🔐 Private, Encrypted Email Providers

ProtonMail

- Based in Switzerland with strong privacy laws
- End-to-end encrypted
- No ads, no profiling
- Free and paid options

Tutanota

- Based in Germany, fully encrypted
- Includes encrypted calendar and contacts
- Supports anonymous signup with no phone number

CTemplar *(currently closed)*

- Was a top choice for ultra-security, now defunct, but mentioned for historical awareness

MailFence

- End-to-end encryption with OpenPGP
- Based in Belgium
- Integrated digital signature features

Strategies for Safer Email Use

- **Use aliases**: Use services like *SimpleLogin*, *AnonAddy*, or *Firefox Relay* to create disposable email aliases so you never hand out your real address.
- **Separate life and identity**: Don't use the same email for newsletters, friends, finances, or subscriptions. Create separate accounts and keep them segregated.
- **Don't link everything**: Avoid using your email as a sign-in method for every app. Opt for username-based logins when possible.
- **Never use real names**: Use a pen name, nickname, or abbreviation for personal accounts. The less they know, the freer you remain.
- **Avoid using your mobile number**: It links your ID across dozens of platforms and can be hacked via SIM swapping. Use secure 2FA apps instead.

How to Transition

1. **Create your private email account** – e.g., ProtonMail.
2. **Forward important emails** from your current Big Tech email.
3. **Update logins** to your new private email gradually.
4. **Set up aliases** for signing up to anything public.
5. **Delete old accounts** once you've finished migrating.

SECTION 3.4 PAYMENTS, CRYPTO & RECLAIMING FINANCIAL AUTONOMY

"You can't be free if someone else controls your wallet."

In a world rapidly moving toward **programmable money** and **CBDCs (Central Bank Digital Currencies)**, reclaiming your financial autonomy is urgent. When your spending, savings, and investments are monitored, scored, or restricted based on **digital ID**, **carbon usage**, or **"social compliance"**, your ability to live freely disappears.

Let's unpack how to **exit the financial control grid**, and don't worry — the advanced steps (like **cold storage wallets**) will be explored in more detail in next month's follow-up booklet:

Exit the AU Matrix: Finances, Land & Legacy

Join our Earthfood Community

to access that exclusive release and learn how to **store wealth offline**, **detox from fiat**, and **build parallel systems** for your family's future.

The Problem with Modern Banking

- Banks are not neutral; they are **enforcement arms** for government policy.
- You already need ID to open or maintain accounts. Digital ID just **tightens the noose**.
- Most fintech apps (like PayPal, Square, Stripe) cooperate with **AUSTRAC**, **FATF**, and other surveillance regimes.

- "Terms and Conditions" allow accounts to be **frozen without cause**, especially for wrongthink or disobedience to mandates.

Just ask the Canadians who donated to the Freedom Convoy, frozen out of their own accounts.

CBDCs: The Final Nail

CBDCs give governments total control over:

- Where you spend
- What you spend on
- Whether you're *allowed* to spend
- Expiry dates on your savings
- Geographic restrictions
- Automatic taxation or fines

This isn't hypothetical—it's already being piloted in over 100 countries. Australia has already completed its pilot phase via the **RBA eAUD white paper**.

Your Options (Simple Steps First)

🔹 **1. Use Cash, Now.**

- Spend in local shops using physical cash. It's anonymous, frictionless, and powerful.
- Encourage others to accept cash. Offer a discount if you're a small business.
- Join **Cash Welcome** movements in your community.

"The more you use cash now, the longer you'll be allowed to."

2. Get Familiar with Decentralised Currencies (Crypto)

Good Entry-Level Platforms:

- **Swyftx** – AU-based, user-friendly, good for learning.
- **CoinSpot** – Australian, supports local bank transfer.
- **Kraken** – International, strong privacy and security.

- **Binance** – Easy interface, but increasingly centralised and compliance-heavy.

NOTE: These platforms are *on-ramps*: they are **still part of the system**. You'll need to **exit from them** if you want real freedom. AUSTRAC will be involved. You are merely learning about them not setting up in them.

3. Self-Custody (Teaser for Next Booklet LOL)

"Not your keys, not your coins."

Owning crypto on an exchange is **not freedom**. You need **offline self-custody tools** like:

- **Cold wallets** (e.g., Trezor, Ledger)
- **Open-source hot wallets** (e.g., Sparrow, BlueWallet)
- **Seed phrase storage** offline in fireproof metal plates

We will go deep into **how to set these up** in *Exit the AU Matrix*. If you're serious about keeping your wealth outside the system, this will be your step-by-step roadmap.

Want access?
Join the Earthfood Community to get the next guide early. 18th October 2025.

4. Set Up Parallel Payment Channels

- **Wise.com** (for now) allows international payments without major banking entanglements and reportable to ATO, AUSTRAC.
- **Monzo**, **Revolut**, **N26** — available outside Australia (check availability and partnerships)
- Consider opening **offshore bank accounts** in nations that respect privacy laws *(more in next booklet)*

5. Deal Directly with People

- Sell or barter directly with trusted groups.
- Join Telegram barter communities or local co-ops.
- Use community vouchers, time-banking systems, and neighbour trust economies.

