Australian Prison Reform Journal

Mandatory national ID?

Australian Prison Reform Journal

Volume 4, Issue 4, Article 3, 2024

Cameron I Russell

View ORCID profile

URL: www.aprj.com.au/articles/APRJ-4(4)-3-Mandatory-national-ID.pdf

Abstract

Australia currently has a voluntary national digital identification system. As Australia's Digital ID system becomes ever more pervasive, this article examines the likely effects on prisoners should the national Digital ID become mandatory.

Background

A national ID card was floated by the Hawke Government at the 1985 Tax Summit with the main purpose of reducing tax avoidance and health and welfare fraud. The *Australia Card Bill 1986* was introduced by the Federal Labor government in 1986 and again in 1987, but it was blocked by the Senate both times. By that time, the Australia Card had become highly unpopular due to privacy concerns, and the Federal Government abandoned the bill. Instead, the Government proceeded to expand the tax file number scheme.

Despite opposing the Australia Card in 1986 and 1987, the Howard-led Liberal Government sought to introduce the Australia Card for security reasons following the London Bombings in 2005. When this Australia Card initiative failed, Howard proposed an Access Card based on an expansion of the Medicare card using a smartcard with a microchip containing encrypted health and social services information, but the Government lost power and the Labor Rudd Government terminated the Access Card initiative in 2007.

Australia still has no national ID card. Identity may be proven by providing documents such as an Australian driver's license, Australian/overseas passport, birth certificate, Medicare

card and proof of age card (typically gathering 100 points of ID). Australians may also access online services by verifying their ID using the Australian Government Digital ID system (Department of Finance 2021) which incorporates the myGov gateway to government services (launched in 2013) and the myID (formerly myGovID), a digital ID app launched in 2019 that allows access to myGov and other government online services. Users can verify their identity using verified Australian ID documents, possibly strengthened by biometrics such as fingerprints or facial recognition.

Introduction

The *Digital ID Act 2024* (Cth) and the *Digital ID (Transitional and Consequential Provisions) Act 2024* (Cth) both commenced on 1 December 2024. The new Acts expand the Digital ID system in a number of ways. The Acts allow the Australian Government to expand the number of government services that can be accessed using the Digital ID. The Digital ID also encompasses the government services of the states and territories if they successfully apply to join the system. Finally, it allows accredited private providers of Digital ID services to create and re-use Digital IDs. The *Digital ID Act 2024* is so broad that it even allows foreign companies registered under Division 2 of Part 5B.2 of the *Corporations Act 2001* (Cth) to apply to act as a provider (s.14(2)(b) *Digital ID Act 2024*).

The Acts govern how these providers are to keep personal information safe, secure and private; with regulation by the Australian Competition and Consumer Commission (ACCC) receiving responsibility for the Accreditation Scheme and the Office of the Australian Information Commissioner (OAIC) undertaking responsibility for the privacy aspects of the Digital ID System.

Although involvement with Australia's Digital ID remains voluntary (both for providers and citizens), the system has now greatly expanded. It is likely that the Digital ID will become so ubiquitous in Australian society that there will be pressure on the government to make the Digital ID compulsory for financial reasons, and unlike in the past, citizens will be disinclined to oppose this for reasons of convenience. This article examines the likely effects on

prisoners should the national Digital ID become mandatory. It is a complex issue because some of the effects on inmates will be positive and others will be negative. Both positive and negative effects of the Digital ID tend to flow from the well-documented vulnerability of incarcerated people who are on average poorer, sicker and with fewer opportunities than the rest of the community.

Potential benefits of a mandatory Digital ID come with downsides

Some of the main advantages of a Digital ID, whether mandatory or voluntary, are convenience, security and savings in costs and time. In the traditional '100 points of ID' system, a person must gather multiple physical documents with assigned points adding up to at least 100 points. These documents may need to be photocopied, witnessed, scanned and/or emailed/mailed/shown in person. The system is cumbersome and open to fraud, lost/damaged documents and ID theft. The Digital ID, on the other hand, is easier to establish and can be used thereafter with greater security to quickly verify ID for a range of government and private services. These benefits of convenience, security and savings in time and effort are typically afforded prisoners when they have access to the Internet. Because very few inmates in Australia have Internet access, a mandatory Digital ID will mainly benefit non-prisoners and contribute to the existing digital and social divide between prisoners and the rest of the community.

Although prisoners may be excluded from many of the benefits of the Digital ID, the prisons may take full advantage of it. The prisoner ID (e.g. 'MIN' in NSW or 'CRN' in Victoria) may be expanded to the Digital ID system in prisons, thereby monitoring the movements and activities of inmates in real time with greater accuracy and control. Biometric information may be gathered under the Digital ID system, so CCTV cameras can record with greater certainty the location of each prisoner at any time. While the biometric surveillance system of China is regarded with horror in Australia, many would consider that such a system makes sense in a prison. Correctional officers could know where everyone is without relying on prisoner ID cards (which can be lost, stolen, swapped, manipulated, etc). This virtual Panopticon, it would be argued, would save their time, reduce cases of mistaken identity

