Submission by Organisation

Concerned Lawyers Network

Date: 27th October 2021

To: digitalidentity@dta.gov.au

Re: Feedback on all other parts of the Trusted Digital Identity Bill 2021 exposure draft package

I Maria Rigoli, Lawyer, both personally, and also in the capacity as founder of and on behalf of the Concerned Lawyers Network and its subscribers, submit our strong objection to the "Trusted Digital Identity Bill 2021" on the following grounds and based on the following facts, testimonies and feedback given by subscribers to the Concerned Lawyers Network.

Where reference is made to the first person it also means in relation to the third person ie "I" or "my" also means and includes "our".

AUTHORITY FOR EXPANSION NOT JUSTIFIED

Section 5.1 allows for authority for expansion. Expansion to what? There is far too much scope for further abuse and intrusion into our private lives under such a scheme as this. Given there is now a capability for police to access, delete and modify our personal electronic communications, how secure would be our personal information from amendment or deletion – thus rendering it useless to the individual and denying them the ability to use the digital ID verification service at all? For example, should there be any future intention to link such a digital identity to bank accounts, Tax File Numbers, Medicare numbers etc., there would be excessive control held in onedigital identity "document" subject to the whim of those controlling the data. It is arguable that access to our own bank accounts, funds, property etc., could be altered or even denied – either legally or illegally.

VOLUNTARY NATURE OF THE DIGITAL ID CANNOT BE GUARANTEED

Just as Scott Morrison P.M. announced in 2020 and 2021 that vaccinations would not be mandatory or compulsory, we can see that these types of express representations from even those highest in office, cannot be guaranteed.

Section 7.3: While participation in this system is currently being promoted as "voluntary", how long before government decides it should be mandatory? Once such a system is made mandatory, an individual's personal information is on record, and actually it is possible to never be deleted, even upon demand.

In an email from Jason Falinski MP, Federal member for Mackellar responding to a constituent's concerns on 26.10.21, he states the following but cannot guarantee future legislation introduced

to make digital id compulsory and necessary to transact as a consumer or trade as a business or for individuals to be able to carry out their day to day activities as they have in the past without being compelled to have a digital id. There is no mention of what oversight and accountability of the government there will be and if it is funded by government departments of any kind then it cannot be impartial or unbiased.

*"Digital Identity is already **entirely voluntary** and **'opt-in**' for the people who choose to use it.*

If people can't use Digital Identity, or don't want to, they can keep accessing government services online, over the phone or in person at government shop fronts. There is no need for them to 'opt-out' of the system to access the services they need.

People always have full control over their information on the system.

Biometric information, such as a person's photo, can only be checked with their consent directly against the photo provided on their identity documents, such as a driver license or passport photo – it can't be checked against other biometric databases.

That means that the photo someone takes of themself is matched only against the photo on their identity document, such as their passport.

The Bill provides that people's biometric information must not be retained unless the entity has been given an exemption for testing. Even if the entity has been granted such an exemption, there is a hard cap of 14 days – after this point, it must be permanently deleted. This will ensure there is no risk of the system evolving into a new biometric data store.

The digital identity system operates under existing laws including the Privacy Act. The Trusted Digital Identity Bill will put additional safeguards in place over and above those already in force.

The legislation, which once passed by Parliament, will also establish permanent oversight and governance structures and enshrines in law important privacy and consumer protections."

<u>Example/evidence</u>

There is already a director digital id that is required of company directors on or before November 2022 otherwise directors of companies face criminal and civil penalties and may not be able to therefore run their companies any further or even hold a bank account in the name of the company. It is stated that directors MUST have a myGov ID in order to comply with the digital ID in order to continue as directors. Further any new directors will have to do the same when they register with ASIC. All the company and business registration bodies are being centralized and

thus director identifications are as well. https://aicd.companydirectors.com.au/resources/director-id

Further, there is no guarantee that an individual can opt out after they opt in of the new Digital Identity framework.

ADDITIONAL PRIVACY SAFEGUARDS WILL FAIL AND CANNOT GUARANTEE PRIVACY FOR AUSTRALIANS

Section 7.5.1: "Additional Privacy Safeguards". Sounds impressive, but under Section 9 and Section 10.1 the relevant Minister has the authority to alter rules and therefore restrictions or uses to which this digital ID could be put to use. I do not trust any politician or bureaucrat to act in my personal best interests, or the best interests of any normal individual/citizen of this country.

Section 7.5.2: Deactivation – Currently states that deactivation of an individual's digital ID must be completed "as soon as is practicable" after the request is made. Deactivation must occur within a mandatory and absolutely minimal time, not what would effectively be at the convenience of the authority or whatever entities and agents involved.

Section 8: In light of many breaches of privacy by various private companies and government Departments shown to already have occurred, I do not trust any government department or any entity authorized, contracted or in anyway engaged to hold any of my personal information.

Cyber attacks are common, and likely to increase, meaning my personal information would not be sufficiently secure for me to trust this system.

Section 8: Any centralized source of all relevant identifying information about individuals is far more vulnerable to being accessed and to fraud and cyber attack, making identity theft far more likely. NO government department, authorized entity, contractor or other agency can ever guarantee the total security of the data and information stored by them. They simply cannot; therefore I do not and will not trust them.

The oversight powers are unlimited and do not provide for accountability and redress to the people of Australia and there is no appeal mechanism or oversight for the oversight authority who may well be only government appointed and/or government tax payer paid appointees:

88 Powers of the Oversight Authority
The Oversight Authority has power to do all things necessary or convenient to be done for or in connection with the performance of

its functions.
89 Independence of Oversight Authority
Subject to this Act and other laws of the Commonwealth, the Oversight Authority has discretion in the performance or exercise of the Oversight Authority's functions or powers and is not subject to direction by any person in relation to the performance or exercise of those functions or powers.

This is a very risky and undesired situation, which should be addressed by substantially limiting its powers in the final legislation.

COST TO INDIVIDUAL AND COMMUNITY TAXES FOR PROPOSED DIGITAL ID IS NOT JUSTIFIED NOR FINANCIAL VIABLE

Section 11.2: Charging – Does this mean that we as individuals be expected to pay for using this system? Even if we do not pay a direct fee, no doubt all businesses, departments and other entities or agents using the system will exact a cost to cover any "charges" they pay for using the system. This would be yet another financial imposition on the individual – simply for existing and being able to prove it using this system.

Section 11.2: Why is "additional domestic and global research" being conducted? Why does "global research" need to be done? If this is a purely Australian government initiative, there should be no need for "global" research or engagement. The implications of "global" use are concerning.

TECHNOLOGY SHOULD NOT BE IMPOSED ON PEOPLE UNABLE OR UNWILLING TO USE IT

Not everyone can or chooses to use on- line applications, computers or smart phone means of conducting business or personal day to day activities.

We have the right to <u>not</u> have to own or use a computer or smart phone or a third party's. We have the right to transact in cash without all of our personal sensitive private information being uploaded anywhere. We have the right to freedom of movement.

Imposing a digital or any type of artificial intelligence system on an individual or group of people infringes human rights laws domestically and internationally. Will the Digital Identity Bill be in accordance with the Universal Declaration of Human Rights signed in December 1948 by the United Nations and additionally will it comply with the seven key human rights treaties that Australia is party to and will it enshrine those principles?

According to the recent NSW Supreme Court case judgement in Kassam vs Hazzard, there is no Bill of Rights in Australia (or the 1688 Bill of Rights was not accepted by the court to be applicable

to Australia). Based on this alone there cannot be this level of intrusion into Australian's privacy and freedom with the Digital Identity bill and similar proposals, without there first being a Bill of Rights or Constitutional framework or legal acknowledgement of same, in order for Australians to have the reassurance that their rights are protected by something higher and with more authority than any passed legislation.