You don't need AI to live your life. You need **other humans**.

SECTION 3.5 DIGITAL STORAGE, BACKUPS & OFFLINE SURVIVAL TOOLS

"When the cloud crashes, will you still have access to what matters most?"

Most people assume their data is safe because it's on Google, Apple, or Dropbox. But **digital ID infrastructure**, **AI surveillance**, and **blackout-level cyberattack** are being discussed in policy rooms across the world. It's not paranoia, it's **preparation** to be **digitally independent**.

This section is about setting up **offline backups**, **encrypted storage**, and **physical redundancy** and tools to **retain access to your truth, documents, wealth, and identity** if things get messy.

Why Offline Storage Matters

- Australia's cyber war division is now active (see: ASD & Signals Directorate).
- Metadata laws mean **your cloud files are not private**: your notes, photos, health data, backups are accessible.
- Entire Google accounts have been **shut down or frozen** over simple "violations" of vague terms.
- In digital ID regimes, **access to your files can be tied to your compliance**.
- Remember: if they control the access, they control the narrative.

Basic Backup Principles

1. **Don't trust one device** – always have 2–3 copies.
2. **Don't trust one format** – mix of USBs, external drives, SD cards, printed hard copies.
3. **Don't trust one system** – avoid all-in-one ecosystems like Google/Apple where they can lock you out of everything.

Best Practices for Digital Storage

1. Use External SSDs or USBs (Air-Gapped)

- **Sandisk Extreme Pro**, **Samsung T7**, or simple USB 3.1 sticks
- Store copies of your ID, title deeds, property records, crypto keys, and seed phrases
- Disconnect from the internet (air-gapped = not connected = untraceable)

1. **Encrypt your drives** with free tools:

- **VeraCrypt** (open-source, highly secure)
- **BitLocker** (Windows built-in)
- **FileVault** (Mac built-in)

2. Keep Printed Copies

- Birth certificates, IDs, land titles, contracts, wills
- Keep them **in a fireproof safe or lockbox**
- Store one backup copy with a trusted person or location

3.Consider Decentralised Storage

For more advanced users:

- **IPFS (InterPlanetary File System)** stores your data across many nodes
- **Storj** and **Filecoin** are Web3-based storage solutions where you rent decentralised space

Caution: You still need a backup strategy even here.

4. Portable OS + Emergency Boot USB

Create a bootable USB with a secure, encrypted operating system:

- **Tails OS** – for anonymity and emergency boot-up
- **Linux Mint** – full-featured OS you can run on any laptop

With one USB key, you can plug into any machine and **access your digital life** without leaving a trace.

5. Paper Wallets and Offline Maps

- Store your crypto seed phrases **offline** and split them in two locations
- Use metal seed backups (e.g., Cryptosteel) for fire and water resistance
- Print local offline maps in case of blackout, including routes, water sources, fuel stations, community hubs

6. Cold Storage: Coming Next Week

- We'll go deeper into **cold wallets**, **how to store private keys**, and how to **transact peer-to-peer** in our *Exit the AU Matrix* booklet.
- **Join our Earthfood Community** to get early access and setup help.

SECTION 3.6 DEVICES, SURVEILLANCE & PROTECTING YOUR PRIVACY

"The device in your hand may be your greatest tool—or your most obedient snitch."

Your phone knows where you are, who you're with, what you say, how you walk, how you breathe, and even what you're thinking. Most people don't realise this level of surveillance is **already live** and integrated into **Digital ID enforcement systems**.

Whether it's facial recognition in shopping centres, **Bluetooth tracking through smart bins**, or **biometric scanning to access banks**, the key to exiting the digital matrix is **taking back control of your devices**—or minimising dependence altogether.

The Risks in Your Devices

- **Smartphones** (Apple & Android) have built-in spyware pipelines for governments (via laws like CALEA in the US and TOLA in Australia).
- **Cameras & microphones** can be remotely activated. Even if turned "off", apps like TikTok, Instagram, and Facebook run background access.
- **Keylogging** (every tap, swipe, and location) is stored and shared with data brokers — Australia included.
- **Facial recognition databases** are being built from your selfies, photo IDs, and "harmless" filters.
- **Bluetooth contact tracing** (still embedded in OS updates) can build real-time movement graphs.

You don't need to be doing something wrong to be tracked.
You just need to be someone with rights they want to remove.

What to Do Instead

1. Dumb Down Your Phone

- Use a **feature phone** (e.g., Punkt MP02 or Light Phone 2) for daily life
- Turn your smartphone into a "tool, not a tracker" by:
    - Removing Google Play Services (via ADB or installing LineageOS / GrapheneOS)
    - Disabling location, biometrics, Bluetooth, voice assistants
    - Blocking background data for all apps

For advanced users: GrapheneOS (Pixel phones only) or CalyxOS are your best bets for **de-Googled privacy-first phones**.

