Family Voice AUSTRALIA
MAIN POINT
A quarterly essay on important social and political issues
OCTOBER 2024

THE DIGITAL ID: A Threat to Privacy and Freedom

BY PETER DOWNIE

What is the purpose of a Digital ID?

The concept of a Digital ID has been gaining traction globally, touted as a solution to streamline identity verification processes, improve access to services, and enhance security. However, while the idea of a Digital ID might seem beneficial on the surface, it carries significant risks that threaten privacy, data security, and individual freedoms.

Centralisation of Identity Information

At its core, a Digital ID aims to centralise an individual's identity information into a single digital profile. This profile could include various personal data such as name, date of birth, address, biometric information (e.g., fingerprints or facial recognition data), and even records of interactions with government and private sector services.

The primary purpose of a Digital ID is to make it easier for individuals to prove their identity across various platforms, both online and offline. Proponents argue that this centralisation reduces the need for multiple identification documents and streamlines processes such as opening bank accounts, accessing government services, and verifying age for restricted activities.

However, the centralisation of identity information into a Digital ID system poses significant risks. By consolidating vast amounts of personal data into a single profile, the Digital ID becomes a prime target for cybercriminals. A breach of this centralised system could expose an individual's entire identity, leading to identity theft, fraud, and other forms of cybercrime. Moreover, the centralisation of data increases the risk of government surveillance and control, as authorities could potentially access and monitor all aspects of an individual's life through their Digital ID.

Standardisation Across Services

Another key objective of a Digital ID is to create a standardised identity verification process that can be used across a wide range of services. This standardisation is intended to enhance security by ensuring that all services adhere to the same rigorous identity verification protocols. Additionally, it aims to simplify the user experience by allowing individuals to use a single Digital ID for various purposes, from accessing healthcare to conducting

financial transactions.

While standardisation may offer convenience, it also raises significant privacy concerns. The use of a single Digital ID across multiple platforms creates a comprehensive digital footprint that can be tracked and monitored. This level of surveillance poses a threat to individual privacy, as it enables the collection and analysis of vast amounts of data on an individual's activities, preferences, and behaviours.

Furthermore, the standardisation of identity verification processes across services could lead to the erosion of privacy protections. As different sectors adopt the Digital ID system, there is a risk that privacy standards will be diluted to accommodate the needs of various industries. This could result in the creation of a system where personal data is shared and accessed by a wide range of entities, often without the individual's knowledge or consent.

THE AUSTRALIA CARD WAS PROPOSED IN 1985, THEN REJECTED

Enhanced Security and Fraud Prevention

Proponents of Digital IDs often highlight the potential for enhanced security and fraud prevention as key benefits of the system. By using advanced technologies such as biometrics and encryption, Digital IDs are designed to be more secure than traditional forms of identification. This increased security is intended to reduce the risk of identity theft and fraud, making it more difficult for criminals to impersonate others.

However, the reliance on advanced technologies in Digital ID systems also introduces new vulnerabilities. Biometric data, such as fingerprints or facial recognition, is often touted as a foolproof method of identity verification. Yet, if this data is compromised, the consequences can be severe. Unlike passwords, which can be changed if compromised, biometric data is permanent. If a hacker gains access to an individual's biometric information, they could potentially use it to impersonate the individual for the rest of their life.

Additionally, the use of encryption to secure Digital ID systems is not without its challenges. While encryption can provide a high level of security, it is not infallible. As technology advances, so do the methods used by cybercriminals to break encryption. The security of a Digital ID system is only as strong as the encryption methods used, and there is always a risk that these methods could be compromised.

A Digital ID: A Re-hashed National Identity Card?

The concept of a Digital ID bears striking similarities to the controversial national identity card proposals that have been debated in various countries over the years. In Australia, for example, the idea of a national identity card was proposed in the 1980s with the Australia Card.[1] This proposal, which would have assigned every Australian a unique number and stored personal details on a centralised computer, was met with widespread opposition and ultimately abandoned.

Critics of the Australia Card, including legal scholar Justice Michael Kirby, warned that the introduction of a national identity card would fundamentally alter the relationship between the individual and the state. They argued that such a system would lead to increased surveillance and government control over citizens' lives.