and increase control over developing situations with regard to drugs, violence, gang/extremist activities and attempted escapes. It would also allow for more easily accessed and efficient health, education, legal and rehabilitation services in prison, all of which aid in rehabilitation and reduce recidivism. Visitors, correctional services officers and staff members may similarly be monitored using the Digital ID for their safety and for accountability. Significant cost savings would flow from the reduced administrative burden. There are, however, some unintended side effects. Some incarcerated people of interest to the authorities may become socially isolated because of the more intensive surveillance on them, which will in turn harm the prospects for their rehabilitation. If correctional officers have access to far more data on each prisoner, there is the possibility of correctional officers engaging in unfair treatment, bribery, coercion and extortion. Another negative effect is that if there is accentuated surveillance and control, prisoners may feel untrusted and act accordingly, adopting an 'us vs them' response that finds ever-more creative ways to skirt the intrusive Digital ID.

> "As the success of Norwegian prisons demonstrates (Johnsen et al. 2011; Benko 2015; Hoidal 2018; Midtlyng 2022:6-9), trusting prisoners and allowing them social interaction and privacy can be restorative, whereas observing inmates at all times and locations makes them adversarial, recidivistic and creative in avoiding surveillance. A study on CCTV in four Queensland prisons notes that, 'CCTV schemes have been criticised as they are frequently implemented based on the presumed benefits that result from camera surveillance rather than being based on any clearly articulated objectives' (Allard et al. 2006:5). The four prisons studied, however, did not select the default blanket CCTV surveillance. Rather, they were consistent in locations not watched (Allard et al. 2006:11). Interviewed managers said that the gym, hall, education/program rooms and industries/workshops had no cameras because people went there for the right reasons and were engaged. Regarding exercise yards, one manager said staff had a good view anyway and another said there were 'some issues in exercise yards' but that the absence of cameras enabled prisoners to 'have a bit of a chat' and gave them 'a degree of privacy' (Allard et al. 2006:15). Enlightened decisions may be risky for brave decisionmakers, but they strike the right balance between safety, security, prevention, operability on one hand and privacy, dignity, freedom and health on the other. Finding this optimal balance applies equally to

prison design, the extent of CCTV in vulnerable locations, and the surveillance powers of law enforcement, security and intelligence agencies."
Russell CI (2022) 'No to expanded powers-1', Australian Prison Reform Journal, 2(2)-1.

Potential negative effects of a mandatory Digital ID on prisoners

People in prison experience higher rates of chronic illness, mental health disorders, communicable disease, family violence, trauma, risky behaviours, addiction, disability and premature death than the general population (AIHW 2023; RACGP 2023, pp. 1-3). Upon release from prison, a high proportion are stigmatized and experience homelessness, unemployment, depression, overdose and premature death (AIHW 2023, Allison 2018, pp. 52,130). Indeed, the downward spiral towards prison begins with disadvantage (Vinson 2007) and, according to many restorative and transformative justice criminologists, incarceration is itself a form of retributive justice and a coercive method of state-sanctioned violence (Downes 2020, p. 209; Grimsrud 2015; Grimsrud and Zehr 2002; Thuma 2019, pp. 11-12). It is hard enough for people in the outside community, with easy access to technology, to safely configure and maintain their Digital ID and consider the implications of allowing more and more of their personal data to be held online. It is, however, a far greater challenge for incarcerated people with engrained disadvantage to try to organize family, friends and a number of prison staff, and follow strict procedures, just to achieve a simple outcome requiring verification of ID. At the same time, being more vulnerable than the rest of society means that prisoners are less able to defend themselves from possible negative effects of a mandatory Digital ID.

One of the first areas of vulnerability is that the privacy and security of the prisoners' ID is not entirely in their hands, and infringements in that privacy and security cannot easily be avoided or rectified. Prisoners are also in a state of relative powerlessness so their data could fall under the control of prisons or corporations. Even if their privacy is protected by the government, their vulnerability could lead to them being coerced or manipulated to give control of their data to others. Corrective services and the government generally could add a great deal of information to the prisoner's Digital ID (including positive things like work and courses completed, and negative things like poor behaviour and shady associates),

some of which could be accessed to influence such things as privileges and parole hearings. Unfair outcomes such as detrimental categorization and decisions could result from biased selection of the inmate's data and lead to ongoing stigma. Even if the prisoner's Digital ID data is used without bias, an inmate could be strongly pigeonholed based on the extensive Digital ID data without allowing for the possibility of redemption following a change of heart. Such pigeonholing could limit the prisoner's opportunities for positive work, training and rehabilitative programs, thereby perpetuating the negative classification imposed. This is of particular concern given that the private sector will now be able to administer the Digital ID system. Private providers will tend to focus on what clients want to pay for, such as an assessment of the suitability of a person for a job vacancy, which will expand the present police check barrier to employment for ex-prisoners. Private providers will be more inclined to use biometrics to label ex-prisoners for the remainder of their lives, thereby harming their efforts to reintegrate with society. The biometrics allowed in the Digital ID system is also a danger to free speech and freedom of religion. As the Electronic Frontier Foundation notes, 'Government mandated biometric systems are invasive, costly, and damage the right to privacy and free expression. They violate the potential for anonymity, which is crucial for whistleblowers, investigators, journalists, and political dissidents' (n.d.).