We have already seen a travesty of human rights with the overreach in passed legislation and delegated legislation and public health directions: officials were put on notice and did not refute the letter alleging crimes against humanity, breaches of human rights and other breaches of the law, some potentially criminal in nature: https://concernedlawyersnetwork.net/#Anchor1

The Digital ID proposal is an absolute abuse of an individual's freedom and right of ownership to one's own biometric information.

This bill does not include "non impediment to serve". This is of grave concern and surely is the beginnings of unjustified exclusions. It has the potential to be used and abused to create the likes of the social credit system of China.

Such a bill would open the door for the garnished information to be controlled, exploited and counterfeited by individuals, groups and government.

Centralised systems of collecting and recording mass information already has a disastrous history of error and ineffectiveness. Centralisation also adds an open doorway for this information to being hacked, exploited and used by criminals as stated above.

This bill also does not provide any option to opt out. This bill is not being openly and widely presented and debated. This means that the general public is not informed. To therefore presume, as this bill does, that if one does not oppose this Bill that they/we are giving our consent. This is trickery not "Trusted".

Such a bill would also be discriminatory against many groups in our society including the elderly, disabled, those who are not technically literate, Australian Aboriginal and Torres Strait islander peoples and those from non-English speaking backgrounds, leaving them unable to access routine government, social and commercial services.

What happens to those who are unable or ,by due right, choose not to consent to this digital identity? This bill has the potential to create an apartheid society, based on unjustified and amoral principles and actions. This is NOT the way forward.

It is more than evident that the relationship of trust between the people and the government, its bearers and associated offices and systems of management, has already been tragically and deplorably eroded. It would therefore certainly NOT serve the good of All to proceed with this Bill. It would in fact be deleterious and likely criminal.

We have been here before. The people have previously already and loudly rejected the notion an identity, 'Australian Card'.

In the words of Justice Michael Kirby, President of the New South Wales Court of Appeal, in evidence to the Joint Select Committee on an Australia Card, 1986

“If there is an identity card, then people in authority will want to put it to use…. What is at stake is nothing less than the nature of our society and the power and authority of the state over the individual”

While this scheme is supposed to be voluntary, I have no doubt that it will become mandatory in time.

No government is going to pass up the opportunity to gather the private information of every person they can. Those who do not engage with on line technology would be disadvantaged by this scheme. Electronic technologies are all well and good – until the power fails.

What use is a universal digital ID if there are no means to use it in an emergency, when the

humanitarian needs of individuals are urgent? It is already clear to thinking people that in natural disasters the electricity is one of the first services to fail.

Exclusion: Stringent ID requirements can generate non-trivial costs in terms of exclusion and inconvenience to genuine beneficiaries. Evidence from India shows that making biometrics compulsory in the public food distribution system created exclusion problems and increased transaction costs, especially for vulnerable groups, without reducing corruption. These findings were corroborated by a second study, which found that biometric IDS led to limited improvements, such as more timely and reliable recording of PDS transactions and resulted in the exclusion of households (usually the most vulnerable ones) that were unable to pass the biometric authentication test. The authors argue that the imposition of the digital system here led to “pain without gain” as it did not address the type of leakages that were prevalent in the given context.

Implementation concerns: Another study in India found that while a biometric attendance-monitoring intervention led to health improvements, its imperfect enforcement illustrated the limitation of technological monitoring solutions when they are not combined with changes in broader rules governing health workers. While there were some health gains from this, the biometric devices led to lower work satisfaction among staff and increased difficulty hiring new nurses, lab technicians and pharmacists. As a result of this and other factors, there was limited appetite at all levels of government to use the better quality attendance data to enforce the government’s human resource policies.

Privacy and data misuse concerns: Biometric authentication raises important privacy and data misuse concerns, especially regarding safety and misuse of collected data. Large data sets have been shown to have great power in surveillance, as well as predicting and shaping people’s decisions. In light of this it seems that broadening our Digital Identity capabilities in Australia may marginalise and potentially discriminate against certain groups and also create a sense of distrust in the public with the continuous sense of ‘monitoring of movement’ in a digital and physical

sense. We already seem to have sufficient access in Australia for essential services that people can elect to use online / digitally, the introduction of such a system would seem to create a pathway for all Australians of less choice and freedoms and potentially open the door to human rights issues and a dangerous level of power in the hands of government officials.

People such as the elderly, young, disabled etc will not cope with the imposition of this technology upon them. The digital identity will discriminate against the over 65 for they don't all have anything but cash and we should help them to feel safe and secure in there latter years of life. It will also discriminate against the people who can't afford a phone for themselves and their children, and against those who have an "off the grid" lifestyle which they are entitled to have and enjoy.

CYBER SECURITY THREAT TO THE INDIVIDUAL

I do not consent to my private & confidential information being centralised,

accessible & potentially misused by a third party. I would be in gross danger with my personal information is being hacked, leaked nor who has access to my personal & private information.

This is a high risk to cybersecurity with possible loss, theft or corruption of very sensitive information or misuse.

Misuse of an individual's personal data for the purpose of greater power of surveillance, and/or predicting and shaping of people's decisions for commercial exploitation are other obvious concerns. There is a lack of clarity regarding ownership rights over the unique personal information contained in our bodies.

This lack of clarity leads me to believe that Australian's biometric information could plausibly be used to covertly modify, control, counterfeit, or monitor our conscious agency of opinion regarding:

- personal information of accounts in healthcare
- banking,
- affiliations with and memberships of political and religious associations,
- sexual orientation,
- vaccination status,
- ethnic and racial origin
- possible criminal records

Examples/evidence:

When the immunization status of citizens in NSW was shared with Centrelink. It clearly does not comply with section 15 of the Privacy Act 1988.

When someone's information sent to another person via SMS stating they were due for their second vaccination is one example, easily copied and shared with anyone. It clearly does not comply with section 15 of the Privacy Act 1988.

The draft refers to information shared with any private entities "for any reason whatsoever" which is unacceptable and a clear breach of the principles of the Privacy Act 1988.

Below is a complete list compiled by Webber Insurance Services of

DATA BREACHES IN AUSTRALIA for 2018 - July 2021

https://www.webberinsurance.com.au/data-breaches-list

A persons Digital Identity, which by default is an extension of themselves, and collectively the Digital ID of the Australian population should be protected under Australian and International Law from potential Human Rights violations that may arise from misuse by governments and affiliated agencies/business

FRAUD THREAT TO THE INDIVIDUAL

I do not consent to my private & confidential information being centralised,

accessible & potentially misused by a third party which gives rise to more risks of identify theft.

I do not agree with the 'New Legislative Bill', being passed, named the 'Trusted Digital Identity Bill' (TDIS), for the following reasons.

- This may pose practical challenges around where the data is hosted and may even prevent some entities from being eligible to onboard on to the TDIS.
- The Bill (TDIS) also provides a statutory framework to limit liability as between accredited entities and participating relying parties but does not specifically address liability to end users.
- The Bill (TDIS) provides the Oversight Authority with the power to make service levels and technical standards relating to the TDIS. The service levels may be related to the availability and performance of the entity's accredited facility, while the technical standards may cover technical integration requirements for entities onboarding to the TDIS or technical or design features that an entity must have before it can onboard.

Among other things, these may relate to the format and description of how TDIS information is handled and how it is shared between entities on the TDIS.