Justice Micheal Kirby said that:

> *If there is an identity card, people in authority will want to put it to use. Those of you who have visited Europe where people must always carry such cards, will have noticed the very real difference between the relationship of authority to the individual and that which has hitherto existed in the English speaking countries. What is at stake is not just catching a few tax avoiders. It is not even the efficiency of policing. It is not the defence of innocent and law abiding citizens from law breakers. What is at stake is nothing less than the nature of our society and the power and authority of the state in relation to the individual.*[2]

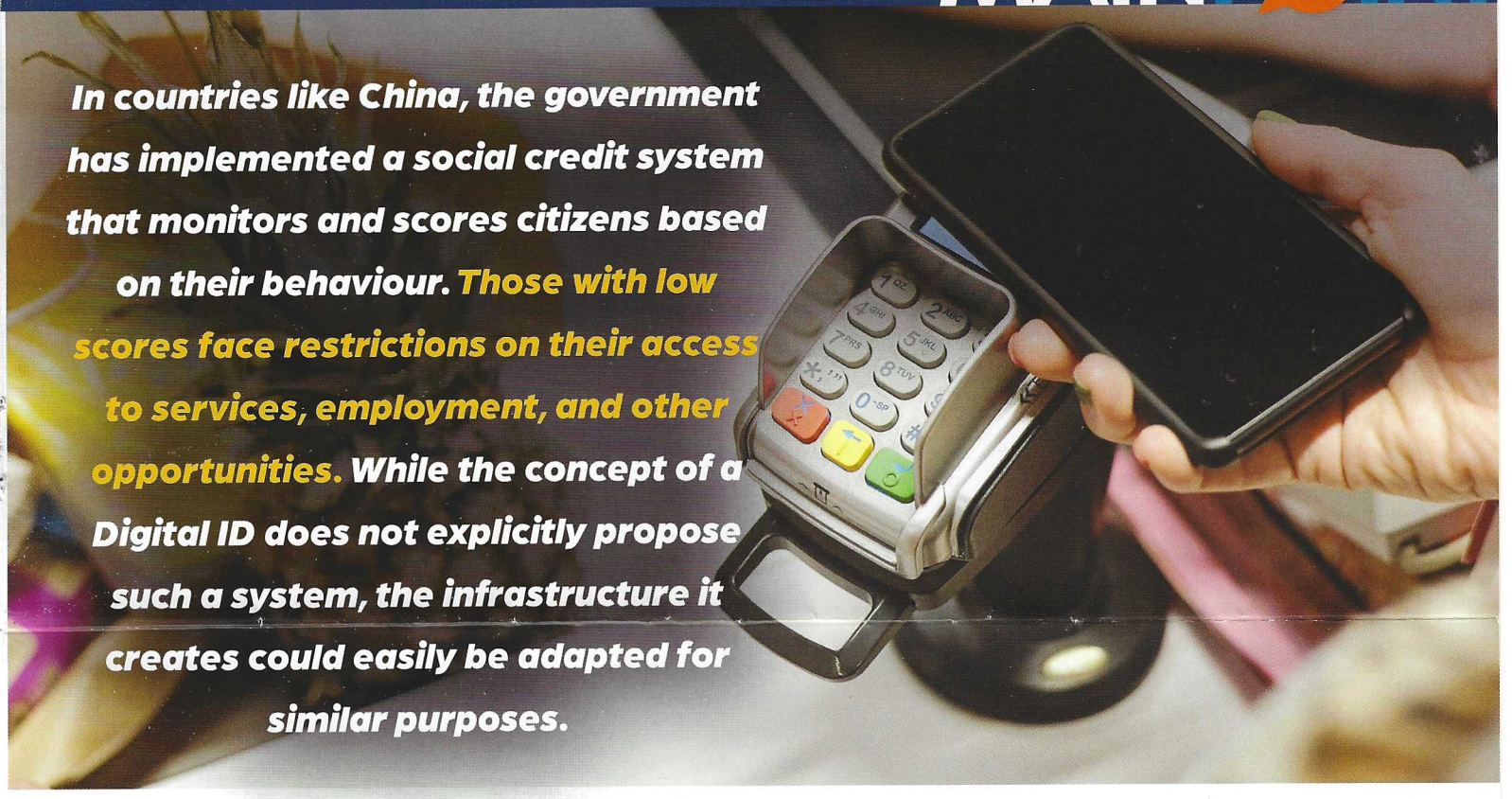
Justice Kirby warned that once an ID card system is established, the risk exists that the database will be enhanced and that more and more officials will seek access to it in the name of efficiency.[3]