***Earthfood Community has access to these phones and personnel to set these up for anyone who wants this. Please contact enquiries@yourearthfood.com

2. Use Burner or Dual-SIM Phones

- Keep **one SIM for official use** (Centrelink, Medicare, Govt services)
- Use **another for private or encrypted messaging**
- Never link both numbers to the same apps
- **Buy your second SIM with cash**

3. Get a Faraday Bag or EMP Shield

- Store phones in **Faraday pouches** when not in use to block all signals
- Use for:
    - Meetings
    - Rallies
    - Travel
    - Car keys (smart theft protection)

4. Use Open-Source & Decentralised Apps

Task	Alternatives
Maps & Navigation	Organic Maps, OsmAnd
Notes & To-Do	Joplin, Standard Notes (encrypted)
Browsing	Brave, Firefox + uBlock Origin
Email	ProtonMail, Tutanota, Mailbox.org
App Stores	F-Droid, Aurora Store (anonymous APK downloads)
Banking	Use physical cash + crypto wallet offline

5. Turn Off Everything You Don't Need

- No location.

- No push notifications.
- No biometrics (use passcodes).
- Turn off “Hey Siri” or “OK Google”.
- Disable app permissions that access your contacts, mic, camera, motion sensors.
- Keep **airplane mode** ON when phone is idle, with **WiFi and Bluetooth OFF.**

6. Stop Upgrading Your Devices

Newer phones = more invasive chips, hardcoded AI surveillance, and non-removable software. If your phone works, **keep it**, or get one with:

- **Removable battery**
- **SD card slot**
- **No Face/Voice ID**
- **No background chipsets for “COVID tracking” or “Digital Health Passport” functions**

7. Know Your Legal Rights

- **You are NOT required to provide biometrics** to private companies.
- If an app “forces” you to scan your face, fingerprint, or voice to access a service, **opt out and document it**.
- You may be able to lodge a complaint with OAIC or challenge them under the *Privacy Act* or *Consumer Law* — especially if data breaches result.

NEXT MONTH in *Exit the AU Matrix*, we’ll walk through:

- How to bank without a smartphone
- What to do if your phone is confiscated
- Offline payments & local trading

Want it now? Join the Earthfood Community on yourearthfood.com and get first access to the unfiltered guides, articles and other important material for life living well.

SECTION 3.7 BANKING, PAYMENTS & KEEPING ACCESS TO YOUR MONEY WITHOUT DIGITAL ID

"He who controls the currency controls the people — until the people stop playing with their currency."

Australia's financial system is increasingly **intertwined with Digital ID mandates**, including:

- Biometric facial matching to access accounts
- Mandatory smartphone apps for 2FA (multi-factor authentication)
- "Know Your Customer" (KYC) policies that now go beyond identification and into **behavioural profiling**

If you want to continue accessing **your own money** without bowing to this system, you'll need to **decentralise your banking** and prepare for a **hybrid strategy** that combines:

- Private accounts
- Physical assets
- Offline transaction methods

The Problems We Face in the Banking System

- **Closed-loop systems** — major banks are colluding with regulators to push CBDCs (Central Bank Digital Currencies)
- **De-banking** — people and businesses are losing accounts for "risk" (political views, cash-heavy activity, not using Digital ID)
- **Programmable money** — already trialled by the RBA, this allows limits on:
    - What you can buy (no meat, fuel, ammo, etc.)
    - When you can buy (expiry dates on stimulus money)
    - Who you can buy from (social credit–based vendors)

CBDCs = fully programmable and centrally monitored money.
It's like Centrelink, but with expiry dates, political strings, and no appeals process.

Hybrid Solutions to Exit the Banking Matrix

Here's what we recommend **for now** until the full Exit the AU Matrix booklet is released:

1. Keep Your Current Bank Account, But Limit It

- Keep balances low
- Avoid automatic deposits
- Turn off biometric app login
- Remove saved devices

2. Open an Offshore Account or Fintech Wallet

- Consider a **foreign bank in a neutral jurisdiction** (e.g. Georgia, Vanuatu, or parts of the Caribbean, not the EU, UK or US)
- Alternatively, use **crypto-friendly fintechs** such as:
    - **Revolut** (UK-based, but offers some layers of privacy)
    - **Wise** (less private, but useful for offshore transactions)
    - **AirTM** or **Payeer** (if operating globally)
    - **Crypto wallets** with fiat conversion (we'll expand in Section 3.8)

***Important**: Don't connect these to your Australian ID if avoidable. Use alternate IDs or company structures offshore where legal. We will explain more in the next booklet.*

> *"For those who've joined the Earthfood Community — stay tuned for the **Exit the AU Matrix** resource kit.*
>
> *This private release will contain the practical steps to navigate programmable banking, superannuation risks, and digital currency control systems. To receive it, make sure you're connected. We don't share everything publicly, for a reason."* Bron

SECTION 4: ALTERNATIVES TO FACEBOOK MARKETPLACE

Gumtree

- Email-only sign-up

- No ID required for most listings
- Easy local buy/sell

Trash Nothing

- Giveaways only
- Community-based sharing, not commerce

Nextdoor

- Address verification, but not facial or biometric
- Local groups, buy/sell functions

Locanto

- Classifieds-style
- ID only for risky categories (e.g., adult services)

Buy Nothing Project

- Now has its own non-Facebook app
- Gift economy, neighbour-led

These will be broken down in the next sections following.