- Every Australian citizen's identification converges into an application or government portal (like MY Gov) that can then be converged around the world on international unknown security level platforms. Australians necessary Government Agencies, already have access to multiple forms of both government and private sector issued personal identification systems (drivers licence, passports, bank records, Medicare, birth certificates).
- Privacy of every individual in Australia is sacrificed for security that is not yet fully established, standardised and/or authenticated, with this Bill (TDIS). Nor is it made clear to the unknown benefits and/or detriments to the Australian people's potential privacy breaches, both Nationally and/or Internationally.
- The act (TDIS Bill) extends to all territories, which abolishes state-centric identification, further centralising our personal information, and this includes our information being accessible by entities outside of Australia.
- The Bill (TDIS) gives power to government and/or other entities to access our social media and other online assets and the ability to reword anything to the contrary. These departments will have the ability to adjust and/or alter our profiles or uploads, which in turn could in certain scenarios, leave us liable and or open to criminal prosecution.
- With all the uncertainties facing Australia, this is certainly not the time to be putting such a Bill (TDIS) forward, nor is it ethical to continue to push such an uncertain synchronised technology standard/system, which could jeopardise the trusted and personal information of each and every Australian citizen.

Although the Bill or other similar digitised systems may have been initially dafted to protect the Australian population from fraudulent interference within the Digital Sector/Domains. However, this is certainly not the time for such a significant and mandated adjustment to be implemented within Australia.

USE OF THE DIGITAL ID AS A MEANS OF SURVEILLANCE UPON THE INDIVIDUAL AND THE POPULATION

I do not consent to my private & confidential information being centralised,

accessible & potentially misused by a third party. I resist to my movement being tracked, monitored & watched. I resist to my movement being tracked, monitored & watched.

I do not consent to any form of geo-location identifiers. I do not want my personal image stored anywhere by any unknown entity, agency etc. Again, if any person genuinely needs to see my image to verify my identity, ***I*** will provide it personally.

Digital information has already been misused by government departments and entities the government has allowed access to.

Examples/evidence:

Queensland Police and Victoria Police (and police from other states and territories) were able to access information from QR code data provided by Australians when it was not intended or approved for such purposes.

USE OF PRIVATE SENSITIVE DATA FOR OTHER REASONS OR ULTERIOR AGENDAS

Section 11.2: Why is "additional domestic and global research" being conducted?

Why does "global research" need to be done? If this is a purely Australian government initiative, there should be no need for "global" research or engagement. The implications of "global" use are concerning. Australians have not voted in any referendum for a One World Government or global data bank of its people.

I do not want to live in a society that is controlled by a digital technology & a digital identity that I have no control over. I do not consent to the potential for any form of social credit system I do not consent to the control, storage & management of my personal information, viz. birth certificate, marriage certificate, tax returns, bank accounts, assets, my social life, employment, medical history records & any biometrics & behavioural information. Such information is my property.

Government and other entities would have access to use the data to compile a list of their detractors or political objectors, making them a target for political persecution.

An individuals' identity for example, health information, payroll, property, banking – to name a few areas – can be compromised and therefore used against will for commercial gain. This infringement of privacy violates the very tenets of a liberal democracy and is at odds with who we are as a nation. Australia has always prided itself on being free and giving its citizens the right to choose. We are not like other non-democratic countries which infringe on the basic right to privacy.

A unique digital identity does not help the individual as it removes their privacy and risks personal information being compromised, resulting in loss – whether this be financial or societal e.g. discrimination.

The draft refers to information shared with any private entities "for any reason whatsoever" which would allow private companies to exploit data lists in relation to marketing selling persuasion, coercion or use of the information to the detriment or disadvantage of the individual.

The proposed bill allows for any Australian government to misuse information by using

facial recognition technology, not giving the individual the opportunity

to opt out, and the ability to silence political protestors.

The Australian Government is deviating from what it has been sworn to do (working for the men, women and children of Australia putting their best interests first) and are rather working towards what will serve a worldwide globalist agenda. The myGov accounts are a clear indication of this, where employers no longer give Group Certificates (Tax Payment Summaries) to employers, but employees have to down load them from the portal. Accountants for example can pick it up off my myGov account without their client's permission permission to access it.

https://hugepatriot.com/breaking-who-releases-tech-specs-and-blueprint-for-global-digital-id-and-vaccine-certification/ The WHO released a guide with tech specs and a blueprint for every government on Earth to collaborate on a massive global digital tracking and surveillance system. From the 'Overview': "The concept of Digital Documentation of COVID-19 Certificates (DDCC) is proposed as a mechanism by which a person's COVID-19-related health data can be digitally documented via an electronic certificate." Australians did not vote for this in any referendum or under any published Australian political party platform.

THE CONVENIENCE AND FISCAL REASONS FOR THE BILL ARE INSUFFICIENT TO WARRANT THE BILL BEING INTRODUCED

This Bill is being introduced to the public as a "convenience", presumably meaning that it is

"inconvenient" to have to supply certified copies of original documents to support any particular purpose requiring proof of identity.

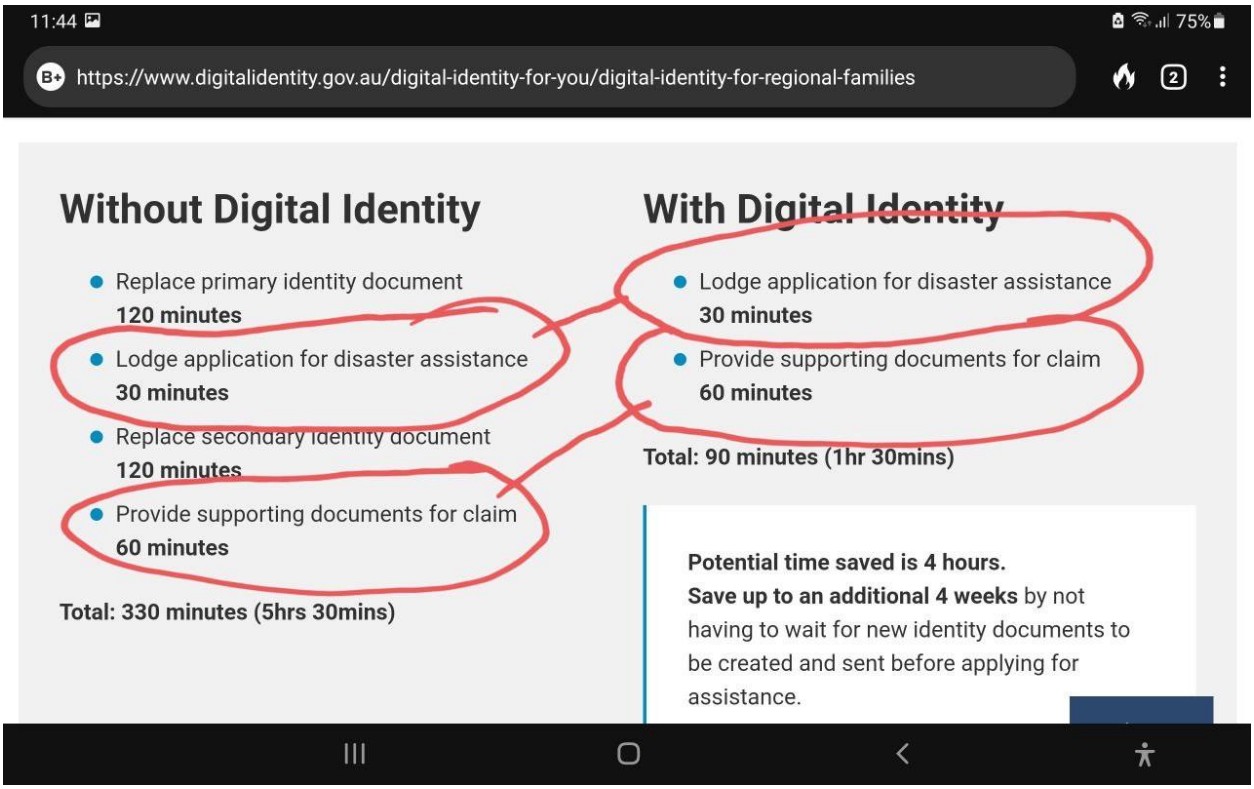
That very "inconvenience" is in itself a safeguard against identity fraud. I have possession and

control of my original documents, and only supply certified copies thereof to those entities that I choose.