The parallels between the Australia Card and the Digital ID are clear. Both systems involve the creation of a centralized database that stores sensitive personal information. While the Australia Card was framed as a physical card, the Digital ID takes this concept into the digital realm, potentially expanding the scope and scale of government surveillance.

Like the Australia Card, a Digital ID system could be subject to mission creep, where the system is gradually expanded to include more data and is used for purposes beyond its original intent. Once established, there is a risk that the Digital ID could be used to monitor and control individuals' behaviour, leading to a significant erosion of privacy and individual freedoms.

Can Governments and Corporations Be Trusted to Securely Manage Our Data?

One of the most significant concerns surrounding the concept of a Digital ID is whether governments and corporations can be trusted to securely



In countries like China, the government has implemented a social credit system that monitors and scores citizens based on their behaviour. Those with low scores face restrictions on their access to services, employment, and other opportunities. While the concept of a Digital ID does not explicitly propose such a system, the infrastructure it creates could easily be adapted for similar purposes.

manage our data.

Senator Alex Antic warned about the Digital ID database:

> *This is going to be the greatest target for hackers. And it will be hacked because it always is.*[4]

Given the track record of data breaches and misuse of personal information, these concerns are well-founded.

In recent years, there have been numerous high-profile data breaches involving both government agencies and private companies.[5] These breaches have exposed sensitive personal information, including names, addresses, financial details, and even biometric data. The consequences of these breaches are often severe, with victims facing identity theft, financial loss, and damage to their reputation.

For example, in 2023, a major data breach involving a government agency in Australia exposed the personal information of thousands of individuals. This breach included sensitive data such as passport numbers, tax file numbers, and Medicare details. The fallout from this breach was significant, with many individuals experiencing identity theft and financial fraud as a result.

Similarly, private companies have also been involved in significant data breaches. In 2022, a major telecommunications company suffered a breach that exposed the personal information of millions of customers. This breach included data such as names, addresses, phone numbers, and email addresses. The company faced significant backlash from customers and regulators, with many questioning whether the company could be trusted to protect their data in the future.

These incidents highlight the challenges of securely managing personal data, particularly in a centralised system like a Digital ID. The more data that is stored in a single location, the more attractive it becomes to cybercriminals. Even the most secure systems can be vulnerable to attack, and the consequences of a breach in a Digital ID system could be catastrophic.

Moreover, the involvement of private companies in the management of Digital IDs raises additional concerns. While these companies may have advanced security measures in place, their primary motivation is often profit rather than the protection of individual privacy. There is a risk that private companies could misuse or monetise the data stored in Digital ID systems, leading to further erosion of privacy rights.

Given these challenges, it is difficult to trust that governments and corporations will be able to securely manage the vast amounts of personal data required for a Digital ID system. The potential for data breaches, misuse, and surveillance is too great to ignore.

A Threat to Freedom

Beyond the immediate concerns about privacy and data security, the concept of a Digital ID poses a broader threat to individual freedom. In democratic societies, there is a delicate balance between the need for security and the protection of individual rights. A Digital ID system threatens to tip this balance in favour of increased government control and surveillance.

One of the most concerning aspects of a Digital ID is its potential to be used as a tool for social control. In countries like China, the government has implemented a social credit system that monitors and scores citizens based on their behaviour. Those with low scores face restrictions on their access to services, employment, and other opportunities. While the concept of a Digital ID does not explicitly propose such a system, the infrastructure it creates could easily be adapted for similar purposes.

In a Digital ID system, the government or other authorities would have access to a wealth of personal information,

including data on an individual's movements, online activities, and interactions with various services. This data could be used to monitor and control individuals' behaviour, leading to a loss of autonomy and freedom.