Another vulnerability is that if sensitive prisoner data is hacked into, the safety of the prisoner could be put at immediate risk. The Digital ID system is presently promoted as highly secure, but there have been recent reports of hackers linking genuine myGov accounts with fake ones in order to make false Centrelink, Medicare and ATO claims (Appleby 2024). Cybercriminals can also find vulnerabilities along the transmission path or acquire the data encryption keys. As we approach artificial superintelligence and with quantum computing coming on board, current encryption protocols will soon be broken (Thorson 2024). While a breach might cost most people or the Government a sum of money, it could lead to the stabbing of a prisoner as a result of gang violence or retribution, or to changes in the prison operations that could harm the prisoner.

Conclusion

Many of the potential positive effects of a mandatory Digital ID system for prisoners are associated with a downside. At the very best, prisoners can be afforded the same benefits from a Digital ID as those enjoyed by the outside community, provided that prisoners have the technological skills to use computers and at least restricted Internet access (which is not presently the situation in Australia). Since inmates cannot use their Digital ID, a mandatory Digital ID would contribute to the digital divide between prisoners and non-prisoners and the sense of isolation from the outside world of prisoners.

It would mainly be prisons that can benefit from the Digital ID by being able to enhance surveillance, control and administrative functions. Tighter control of prisoners, however, does not encourage the rehabilitation of prisoners – indeed it harms their reintegration into society by impairing trust, dignity and autonomy.

In many ways, a mandatory Digital ID system would represent a number of dangers and disadvantages for prisoners alongside the limited benefits. The solution is not, of course, to deny all Australians the convenience and other benefits of the Digital ID so that prisoners and non-prisoners have the same access to Digital ID. Rather, keeping the Digital ID system voluntary would ensure that prisoners who believe that a Digital ID would be personally dangerous or disadvantageous can avoid it and instead rely on the '100 points of ID' system. In the long term, prisons can progress towards at least restricted access to the Internet so that prisoners have the option of controlling their Digital ID and some of the government services, and even certain health/educational/informational/rehabilitative services. It will then not be such a giant leap when people are released from prison and start trying to access government and private services with their Digital ID.

References

AIHW [Australian Institute of Health and Welfare] (2023) 'Adults in prison', Australian Government, accessed 19 January 2025.

Allard T, Wortley R, and Stewart A (2006) 'The purposes of CCTV in prison', *Security Journal*, 19(1):58-70, Palgrave Journals.

Allison, F (2018) 'Justice reinvestment in Cherbourg: Report on initial community consultations', Steering Group of Cherbourg community, government and non-government representatives, Cherbourg.

Appleby B (10 October 2024) 'Addressing the Rise in myGov Account Hacks: What you Need to Know!', Highview Accounting & Financial (accessed 19 January 2025).

Benko J (26 March 2015) 'The radical humaneness of Norway's Halden Prison', *The New York Times Magazine*.

Department of Finance (2021) 'Australia's digital ID system', Australian Government, accessed 13 January 2025.

— (2024) 'Digital ID Act 2024 legislation is coming', Australian Government, accessed 16 January 2025.

Downes, J (2020) 'Re-imagining an end to gendered violence prefiguring the worlds we want'. In EL Hart, J Greener, and R Moth (Eds.), *Resist the punitive state: Grassroots struggles across welfare, housing, education and prisons* (pp. 208-231). Pluto Press.

Electronic Frontier Foundation (n.d.) 'Mandatory national IDs and biometric databases', EFF, accessed 19 January 2025.

Grimsrud, T (2015) *Violence as a theological problem*. Zehr Institute for Restorative Justice.

Grimsrud, T, & Zehr, H (2002) 'Rethinking God, justice, and treatment of offenders', *Journal of Offender Rehabilitation*, 35(3-4): 253-279.

Hoidal A (2018) 'Normality behind the walls; Examples from Halden Prison', *Federal Sentencing Reporter,* 31(1):58-66.

Johnsen B, Granheim PK, and Helgesen J (2011) 'Exceptional prison conditions and the quality of prison life: Prison size and prison culture in Norwegian closed prisons', *European Journal of Criminology*, 8(6):515-529.

Midtlyng G (2022) 'Safety rules in a Norwegian high-security prison: The impact of social interaction between prisoners and officers', *Safety Science*, 149(May 2022):1-10.

RACGP (Royal Australian College of General Practitioners) (2023) *Standards for health services in Australian prisons* (2nd ed.).

Thorson C (26 June 2024) '[Cracking encryption: The quantum threat]', Govloop, accessed 19 January 2025.

Thuma, EL (2019) *All Our Trials: Prisons, policing, and the feminist fight to end violence,* University of Illinois Press.

Vinson, T (2007) *Dropping off the edge: The distribution of disadvantage in Australia,* Jesuit Social Services.

Legislation

Corporations Act 2001 (Cth)

Digital ID Act 2024 (Cth)

Digital ID (Transitional and Consequential Provisions) Act 2024 (Cth)