The current system works well and is safe and trusted. There is no need to introduce a new digitised system which has such potential for harm to individuals and businesses.

The potential risk for great harm to the Australian people far outweighs any possible benefits.

There is no time saving involved: (see below):



The benefits of using digital ID to me as a citizen are negligible. I don't believe the trade-off between time saved (eg. the examples given on the website for rural families and buinesses) is worth the risk of potential abuse of massively centralised data. Even if that data used by different providers, commercial, bank, financial, health, retail, government etc, is ostensibly not linked, the use of single number can make it so with the flick of a switch and a few lines of code.

The inconvenience of preparing said documents is a small price to pay for our identity to remain safe.

The benefits of the bill flow in the main to the government, making it easier and cheaper to control and monitor citizens activities. The government did not seek nor receive an election mandate to develop the scheme of the Bill, and the supposed consultations described on the website have been only with groups with a vested interest in monitoring and controlling citizens, whereas the citizens have scarcely heard of the schemes proposed in the Bill.

Alternatives schemes must be fully discussed in the public eye. For example I quote here from Misha Ketchell writing in "The Conversation" January 28, 2020.

https://theconversation.com/australias-national-digital-id-is-here-but-the-governments-not-talking-about-it-130200

"For example, some localities in Canada and Switzerland, faced with similar challenges, chose an alternative to the federated model for their Digital ID systems. Instead, they used the principles of what is called Self Sovereign Identity (SSI).

Self-sovereign systems offer the same functions and capabilities as the DTA's federated system. And they do so without funnelling users through government-controlled Identity Providers.

Instead, self-sovereign systems let users create, manage and use multiple discrete digital identities. Each identity can be tailored to its function, with different attributes attached according to necessity.

Authentication systems like this offer control over the disclosure of personal information. This is a feature that may considerably enhance the privacy, security and usability of digital identification.

Based on the idea of giving control to users, self-sovereign digital identification puts its users ahead of any institution, organisation or state. Incorporating elements from the self-sovereign approach might make the Australian system more appealing by addressing public concerns."

It is anti-democratic and unconscionable for this Bill, whose core concept of a single digital ID has already been rejected by Australians at a referendum, to be introduced as legislation without an election mandate.

Justice Michael Kirby, [then) President of the New South Wales Court of Appeal, who observed in evidence to the Joint Select Committee on an Australia Card, 1986 stated:

"If there is an identity card, then people in authority will want to put it to use….What is at stake is nothing less than the nature of our society and the power and authority of the state over the individual". This Bill is again an attempt to assert unwarranted uses of state power over the everyday lives of citizens.

The bill must be rejected in total, and any alternative scheme must start with full transparency and consultation with the public.

Explanatory notes to the bill are not convincing

The two examples provided to support the passage of this Bill are both weak and dubious.

The first example refers to "Alex," the owner of a new business and how a Digital Identity will reduce costs and time associated with opening his new enterprise. A dollar figure as well as an estimate of the set-up time is provided to support the case. Unfortunately, "Alex" will soon realise that costs are never static; governments always raise fees and charges without redress and this will be no different despite this "new" platform; while ordinarily government departments make citizens wait, regardless of the area of concern. Consequently, that is not a reasonable case for

the affirmative. And in-so-far as the possibility of numbers of SMEs opening up in the next few months/years; in what world does Stuart Robert live? The Government's response to Covid-19 has seen thousands of small businesses forced to close and many will never open again. Given the heavy hand of government and the way that public servants have prospered under Covid-19 government restrictions, whereas private enterprise has been poleaxed, I would consider many people may think twice about any thought of opening a new business and opt instead for a public service job. So, "Alex" is actually a dinosaur in this new big government world.

The second example concerns a family residing on a farm who, because of a bushfire, lose key documents that can then be retrieved easily because of a Digital Identity. But what type of documents are causing father "Henry" such concern and requiring him to expedite their replacement? It seems the big deal is the loss of birth certificates and passports.

Regarding the "living in the country" stuff; what is the proportion of family farms today - are there reasonably enough to justify an entirely new online framework for every Australian to access government departments and services? The answer to that question is 'no.'

However, in reality the vast majority of Australians live in towns and cities and not on family farms. And while there is a case for universal service provisions wherever Australians may live, that argument relates directly to mobile phone coverage, which remains in some areas abysmal despite consecutive Australians governments promising to fix this problem. Were one to extrapolate "Henry's" predicament, along with the rest of his possessions "Henry" may have lost his laptop/computer in the fire thus necessitating a trip to town anyhow given that the service provided by Australia Post is nothing to crow about.

Not only are "Alex" and "Henry" members of what are now minority groups in this country, suggesting therefore a niche cohort of concerns, their "problems" are in fact only mid-range issues, which do not justify the requirement for the entire country to submit to a digital identity that could be used at some future time to control individuals or indeed the entire populace. As an example of the way good intentions can be misused, over the last twenty odd months of this pandemic every government in Australia has used a variety of force/punishment against Australians to ensure certain government mandated outcomes. People and communities have been materially injured by policies that we were informed were designed to "keep us safe," but which have resulted in the blanket removal of Australians' human rights - rights that were previously believed to be inherent to Australian citizenship. As a result, many Australians (the majority of Australians?) have lost trust in all levels of government to respect our rights. How, therefore, could we ever think that should a digital identity be foisted on us the government would deal fairly with each citizen when it has not during this pandemic?

Under the health orders currently operating because of Covid-19, look at what the NSW Government has done to force residents of the state to be vaccinated. While denial of the right

to work is possibly the most egregious, suddenly there are now two classes of citizens in that state

- the vaccinated and the unvaccinated - and though the NSW Government has advised that all restrictions on the unvaccinated will be removed from 1 December, every Australian state government, as well as the Commonwealth, has announced that unvaccinated individuals will be denied the right to cross state borders, simply because for whatever reason, they refuse to have a vaccination. If Australian citizens can be treated in such a shocking and undemocratic way and discriminated against under some type of "health segregation" what could occur to rights under a digital identity?

Risks outweigh any potential benefits

Currently, Australians do not need any new legislation to contact and utilise government services of the type described by the two scenarios above. So the government has not made a reasonable case that this new legislation is necessary or beneficial. But what has been shown by the detail of the Bill is that there are a number of inherent risks should the legislation pass the parliament. First, the government is compelling the citizen to engage in one way only with the government and to make available their data in one form or another, or perhaps completely, to private business interests, which must be salivating at gaining access to personal and private information on this scale. And what of the hacking risks from foreign interests both government and private? The hacking of information by rogue actors is well known with both public and private interests at material risk from this practice. Forcing Australians to have a digital identity will only increase the risk of third parties obtaining by surreptitious means our private information.