For example, a Digital ID could be used to enforce compliance with government regulations or social norms. Individuals who fail to comply could be penalised, with their access to services restricted or their movements monitored. This level of control is incompatible with the principles of a free and democratic society.

Moreover, the centralisation of personal data in a Digital ID system increases the risk of government overreach. In times of crisis, governments may be tempted to use the system to monitor and control citizens in ways that would be unacceptable in normal circumstances. For example, during the COVID-19 pandemic, some governments used digital tools to track individuals' movements and enforce quarantine measures. While these measures may have been justified in the short term, they set a dangerous precedent for the use of digital tools to control citizens' behaviour.

The potential for government overreach is not limited to authoritarian regimes. Even in democratic societies, there is a risk that a Digital ID system could be used to suppress dissent and stifle free expression. For example, individuals who participate in protests or engage in political activism could be tracked and monitored through their Digital ID. This could have a chilling effect on free speech and political participation, as individuals may fear retribution for expressing their views.

The introduction of a Digital ID also raises concerns about discrimination and inequality. In a society where access to services and opportunities is increasingly dependent on digital identity, those who are unable or unwilling to participate in the system may be marginalised. This could include individuals who are concerned about privacy, those who lack the necessary technology, or those who face barriers to obtaining a Digital ID. The result could be a two-tiered society, where those with a Digital ID enjoy greater access to services and opportunities, while those without are left behind.

What is the alternative?

Given the significant concerns surrounding the concept of a Digital ID, it is essential to consider alternatives that protect privacy and freedom while still addressing the need for secure identity verification.

One alternative is to enhance existing identification systems rather than creating a new centralised Digital ID. For example, governments could focus on improving the security and privacy of current identification methods, such as driver's licenses or passports, without centralising all personal data into a single digital profile. This approach would reduce the risks associated with centralisation while still providing a reliable means of identity verification.

Another alternative is to explore decentralised models of digital identity. In a decentralised system, individuals retain control over their own personal information, rather than relying on a central authority to manage it. Blockchain technology, for example, has been proposed as a means of creating secure, decentralised digital identities that are resistant to hacking and government surveillance. By distributing data across a network of computers, rather than storing it in a central location, decentralised systems can offer greater security and privacy.

Finally, it is essential to consider the ethical implications of any digital identity system. Rather than prioritising convenience or efficiency, the design and implementation of digital identity systems should be guided by a commitment to protecting individual rights and freedoms. This includes ensuring that individuals have control over their personal data, that privacy is respected, and that the system cannot be used for surveillance or social control.

Conclusion

The concept of a Digital ID represents a significant shift in how personal information is managed and controlled. While the idea of a Digital ID may offer some benefits in terms of convenience and security, it also poses significant risks to privacy, data security, and individual freedom. The centralisation of identity information into a single digital profile creates a prime target for cybercriminals, while also increasing the potential for government surveillance and control.

As societies grapple with the challenges of the digital age, it is essential to approach the concept of a Digital ID with caution. The lessons of the past, such as the debate over the Australia Card, remind us of the dangers of centralising personal information and the potential for government overreach. Rather than rushing to implement a Digital ID system, governments should explore alternative models that protect privacy and freedom while still addressing the need for secure identity verification.

Ultimately, the protection of individual rights and freedoms must be the guiding principle in the development of any digital identity system. By prioritising these values, we can create a system that enhances security and convenience without sacrificing the privacy and autonomy that are essential to a free and democratic society.

References

1. Alasdair Livingston & Roslyn Phillips, "State control by stealth: The Australia ID Card", Resource paper November 1986
2. *Ibid.*
3. *Ibid.*
4. Senator Alex Antic interview with Alan Jones, "New bill introduces a China-style digital identity system: Senator Alex Antic", ADH TV, 20 July 2022, https://www.youtube.com/watch?v=jXfVeygdYL0
5. Erica Mealy, "A national digital ID scheme is being proposed. An expert weighs the pros and (many more) cons", The Conversation, 27 September 2023, https://theconversation.com/a-national-digital-id-scheme-is-being-proposed-an-expert-weighs-the-pros-and-many-more-cons-214144