Digital Maps & Tracking

(Alternatives to Google Maps, Apple Maps & location tracking tools)

You might not realise it, but every time you open Google Maps or Apple Maps, you're not just getting directions — you're giving away your **real-time location**, **travel patterns**, and even **preferred routes**, which are then logged and often used to build detailed **predictive behaviour profiles**.

These platforms are designed to "personalise" your experience — which often means **tracking you permanently**, even when you think location settings are off. Worse, when paired with your **device ID**, **search history**, and **camera access**, this data can form part of a permanent behavioural record linked to your Digital ID.

Here's how to **take back control** of your navigation, mobility, and spatial freedom — without feeding the beast.

Privacy-Respecting Map Alternatives

Organic Maps

- 100% open-source
- Runs **offline** (no mobile data required)
- Based on OpenStreetMap (community-driven mapping)
- No ads, tracking, or Google integration
  🔗 organicmaps.app

Magic Earth

- Offers turn-by-turn navigation
- Includes traffic & 3D maps, without collecting personal data
- Compatible with Android Auto & CarPlay
- Built-in tracker blocking
  🔗 magicearth.com

OsmAnd (OpenStreetMap Automated Navigation Directions)

- GPS navigation based on OpenStreetMap
- Offline functionality
- Route planning for driving, cycling, walking
- Not as user-friendly as Google Maps, but very secure
  🔗 osmand.net

Additional Tools & Tips

- **Turn off GPS tracking** when not needed — not just "Location Services" in your phone settings, but also in **individual app permissions**.
- Use **offline maps** and **pre-download routes** before travelling.
- If you use Apple, turn off **"Significant Locations"** in Settings → Privacy → Location Services → System Services.
- On Android, regularly review **Location History**, disable **Web & App Activity**, and revoke **location access** from apps that don't need it.

Warning: Vehicle Tracking

Even your car is no longer private. Newer vehicles have:

- **Embedded SIMs** (eSIMs) with location reporting
- GPS + camera sync for insurers
- Microphones for voice command features

- Automatic syncing with your mobile phone's data

Opt out of all data-sharing agreements where possible. If you're buying a car, **ask the dealer** about data settings and privacy controls.

The Real Agenda

Just like social media, maps are being weaponised. Surveillance maps are already being integrated with **smart cities**, **facial recognition zones**, and **automated vehicle checkpoints**. Your GPS data isn't just for you — it's potentially being used to:

- Deny access to areas in "smart cities"
- Flag behaviour as "non-compliant"
- Match movement with digital ID logs

Don't let your feet become traceable data points in someone else's system.

Email & Calendar Alternatives

Most mainstream email and calendar services (Gmail, Outlook, iCloud) are heavily integrated into surveillance infrastructure, with AI scanning your content, attachments, and location data.

Here are **privacy-focused options** for reclaiming your communications and scheduling:

ProtonMail & Proton Calendar

- **Based in Switzerland** with strong privacy laws
- **End-to-end encryption** by default
- **No ads, no data mining**
- Offers secure **calendar**, **VPN**, and **Drive**
- Free tier available, paid gives more storage

🔗 https://proton.me

Tutanota

- Germany-based, open-source
- **Encrypted email and calendar**
- No tracking, ads, or spam mining

- Clean UI, Android/iOS apps

🔗 https://tutanota.com

Mailbox.org

- German secure email provider
- Full-featured suite: calendar, contacts, tasks
- Custom domain support
- Includes Office tools with strong encryption

🔗 https://mailbox.org

Cloud File Storage Alternatives

Google Drive, iCloud, and Dropbox are convenient—but they are **surveillance tools**. They scan your files, flag "policy violations," and store your data on servers subject to government access.

Consider these ethical alternatives:

Internxt

- Zero-knowledge encryption
- GDPR-compliant, no tracking
- Offers file storage, backup, and photo vault
- Based in Spain

🔗 https://internxt.com

Sync.com

- Canadian company with strong privacy policies
- **End-to-end encrypted cloud storage**
- File sharing, password-protected links, team access
- Great for business or family backup

🔗 https://sync.com

Nextcloud (Self-Hosted)

- Host your own cloud system
- Fully private: email, calendar, docs, chat
- Open-source, used by universities, health orgs
- More technical, best for communities

🔗 https://nextcloud.com

Quick Summary

Tool	Feature	Replaces	Notes
Proton	Email + Calendar	Gmail, Outlook	Free + paid tiers
Tutanota	Email + Calendar	Gmail, iCloud	Fully encrypted
Mailbox.org	Full suite incl. Office	Google Workspace	Ideal for SMEs
Internxt	Cloud Storage	Google Drive	Zero-tracking
Sync.com	File Storage	Dropbox	Private & simple
Nextcloud	Self-hosted Suite	All-in-one	For tech-savvy users

Office & Document Tools (Google Docs, MS Office replacements)

If you're using Google Docs, Sheets, or Microsoft 365, you're already inside the belly of the beast.