But third party access to private information is not the only or indeed the main concern from this Bill. Worrying, the Bill has no opt out provision - therefore everyone will be made to have a digital identity. And with a digital identity, the citizen is at risk of being "closed out" of their own data, or even their own personal resources, by the government. Imagine, for example, a civil fine situation - unpaid for whatever reason - that becomes a "black mark" that is "attached" to the citizen's digital identity with the result that it could be used negatively against the citizen; like the way a credit score of a borrower is used by a financial institution. While somewhat acceptable in the financial institution/client relationship scenario, this would be wholly unacceptable for how the relationship between the government and the citizen should operate. And what if the government determined that the infraction was more serious than that parking fine scenario - perhaps, since private business would be utilising the same platform, the government could decide to freeze the citizen's relationships with other institutions like, for example, their bank or their Facebook account. How would the citizen be able to restore to their possession their digital identity account? Given that we have already explored the circuitous processes inherent to government process, not well and not timely would that restoration occur. Suddenly, we're on

the cusp of something like the Chinese Social Credit System, which would be anathema in a western liberal democracy such as Australia.

Australia and Australians do not need a digital identity platform, if "Alex " and "Henry" are the best arguments the Government can provide to introduce this Bill. What instead we are seeing from this proposed legislation is a a clear example of dangerous government overreach. Consequently, the Trusted Digital Identity Bill needs to be withdrawn.

PRIVACY LAWS BREACH & NATIONAL SECURITY THREAT

The public have not been shown the privacy impact assessment statement (pia) if there is one at all, in relation to this proposed bill in accordance with law. Privacy rights are breached by this proposed bill as the individual no longer has privacy with a centralized digital id data base.

Private sectors do not and should not have any right to access our identity digitally as this could lead to discrimination against individuals and groups, as well as violation our privacy as individuals.

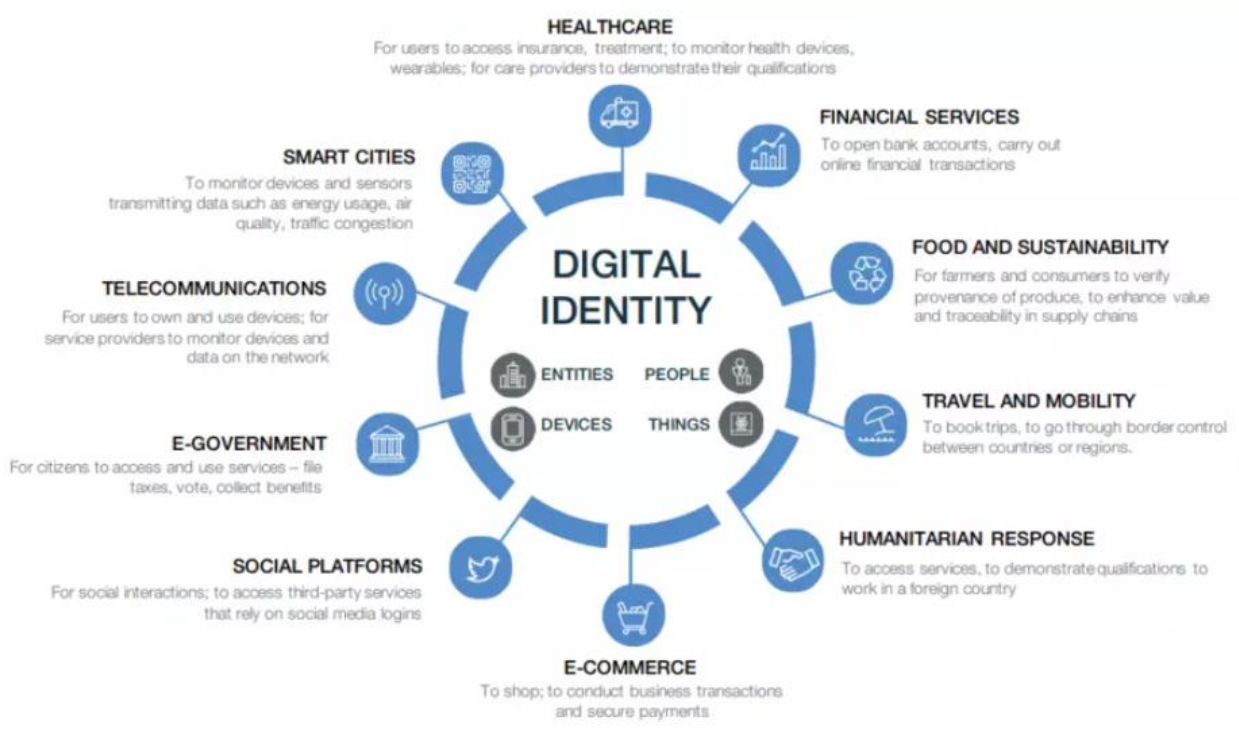
The digital certificates are in violation of private right of individual citizens

The hidden nature (during a pandemic) of the progress of this Bill should immediately raise alarm bells for all Australians. It is not appropriate for governments to engage 'third-parties' to manage sensitive medical and other personal records (records citizens often will only share with Gov under threat or coercion) including any foreign entities. Such a centralized mass of data creates a highly visible and highly-risky "honey pot" for subversive forces and puts our national security at risk.

There is too much tempting potential for Government or other parties to misuse this information (not just privacy breaches but also for political advantage) without oversight or accountability.

The real purpose is the enact the World Economic Forum (WEF) Great Reset, and the United Nations ID2020 who's agenda is to reshape the global economy, governments, consumption, AND every aspect of society. An integral part of that requires everyone on the planet to be linked with a digital identity.

The agenda and direction is of a global nature and Australian government leaders are following it including the digital identity aspects as per below diagram summarizing WEF objectives.



Control

The WEF envisions our digital identity being connecting our every online/offline interaction such as:

- Search history
- Social media interactions
- Online profiles
- Device location
- Medical records
- Financial ledgers
- Legal documents
- Every click, comment, and share you make on social media
- Every financial transaction you record
- Your location and where you travel
- What you buy and sell
- Your personal health data and medical records

- The websites that you visit
- Your participation in civic functions (i.e. voting, taxes, benefits, etc.)
- How much energy you consume

With the proposed Internet of Bodies, not only would your every societal behavior be recorded, but also everything you did in private.

Thus, our digital identity becomes an account of our social behavior, which can be policed.

If you had a digital identity like the WEF proposes, the authorities would know the moment I broke a curfew, went somewhere they told me not to, opened my business after they said to shut it down, or let my mask slip down when told to keep it up.

That system is intended to be used to eventually enslave populations, eradicate people's privacy, liberty, rights, freedoms, behaviors, and permissions. It will gradually become a dictatorship and totalitarian system that will control every aspect of a persons' life and will impose tyranny upon those who do not comply.

An example from history

Under Pol Pot, the state controlled all aspects of a person's life. Money, private property, jewelry, gambling, most reading material and religion were outlawed; agriculture was collectivized; children were taken from their homes and forced into the services; and strict rules governing sexual relations, vocabulary and clothing were laid down.

A system like this will eventually lead to the erosion of privacy because of the ultimate purpose required behind it

Build back better?

Pol Pot announced the implementation of a new calendar, the first year of which was designated "Year Zero," an idea he lifted from the French Revolution and its Reign of Terror. Literally, he reset the entire timeline of the country at the ascension of the new order and new system of government. This furthered the idea that all previous history, culture, and societal institutions were to be completely obliterated and rebuilt from the ground up.

Doesn't this remind you of the Great Reset slogan "Build Back Better"?

