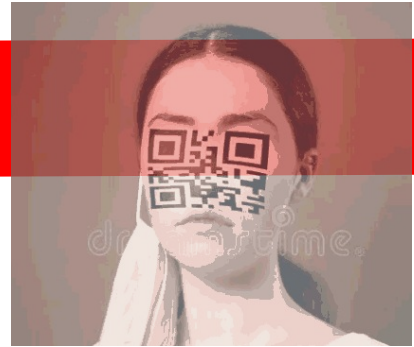


DIGITAL ID IS COMING

This raises issues of:

Privacy Freedom & Control



Profound changes are upon us in how we are identified and monitored

Globally, Digital Identity [DIGID] is being pushed under the banners of convenience, safety, child protection, modernisation and profits

Convenience today - Control tomorrow?

Proving your identity is moving away from real relationships - to digital forms and biometrics where features of your body are scanned to be machine readable and automatically linked to credentials and scores to grant, limit or deny access to services and benefits

NZ DIGID

- **A digital wallet on your phone will store your ID tokens. Encrypted tokens are issued by 'trusted' parties such as Gov agencies. Using the NZ Verify app a token is shown and the verifier only needs to check that its authentic - they do not see or store personal information** [this is positive, but risks need addressing]
- **Includes Gov documents such as passports and licenses**
- **But can expand to include financial records, qualifications, assets [car, house etc], employment, health and criminal records, benefits etc**
- **Is accessed via biometric data (fingerprints or face scans)**

Concerns include [but are not limited to]:

- **Data breaches:** ID databases are high-value targets for hackers risking exposure of people to theft and other abuses.
- **Third party providers** [AWS and Microsoft Azure and undisclosed others!] are under foreign jurisdiction and could access user ID, device or behavioural data
- **Exclusion and coercion:** Refusing a digital ID may block access to essential services, effectively **forcing participation** and enabling digital exclusion.
- **Function creep:** Data can be repurposed for law enforcement, immigration control, or political monitoring. Can start out optional but become unavoidable or mandatory. Can become more centralised

● **Integration with other systems:** DIGIDs are key to the operating and linking of digital currency and behavioural scoring systems, thus enabling total social control

A note on Child Protection

Measures to “protect children online” will regulate and expose everyone. Protection matters, but **broad state control is not protection**

NZ DIGID -----

is decentralised and voluntary – likely a soft start to entice buy-in.

These systems can creep towards enabling ...

Mass tracking of online activity: Link every login, post, purchase to a real ID This enables a comprehensive profile of a person’s life

Loss of anonymity: Impossible to browse or speak without state identification

Censorship and control: block dissenters, deny access to services based on demographics or behaviour

Integration: Combined with facial recognition, location tracking, digital money or behaviour scoring systems for deeper social control

Pre-crime: Using AI analysis of behaviour, face scans, movement patterns, social networks, cameras and phones, a risk score is made and used for restrictions or investigations

We believe these systems pose significant threats to privacy, liberty, and democracy.

**Our aim is to push back and raise public awareness.
Gains should not be at the cost of the right of all Kiwis to live
without excessive surveillance and control**

Is the risk worth it?

As it is, we believe the risks are unacceptable

SAY NO TO DIGITAL ID

Use physical ID. Use cash

For more information and solutions go to <https://didyouknow.nz/digital-id>