Your documents are being scanned for keywords, "policy violations," and can even be auto-deleted or flagged by AI without human review. These platforms are **not private**, and often your files are **legally accessible** to authorities under broad data-sharing agreements.

Secure Office & Collaboration Alternatives

OnlyOffice

- Open-source alternative to Microsoft 365 & Google Docs
- Supports docs, spreadsheets, presentations
- Compatible with MS formats (.docx, .xlsx, etc.)

- Self-hosted or cloud-hosted with encryption
- Collaborate without surveillance

🔗 https://www.onlyoffice.com

CryptPad

- Fully encrypted collaborative docs, spreadsheets, whiteboards
- Anonymous use allowed, no tracking
- Based in France with strict privacy laws
- Great for group editing or planning

🔗 https://cryptpad.org

LibreOffice

- Free, open-source desktop suite (no cloud)
- Runs locally, no internet needed
- Extremely powerful (used in schools, NGOs)
- No spying, no ads, completely private

🔗 https://www.libreoffice.org

Etherpad (for communities)

- Simple shared text editor for live notes
- No sign-up required
- Good for activist groups or co-ops
- Host your own for full control

🔗 https://etherpad.org

Why This Matters

Every time you upload a file to Google Docs or Microsoft 365:

- AI reads your work
- Data is stored on U.S.-controlled servers
- You are subject to Terms of Service that allow removal, censorship, and access without notification

Tools like **OnlyOffice** or **CryptPad** allow you to retain ownership of your data, work offline or in encrypted environments, and collaborate without being tracked.

Quick Summary

Tool	Feature Set	Best For	Surveillance-Free?
ONLYOFFICE	Docs, Sheets, PPT, Collab	Business or privacy-conscious users	✅
CryptPad	Encrypted Docs & Boards	Activists, journos, small teams	✅
LibreOffice	Full desktop suite	Home office, offline use	✅
Etherpad	Shared live notes	Groups, temporary colabs	✅

SECTION 5: FINANCIAL FREEDOM (WITHOUT ID OR BIOMETRIC LOCK-INS)

Why this matters: Vietnam recently erased over 86 million bank accounts in an overnight "restructure." Central Bank Digital Currencies (CBDCs) are being trialled globally. In Australia, every bank transaction over $10 is logged and linked to your ID.

To protect yourself:

- Hold cash where possible
- Use physical silver and gold exchanges (see local buyers)
- Set up international banking (more in Booklet 2: Exit the AU Matrix)

- Explore privacy-respecting fintech (Revolut, etc., but beware of those complying with AUSTRAC)

What about crypto?

- Use cold wallets, such as Trezor or Tangem cards (offline)
- NEVER store crypto on an exchange
- Use Monero or privacy coins if safety is paramount

Online Payments & Banking Alternatives

Get your money out of the digital leash while you still can.

If your bank can freeze your account at the flick of a switch or block you from transferring *your own money* without approval, you're not free. And worse, under Australia's **Consumer Data Right** and **Design and Distribution Obligations**, your financial patterns are already being analysed to shape your "behaviour score" or worse, deny you access in the future.

But first: **Don't panic. You have options.**

What's Actually Happening?

- **Digital ID & Payments Merge**: Your identity, spending, and location are being tied together in one control system.
- **Cashless Economy Push**: Australia is phasing out cash. ATMs are disappearing. Large cash deposits are flagged. Many bank branches now only deal with "digital services."
- **Programmable Money (CBDCs)**: The Reserve Bank of Australia (RBA) is actively testing **Central Bank Digital Currencies** (CBDCs). These can be **programmed** e.g. to expire, only work on "approved" purchases, or block donations to non-government-sanctioned causes.
- **Bank Account Freezes**: People have already been debanked for having "wrongthink" on social media or participating in protests.
- **No Legal Recourse**: Most digital terms of service (ToS) exempt the platform from responsibility. Even if they breach you — *you lose*.

Strategies for Digital Financial Independence

Here's a breakdown of what you can start doing today:

1. Use Independent, Ethical Banks

Move your money out of Big 4 banks (ANZ, Westpac, NAB, CBA) who:

- Fund fossil fuel projects
- Partner with WEF digital control agendas
- Block transactions and freeze accounts based on "internal policies"

Alternatives:

- **Regional Credit Unions**
- **Bendigo Bank (better, but still partnered with some big-tech)**
- **Heritage Bank (the best so far)**
- Some **faith-based or cooperative banks** may offer ethical finance with less data-sharing

Check: https://www.marketforces.org.au to see if your bank funds control-based projects

2. Use Cash Wherever Possible

- Cash is **untraceable**, **unprogrammable**, and **immediate**.
- Buying from farmers markets, local stores, or services with cash is a direct *act of sovereignty*.
- Learn to **organise your budget in envelopes** like the old days, it keeps you disciplined and independent.