The chief aim of Pol Pot was total control in order to wipe the slate clean, start over, and achieve their false utopia. This is the same promise of the UN & WEF of starting over by 'building back better' and this ID system will eventually be used for the same aim of control.

Social credit system

This is the beginning of a system that will install a a social credit system that will eliminate privacy, influence behavior, record and control every aspect of a person's life. A record of everyone's

behavior and activity will recorded on their digital identity which will socially engineer new classes of people.

A digital ‘health record’ will eventually determine what products, services and information we can access. Good ‘health’ according to their set rules will allow access, but conversely ‘bad health’ will exclude access.

Purging

Pol Pot declared, "This is Year Zero," and that society was about to be "purified." In his revolution Capitalism, Western culture, city life, religion, and all foreign influences were to be extinguished in favor of an extreme form of Communism. A Khmer Rouge slogan proclaimed "What is rotten must be removed" and as a result throughout Cambodia, deadly purges were conducted to eliminate remnants of the "old society".

Most people had no choice but to beg for food and shelter whilst millions of others were murdered.

This digital identity will eventually determine what products, services and information we can access – but also what is closed off to us. Step out of line, and every social media interaction in which I partake, every dollar is use, and every move I make — can be used against me.

In their zeal to root out unworthy New People, Khmer Rouge targeted a number of people groups in Cambodian society. All Cambodian citizens were reclassified and as a result many were vilified or targeted for murder. Upon seizing power, Khmer Rouge began a campaign to identify enemies and determine whether they were more suited to "re-education" or extermination.

Pol Pot required:

- Total obedience to the regime,
- Identify those suspected of being enemies of the regime
- Eliminate the enemies of the new regime

In days to come the ID will eventually enable governments and elites to target and eliminate individuals and groups by locking them out of medical, employment, banking, investing, shopping, and starving them to death.

It is inevitable that the controlling digital ID will carry similar aims and lead to a purging of unwanted people. (We know that because it's already happening with the vax-free people) Is this what the Aust is ultimately allowing?

Fourth Industrial Revolution

This system will also become integrated into the WEF vision of the 'Fourth Industrial Revolution' that creates a fusion of our physical, our digital, and our biological identities, and can therefore be controlled biologically. The 'internet of bodies' and most others will have implanted biosensors and tracking to enable 24/7 surveillance

Sensors that detect when you go to the toilet, where you sleep, your temperature, and even how fertile you are, will all be connected to the internet within the Internet of bodies ecosystem.

Abuse of opt in digital id requirement example

Look at the biometric ID system, India's Aadhaar program.

But critics said that the scheme, while supposedly voluntary, had imposed itself increasingly onto citizens' private lives. It became near impossible in India to buy a cellphone contract or open a bank account, for example, without providing an Aadhaar number.

This is now becoming linked to fingerprints and iris (eye) scans.

All above is in breach of Human Rights

The Siracusa Principles and the International Bill of Rights, of which Australia is a participant protect our privacy and human rights.

The Human Rights Commissioner has been exploring the human rights implications of new technologies and AI and the need for strengthening of human rights.
https://www.corrs.com.au/insights/international-human-rights-law-and-the-covid-19-response

> These human rights concerns are real. In Australia, the Human Rights Commissioner has been exploring the human rights implications of new technologies and artificial intelligence. A draft consultation paper proposes limitations to the use of some technologies in certain circumstances, including recommending a 'legal moratorium on the use of facial recognition technology in decision making that has a legal, or similarly significant, effect for individuals, until an appropriate framework has been put in place'. [3] It is intended that the framework should include robust protections for human rights.

THE PROPOSED BILL BRINGS IN THE POTENTIAL FOR ELECTION FRAUD AND/OR A TOTALITARIAN GOVERNMENT

There is no guarantee that the Digital ID proposed will be then mandated for use for voting. Voting electronically is fraught with issues of fraud. Court cases in the USA have shown that the

Dominion system was used to manipulate and change votes even after manual voting. If voters were later compelled to vote with their Digital ID it would not guarantee secure voting.

Without the below protections solidified in legislature, the Trusted Digital Identity Bill appears Totalitarian in nature disguised as convenience for the end user.

Ultimate ownership and control of an individual's Digital Identification (including restricted attributes, attributes, personal information, biometric data, etc.) must exclusively belong to the individual person the Digital ID was created for- the individual/human/person - The end user.

The end user needs to be protected from potential Human Rights violations by:

- Corrupt Governments (national and international)
- Ministers and the Oversight Authority with excessive, unchecked & unbalanced power
- Accredited entities, companies and private sector participants

collecting, storing, and utilising Digital Identification to the detriment of the end user.

Correction of loophole in Australian legislation and law impacting the privacy and rights of every Australian with a Digital ID in the TDI system - International governments/companies/agencies not breaching an Australian Privacy Principal (6A of Privacy Act 1988) if the act is done, or engaged in, outside Australia and the act or practice is required by an applicable law of a foreign country.

Provisions in legislature for the protection of the end user (owner if the Digital ID) from inevitable security breaches magnified to disastrous consequences considering the volume of personal and restricted data (Digital Identity information) being held, stored, handled, and transferred between TDI network, government agencies and accredited entities both national and international.

The draft Trusted Digital Identity Bill 2021 is very detailed in outlining the authority and power of The Oversight Authority and Minister as well as protecting themselves from civil action. The end user – the person/individual/human who the Digital ID is derived from and belongs to needs to be recognised in legislation as the ultimate owner of their Digital ID and the protection of Human Rights needs to be at the core of every law relating to Digital Identification.

The Oversight Authority, Government Ministers (Australian and International) and other organisations have the power to misuse information derived from a person's Digital Identification to potentially profile individuals in a way that would violate their human rights.

THE PROPOSED BILL IS JUST ANOTHER AUSTRALIA ID CARD THAT WAS PREVIOUSLY REJECTED BY AUSTRLIANS WHO WERE HOSTILE TO IT

See arguments here and history to be included in this submission:
https://privacy.org.au/about/history/davies0402/

This paper describes circumstances where the public have reacted with hostility to proposals for a national ID card system, focusing in particular the successful campaign against the Australian government's Australia Card. The findings of this paper are particularly relevant because, at the time of writing the United Kingdom and Canada are debating such systems.

See below links which explains why the national ID card proposal was abandoned in 1980's. Every aspect of our privacy is under attack.

https://privacy.org.au/about/history/davies0402/

https://www.aclu.org/other/5-problems-national-id-cards

INSUFFICIENT PUBLICATION OF INTENTION TO INTRODUCE BILL, INSUFFICIENT CONSULTATION WITH THE PUBLIC AND RELEVANT ORGANISATIONS AND INSUFFICIENT TIME PROVIDED TO THE PUBLIC TO RESPOND AND PROVIDE SUBMISSIONS (TRUST ERODED)

There has been a very disturbing lack of publicity and genuine and widespread public consultation around this Bill and the proposed changes it encompasses. That it has reached this third stage without so much as a mention in the main -stream media indicates a sleight of hand by government that raises serious suspicion about the government's intentions.

This whole community consultation process has been limited to the community the Government wanted to get feedback from. There was no clear advertising in the media or social media that this process had been started and it is only in the 11th hour that we came to know that we are already in Phase 3 of the process and it's the last phase where community can contribute.

The writer had only 3 hours to consolidate her own submissions together with others for Concerned Lawyers Network prior to submitting. Three months would have been more appropriate. However it did not come to our attention but for a random Telegram message, the knowledge of opportunity to make submissions about this Bill.

Although this legislation has been 5 years in the planning, there has been virtually no public debate on the topic. The consultation process has been with big business and organisations who may have a vested interest in the area. This is not always in the best interests of the individual.

The lack of transparency in the development of this legislation is highlighted by the lack of consultation with the community.

People can only be involved through open promotion and exposure of the proposed legislation from the beginning of the process. There has been no concerted effort to involve the average person in this way and yet it is the average person who will be most directly affected by this legislation.

The Government's own Fact Sheet from the website outlines only one side of the issue with no recognition or acknowledgement of any negative impacts. Nothing more than a marketing document, it assumes the legislation will be passed and that there will be total compliance. It is full of generalised statements of benefits with no details outlined that would allow identification of potential gaps or concerns.

Broadly speaking, the general community is completely unaware of this wide ranging and complex legislation and Government silence on this matter only serves to further undermine public trust in both business and government's handling of personal information.

Trust eroded

Trust between the people of Australia and the Australian government has eroded to an all time low after breaking promises about vaccinations being completely voluntary. Thus it follows that such a rapid introduction to a digital identification system that is centralized is not trusted in any manner.

These are typical responses quoted from public subscribers of the Concerned Lawyers Network:

The response of Australian governments to Covid19 has lead me to no longer place any trust in our governments and especially when it comes to the collation and storage of data. As a previously free Australian citizen I object to the digitisation of our identities and to the risk I believe that exposes us to. This type of bill should be widely, openly and very publicly debated but it was almost by chance that I even heard of it. I would like to remind the parliament that Australians have previously voted against an Identity Card and I believe if they were again given an opportunity to choose would again vote against this bill.

Legislation like this with such massive potential future impact should always be strongly debated in as many forums as possible and it is difficult to shake the feeling that government is hoping to slide this past us 'punters' and present it as a fait accompli. At absolute minimum we must given given an option to opt out.

Digital identity leads to a widening access and use of private information and medical records. Possibility of breach of privacy whether accidental or criminal is a concern for many. Even though your information states it is secure the current situation and government dealings,

censorship and misinformation surrounding the "pandemic" has left many sceptical and untrusting of the current main government parties.

The government has not fostered enough public awareness and discussion. The media have also been very silent on the content, purposes safeguards, risks, and regulation impacts of the Bill.

My personal information will not be adequately safeguarded in the Bill.

Even if the government of the day is scrupulous and does not abuse the infromation, there is no safeguard that such a large trove of personal infromation held by government will not be linked, manipulated and abused in future.

Existing methods of identification are adequate for my security. I believe the safety of my ID is made more secure, not less, by requiring several unlinked documents, for example 100 points ID to open a bank account.

I do not believe or trust the government when it says the use of digital ID will be voluntary. The government burnt its claims to be worthy of trust by the coercive handling of covid vaccinations and travel and movement restrictions based around those. On a similar note, the Bill unavoidably contains many subjectiove tersm which can be interpreted at will should it suit the government of the day or its bureaucrats... for example "adverse or qualified security assessment" can be used to justify anything from petty repressions (arresting mothers in pyjamas in their own kitchen for making facebook posts for example), to full blown persecution and silencing of political opponents.

I have strong objections to commerce and business (non-government) goods and service providers using and collating information about a single ID number that is linked to my personal details. This doesn't serve any legitimate purpose. It will facilitate unwarranted intrusion by governments into personal freedom to buy and sell and travel. In short it establishes a mechanism for full control over every citizens rights freedom and privacy, even if such a mechanism is kept dormant in the short term. It also establishes a huge potential financial incentive for dishonest illegal gathering and sale of number-linked information.

I am 100% against this legislation. This is simply the first step towards a social credit system. If this is passed as it stands, it will only be months before Australians' every move is surveilled and controlled.

We will need our digital identity to pay our utility bills, get funds from our financial institution, buy petrol, shop, etc. We will not be permitted to participate in society if we don't show our digital identity. I do not trust the government, financial institutions and other organisations with this technology. All our information will be stored on it including government info, financial info, social media, the list goes on. This is all about mass surveillance of the Australian population and I will not sit idly by and let it happen!

This is not communist China but all Aussies could be forgiven for being confused about that right now because as each day goes by the resemblance becomes stronger and stronger. Australians deserve better. We deserve to have our God-given freedoms returned to us. Removing them, however temporarily, is not the remit of any elected government.

As Australian citizens we have the right to live free and make decisions that affect us as individuals - void of excessive government intervention. We are entitled to privacy and regardless of whether something is sold as 'convenient', it can easily (and unexpectedly) be turned against us. Should the collated information be intercepted, hacked or illegally disseminated, the data-set can easily be used by organisations (either foreign or domestic) to undermine the rights we currently enjoy as citizens of this great nation. As such, we would be better served to keep this information on a 'need to know' basis. Although this may seem 'old-fashioned' and not entirely 'convenient', at least the individual can control where, when and how their data is shared and therefore better positioned to determine their own future.

I consider this information of such a sensitive nature that no amount of security would be sufficient to protect it. I do not conceive any form of encryption or cyber-security as being trust-worthy enough to enshrine this valuable and potentially highly dangerous database.

To whom it may concern,

I completely oppose any part of this bill and do not agree nor approve with the Digital Identity Bill or any of the associated Bills or Laws.

I do not give authority or trust to any government or its department, private enterprise or other entity to collate and create my digital identity and securely retain/keep the data.

The Digital Identity Bill and any associated Laws or Bills is a major breech of privacy and has the potential to discriminate and is not necessary.

This Bill Must Be Scrapped.

RE: (Un)trusted Digital Identity Bill

If the purpose of this Bill, were singularly to assist my fellow Australians in their interaction with the government, in order to facilitate service delivery, then maybe I could support it.

However, I given the despotic and tyrannical behaviour of the political elite class, I am led to believe that our government, its officials and politicians are comprehensively untrustworthy.

The behaviour of your government proves beyond doubt that you are not guardians of our democracy, nor do you give a shit about our divinely conferred human rights, granted by virtue of each person on planet being the imago dei.

Your support mandatory vaccination in order to work, was a monstrous betrayal of trust. You have committed an unconscionable crime against the citizens of this nation. You don't deserve our trust, nor will you receive it.

Your Digital Identification Bill is just another weapon which you can use to harm, harass and hurt those who elected you and for whom you no longer care. It's imponderable the tyranny that you could unleash on us if you proceed with this Bill.

Therefore, I am vehemently opposed to your Globalist agenda to store our data, which will later be used against us.

I demand that you don't proceed with this insanity.

I am against the implementation and passing into law of the proposed Digital Identity Legislation.

Statements in this proposed legislation indicate that Digital Identity is optional by choice, with the freedom to terminate the account at any time. However, there is cause for concern when any larger Government organisation or entity which has already acted with severe overreach on its citizens and residents, when it comes to human rights and privacy, particularly in the management of COVID–19, wishes to further install a system for tracking and monitoring. Transparency and accountability in our leaders have been severely lacking throughout 2020, 2021 and the peoples trust in their roles have become depleted. Furthermore, the mishandling and incompetence of the Government throughout this time period concerning COVID-19 instils lack of faith.

Personal identity is just that. Personal.

With ever-growing numbers of online identity theft and fraud, I remain unconvinced that this legislation will protect and indemnify the citizens and residents of the country it purports to protect.

This corrupt government spends billions on advertising their experimental, unsafe vaccines but very little of our money on informing us of this devious digital identity legislation! What are my major objections to the digital identity bill? Loss of privacy! Human rights eroded! Increased government control!

This plan was actioned in 2016/2017 by the WHO.