3. Get a Prepaid Visa/Mastercard

- Buy at Australia Post, petrol stations, or supermarkets
- Not linked to your ID or main bank account
- Use online with a bit more anonymity

Example: Australia Post "Everyday Mastercard"

These are great for low-value transactions like eBooks, subscriptions, or buying seeds without data tracking.

4. Explore "Parallel Economy" Payment Options

Platforms that support sellers and buyers **without** Big Tech surveillance:

Platform	Use Case	Notes
Buy Me a Coffee	Small donations / supporter revenue	Easy setup for creators
Ko-fi	Artist & small business support	Some crypto options
Zelle (not AU)	Peer-to-peer transfers	US-only but good model
Wise	Currency transfers & holding	Low fees, works globally, but still KYC AUSTRAC'ed
Cash App / Venmo (US only)	Peer payments, crypto	Requires ID
Square / Stripe (AU)	For selling services	Easy but surveillance-prone AUSTRAC'ed

These are only useful **if you set them up with alternative ID, emails, or under a trust structure** (see next booklet on living outside AU Matrix).

*KYC=know your customer

5. Cold Storage Your Crypto

We'll go deeper on this in the **Exit the AU Matrix** booklet, but for now:

"If it's not your keys, it's not your crypto."

- Get a hardware wallet (e.g., **Ledger**, **Trezor**)
- Move Bitcoin, Ethereum, Monero, etc. off exchanges
- Back it up with **seed phrases** offline, not in cloud storage

Join our Earthfood Community for our **Cold Storage Quickstart PDF** (coming next month)

6. Avoid Buy Now, Pay Later (BNPL) Traps

Afterpay, Klarna, and others:

- Harvest enormous amounts of behavioural data
- Are building predictive AI spending profiles
- Penalise those with alternative shopping habits
- Will absolutely be part of the CBDC rollout

7. Prepare for Superannuation Shifts

As mentioned earlier:

- Super is no longer guaranteed to be yours
- Programmable money may restrict what you can "spend" your super on
- Some global policy docs hint at **"retirement alignment"** with sustainable behaviour

Future-proof yourself by moving your cash into tangible, usable assets: tools, property, seeds, trade skills, or community projects.

Add-ons for Privacy

To maximise the privacy of even a good browser, install these add-ons/extensions:

- **uBlock Origin** – Blocks ads, trackers, malware
- **Privacy Badger** – From EFF, learns what to block
- **Decentraleyes** – Local content delivery to avoid external tracking
- **ClearURLs** – Strips tracking tokens from URLs
- **Cookie AutoDelete** – Deletes cookies after each tab is closed
- **NoScript** – Advanced tool that blocks unwanted scripts

Install only from trusted sources like addons.mozilla.org or Brave Web Store.

Your Browser, Your Mind

Here's what most don't realise:

- Your *Google bubble* has already been trained for years — it won't show you what you need, only what keeps you in the loop.
- You'll be shocked at what **StartPage** or **Brave Search** shows you — completely different results, often with buried or shadowbanned truths.
- Even worse, in an emergency, you might only be shown **approved narratives.** That could be the difference between freedom and control.

In Summary

To exit the Matrix:

- Your browser = your gateway
- Your search engine = your filter
- Your add-ons = your shield

"Be not conformed to this world, but be transformed by the renewing of your mind..." Romans 12:2

Concrete Actions You Can Take This Week

- Open a credit union account (and use it)
- Withdraw some cash each week and practise budgeting without apps
- Buy a prepaid debit card and test it on a small transaction
- Research Ledger wallets or open-source wallets for crypto
- Begin paying small local purchases in cash and build relationships
- Join our Earthfood Community to get the **Exit the AU Matrix** workbook when released

SECTION 6: WHAT HAPPENS IF YOU DON'T COMPLY

If you refuse digital ID, you may be:

- Denied Medicare access
- Refused service at banks or Centrelinkprivate
- Blocked from MyGov
- Excluded from airlines
- Barred from future property sales

But that's *their* system.

There is another path. We build parallel systems. Local food, direct exchange, barter, local markets, Earthfood Tribe, Private Associations, co-ops, and private land trusts. These are lawful, ethical, and do-able.

SECTION 7: FOR THE OLDER GENERATION (STEP-BY-STEP BASICS)

1. Get a smartphone with NO biometric login
2. Download and learn: Signal, Brave, Protonmail https://brave.com/
3. Avoid MyGov or only use minimal services
4. Don't scan your face at supermarkets or banks
5. Ask for paper statements and physical mail again
6. Use local farmer's markets, barter where you can
7. Stay in community. Isolation makes you vulnerable.

If in doubt, ask someone from the Earthfood Community or other communities to help. We support our elders.

SECTION 8: A CASE STUDY – THE VIETNAMESE DONG

A strange trend swept the alternative community: people started buying Vietnamese Dong in hopes of a currency reset. Many still hold it.

Use your Dong as a symbolic reminder:

What if your local currency becomes useless overnight?

This happened in Vietnam. It could happen here.

Tips:

- Sell if you need the funds
- Hold as a symbolic hedge
- Talk to others who have it: barter, trade, create shared support systems

SECTION 9: LAST THOUGHTS FOR MORE SAVVY OPERATORS.

Practical, low-effort steps to secure your Word doc and workflow (do these now if you want calm)

1. **Work offline on sensitive docs.** Turn off cloud sync (OneDrive/Google Drive/Dropbox) and edit locally.
2. **Remove metadata from Word**:
    - In MS Word: *File → Info → Check for Issues → Inspect Document → Remove All* (this strips author, edits, hidden text).
3. **Save a plaintext copy** for sharing (copy into Notepad and save) removes hidden data and formatting that can leak info.
4. **Encrypt the file** before sending use VeraCrypt container or 7-Zip AES-256 encrypted archive with a strong passphrase. Share the password by voice or Signal, not the same channel.
5. **Use secure messaging/email for sending**: Signal for messages; ProtonMail for email (both are widely used by privacy folks). Don't send passwords in the same message as the file.
6. **Make a checksum** (SHA-256) of the final file and save it. That way you can verify integrity later. (I can give exact command lines if you want.)
7. **Backup to an encrypted USB** (air-gapped is best) and keep a copy offline.
8. **Consider version control**: keep a local folder named something like EDM_Drafts_v1 and move final versions to an encrypted archive.
9. **If collaborating** invite only people you trust into a private folder; remove access once the job is done. Use two-factor authentication on those accounts.
10. **If you're very concerned**, create a burner email / alias for sharing drafts rather than your main accounts.

SECTION 10: EARTHFOOD COMMUNITY DECLARATION

We, the people, declare:

- We do not consent to biometric digital ID systems

- We will not participate in global AI surveillance grids
- We uphold the right to bodily integrity, freedom of thought, and private life
- We will protect each other through local systems of trade, care, and exchange
- We choose living microbes, not digital leashes

Join us. This booklet is just the beginning.

SECTION 11: WANT TO OWN YOUR DIGITAL SELF?

What if there was a way to completely reclaim your digital identity forever? To step outside the system of corporate tracking, spyware, and identity theft... and into a private, encrypted space that only you control?

CYN and the JUBU L33T system offer exactly that: a world-first solution to securing your digital presence with no traceable footprint. Designed for individuals and organisations who value autonomy, this military-grade encrypted system lets you interact online without surrendering your data, privacy, or freedom. From an ephemeral, untraceable operating system on a USB, to secure multi-factor authentication, this technology bridges your physical and digital selves safely and privately. This is not available to the general public.

To learn more or request access, email enquiries@yourearthfood.com with the subject line:
“CYN Tech Enquiry”
We’ll send you private information on how to access and secure your own JUBU L33T Digital Self through our network.

Take the Next Step: Reclaim Your Digital Identity

If you're ready to go further and want real tools, not theories, to help you exit the matrix, we’ve done the work to vet what’s out there. One powerful, real-world solution is the Cyvizen suite, which includes Cytcom, a secure conferencing platform for business and private meetings; and JUBU L33T, a portable OS stack that enables you to operate entirely off-grid while reclaiming your Digital Self.

This is no gimmick: these tools were built for individuals and businesses serious about protecting their identity, data, and autonomy in a world of increasing digital surveillance.
If you’d like to know more or want access to the exclusive ordering and setup info, reach out to our team at enquiries@yourearthfood.com.

Our full resource pack is available upon request for community members only.

Reclaim Your Digital Self with CyviZen OS

If you're serious about escaping surveillance and reclaiming your autonomy, CyviZen OS might be the missing piece. Unlike Windows or MacOS which are riddled with telemetry, hidden backdoors, and data leaks CyviZen OS offers a clean slate every time you boot up, with no persistent tracking, zero data harvesting, and even a Scorched Earth option for secure deletion in emergencies.

Whether you're using the JUBU L33T portable stick or installing it directly onto your device, this operating system empowers you to control your Digital Self. It's your encrypted, untraceable, no-strings-attached escape route from the data-guzzling corporate machine.

Want to know more? Our full CyviZen pack is available to members only join the Earthfood Community and request your access Enquiries@yourearthfood.com in email description **"CyviZenOS"** Your identity. Your data. Your life. Take it back.

Closing Thoughts

They built a system of control. We will build a system of life.

Your consent is powerful. Your refusal is even more so.

This isn't just a document. It's a lifeline. It's your call to look up from the haze, see the world for what it's becoming, and step out of the programmed path. Because that path is heading somewhere, fast, and it doesn't care about you, your family, or your right to live a free life connected to nature, community, or truth.

If you've made it this far, you already know too much to go back. You've read the facts. You've seen the patterns. Now it's time to decide what kind of life you want to lead—and which systems you'll allow into it.

The digital ID push is not about convenience. It's about control. It's about building a programmable future, where access to the basics—food, fuel, finance, freedom—can be revoked at a keystroke. We are not alarmists. We are Australians with our eyes wide open. And we're inviting you to join us in building a parallel system that actually serves people.

This booklet is the first step. A practical toolkit. A digital wake-up call.

But we're not stopping here.

A third booklet is coming. It's called:

EXIT THE AU MATRIX: DOX, DEBT & DOMINION

How to step outside the economic traps, find financial breathing room, protect your patch of Earth, and rebuild from the roots up.

We'll be diving into:

- The truth about the banking system
- Superannuation seizure and housing land grabs
- Food systems collapsing under global treaties
- How to reclaim your wealth, property, health, and purpose
- How to build local economies that actually work

This next booklet will be reserved for Earthfood Community members only. If you want to be among those who rebuild what the system tries to destroy, **join us.**

Because the hour is late. But it's not too late. Prepare. Exit. Thrive.

Next booklet: **Exit the AU Matrix** (Banking, Barter, Water, Growing Your Own, Travel)

For more information, connect with us privately: voice@earthfoodonline.com

of education is granted to the recipient. This licence does not transfer any intellectual property rights. **Any reproduction, modification, distribution, public display, or commercial exploitation of this document (in whole or in part) is prohibited without prior written consent.**

Moral Rights / Attribution
All moral rights in this work are asserted and reserved. Any permitted use must provide appropriate attribution to the author(s) and must not derogate from the honour or reputation of the author(s) or The Earthfood Project.

Confidentiality
Confidential: This document may contain confidential and commercially sensitive information intended only for the named recipient. If you are not the intended recipient, you must not read, copy, forward, use or disclose this document. If you have received this document in error, please notify the sender immediately and delete all copies.

Claims & Notices
If you believe any material in this document infringes your rights, please contact: The Legal Division Enquiries@earthfoodonline.com with full details. All claims will be investigated promptly.

Governing Law & Jurisdiction
This document and any dispute arising out of, or in connection with it, shall be governed by the laws of the State of Queensland, Australia and the parties submit to the non-exclusive jurisdiction of the courts of Queensland.

The Earthfood Project is governed within its own jurisdiction under the Ministry of Agriculture and Soil with of the Great Southern Accord, under Royal Tribal Administration, where members agree by contract to our charter, soil sovereignty mandate, and ethical standards on private, contractual, member-to-member, community standards, sovereignty of soil/seed/water. We choose to operate under private association law, with clear contracts and ethical frameworks.

About the Author

Bronwyn Holm is not your average Australian entrepreneur. She's a soil lover, truth-teller, regenerative agriculture advocate, and the founder of **Earthfood**, a revolutionary microbial solution for growing real food in living soil, by the near extinct Nitrifying Living Soil Microbes. With deep roots in both ancestral farming wisdom and future-facing innovation, Bronwyn has made it her life's work to restore the Earth one patch, one person, and one plant at a time.

After watching governments and corporations accelerate digital control systems under the guise of convenience, Bronwyn knew it was time to speak up. Not as a politician.

Not as a professional activist. But as a mum, a small business owner, a daughter of this country. One of the **Mud Army and descendant of ANZACS, Light Horse Men warriors (4), Bush Fire**

Brigades Founders, Country Town leadership and building of towns from pioneering to CWA presidency for over 25 years accumulatively, legacy Australian sports leaders and way more.

This booklet was born from long nights, deep research, and a driving desire to protect the next generation from a life of biometric servitude, surveillance, and system collapse. It's her way of lighting a signal fire for those ready to exit the artificial matrix and build something human again.

She's not sponsored. Not paid. Not part of any party.

Just one Aussie woman doing what she can, while she can.

You can find her at **yourearthfood.com** or speak with her in person at talks across Australia and soon around the world. Because **this is not just a business, it's a movement.**

Disclaimer: I am not a licensed legal or financial advisor and, therefore, I do NOT provide any legal or financial advice. All information in this document is provided with best intensions, latest research and with a team of experts, hackers for good and a knowledge supply with support by remote computer applications for those who can't work it – We try to support all our community members. We are grounded, ethical and life-giving.

The Matrix is no longer a metaphor. It's a system of biometric IDs, predictive tracking, programmable money, and total control over how you live, move, think, and spend.

Exit the Digital ID Matrix is your field guide to slipping through the cracks: ethically, legally, and powerfully.

Written for ordinary Aussies by someone who refuses to go quietly, this booklet is for truth-seekers, farmers, nurses, grandfathers, builders, mums, and doers of all kinds.

If you want your kids to inherit something more than QR codes and centralised platforms - start here.