It involves all state premiers in Australia being told that the Public Health Dept will be planning to vaccinate 95% of the Australian population, gather up all our DNA and hook us all up to a Biometric Digital ID Pass System. With all that personal data to be handed over to the WHO.

It was signed off in 2018. Its set for completion in 2023.

Which means none of us will be allowed out of our homes until every single one of us has been poisoned. It's part of the IHR agreement that was signed in 2005 that activated the "pan-corona" measures. The IHR is a Public Private Partnership deal with 196 nations that agrees to ensure that International Trade and Commerce traffic is not disrupted during a WHO declared emergency.

This is why we are locked in our homes. Its to keep us out of Mr Globalists way.

Its looks like the IHR has been hijacked and corrupted by the Globalists and is why we are being driven into the ground by unlawful activity and stealth. It's being used as a WMD using a pen.

All the people need to demand the PM ScoMo immediately withdraw from the IHR agreement and corona will cease to exist for Australia.

The Corona pandemic was declared to facilitate the nations to implement their NAPHS plan – ("National Action Plan for Health Security"), that's all. There is no real pandemic. It is simple treason.

https://www1.health.gov.au/internet/main/publishing.nsf/Content/054D7F36DA7F8F72CA2581A8001278EB/$File/Aust-Nat-Action-Plan-Health-Security-2019-2023.pdf?fbclid=IwAR35fmoOPwa2Mky_7jQ_K-H9j66-dWfAOWltsTsUnV373SfmmO5SYnrVYwY

It violates the rights of all citizens of Australia to have a free and uncoerced existence. We are not criminals, and we don't deserve to be treated as such. We don't need to be under constant surveillance of the Australian government: it is undemocratic and against the will of all people who value their basic freedoms.

By passing this Digital Identity Bill 2021, the Australian government officially admits it is no longer a democracy but a totalitarian regime.

I categorically say NO to a Digital Identity Bill, and I represent everyone who wishes to continue to lead a free life on the Australian land.

After reading the Digital Identity information provided on the government website, I notice the expectation is that Digital Identification will be expanded to the whole economy in the future.

As Biometrics will be utilised as part of the security network and given the current state mandates, I fear that controlling bodies in the future ie, Governments etc, may use this as a process to deny citizens from accessing everyday services

and/or retail as they see fit. Our nations freedom and trust must not be broken and privacy should be of the utmost importance so I strongly disagree with Digital Identity.

If it is to proceed then Legislation must not be altered or changed unless a Public Referendum is guaranteed.

I do not approve of this Legislation. In an ever increasingly digital world, the government should be working to give people more control - not less as this legislation does.

From an individual's perspective, there is nothing in this Exposure Draft that demonstrates how the government is working to safeguard individuals in this space. The document is wholly focussed on the structure of a centralised Digital Identity System to the exclusion of the rights and protections of the individual.

If such a Bill that affects the rights and movements and surveillance of a person, the Government is under a duty to prepare a transparent communication that gets distributed on all forms of media and social media what their intentions are with this digital identity. What their intentions are for the future with all uses of digital id must be stated to the public.

OBJECTIONS TO THE DRAFT BILL

Personal rights and Protections including Freedom of Choice

The majority of the document deals with the setup and management of the Identity system. As important as this may be, the sheer lack of focus on individuals within this draft is a clear indicator of the neglect of their personal rights and protections under this legislation.

As such a system becomes ubiquitous, it becomes more and more difficult for individuals to opt in or out as desired and hence it becomes "mandatory by stealth". Yet no acknowledgement of these issues nor appropriate safeguards via alternative channels are identified. This risks social and economic discrimination for all and would be particularly profound for vulnerable sectors of the community. Simple and accessible alternatives need to be embedded and legislation must expressly preclude any form of mandatory involvement.

Chapter 2, The Trusted Digital Identity System Part 2, Division 4 Other Matters Relating to the TDIS, Section 30 states "*Generating and using a digital identity is voluntary*". However, subsections 2 – 8 proceed to explain how and when this does not apply. It can, in fact, be effectively rescinded by other government legislation.

Chapter 4, Privacy outlines obligations of entities and additional privacy safeguards within the system but this seems more like "lip service" to the concept of privacy and safeguards for the individual since, at no point, does the document focus on any individual rights or recourse to action, when, *not if*, the entities do not comply. Additionally, measures to mitigate the impact on vulnerable sectors of our society are completely non-existent.

Centralisation of Digital Identity

Centrally consolidated information managed by others including, but not exclusive to, highly sensitive data such as biometrics, brings profound risks for individuals. Individuals rightly have concerns about accessibility, the use of biometrics, and a lack of legal rights. Nowhere in the documentation is the protection of individuals rights, or even their ability to choose whether or not to participate, enshrined or addressed appropriately.

Personal Control over Information

Individuals should be allowed to control their own identity. Even if "Informed Consent" is embedded, the concept is useless if there is no alternative to the centralised collection, storage and use of personal information managed by others.

Undeniable security rules ensuring that individuals can self-manage their personal information with all the rights that go with that by way of full control over participation in such a system should be the bare minimum standard. Safeguards should be expressly defined and be embedded in this primary legislation.

Chapter 1: (3) Objects

- The act will NOT provide individuals with simple and convenient methods for verifying their identity in online transactions as it not just a simple 'system' that is being imposed. It is a complex system that encapsulates all elements of our lives in one place. If you do not consent of 'voluntarily' participate in 'the system' you will essentially be outcast and discriminated against.
- It will NOT promote economic advancement by building trust in digital identity services as it is doing the opposite.
- It will NOT facilitate economic benefits for, and reduce burdens on, the Australian economy as it is not a burden to continue using the methods already established i.e., Credit cards and cash. These methods have been used for decades, how is this a burden to the Australian economy?

- It will NOT enable innovative digital sectors of the Australian Economy to flourish as it will give rise to identity theft and fraud which pose as even higher risks on the individual, organisations and businesses.
- It is stated that the objects are to be established via reliable and 'voluntary means', there is no indication on the boundaries of this. As we have witnessed with the COVID-19 vaccinations, coercion was undertaken to enforce the vaccinations else livelihoods were lost. People did not voluntarily give consent to be administered a trial vaccination, they were forced to in order to be able to work, provide and survive. They have families and children to feed, yet no one seems to be addressing this term 'Voluntary'. To uphold the definition of the term, Voluntary means there will be no segregation nor discrimination on those that choose not to participate. Their rights and ability to interact with society should not be affected nor restricted in any way as they have the same rights as those who choose to use the system. I It will only cause a repeat of what we are already seeing in society. The Australian people have gone through enough pain, anguish and bullying.
- The privacy and ethical ramifications behind this Bill will be costly to all those involved.

Other chapters:

The 'interpretation' under the 'personal information' (a) on page 9 of the draft, what is being referred to by 'opinion'? Is this in reference to an opinion made about an individual using 'the system' by someone else within an organisation?

Including attributes of the individual, if they are alive or dead, restricted attributes and biometric information of an individual? In all instances of this mentioned, they all violate the basic principals of privacy. Why would any retailer or organisation need information so specific? It is an invasion of privacy on all levels to ask any individual for these and so unresponsible to list them like it is free information everyone would want to share.

Page 12 of the document continues to address the (c) information or an opinion about the individuals, racial or ethnic origin, political opinions, membership of political associations, religious beliefs, philosophical beliefs or affiliations, memberships, sexual orientation or practices, and criminal records. WHY WOULD ANY OF THIS INFORMATION NEED TO BE COLLECTED TO MAKE SIMPLE PURCHASES!

Further along the next paragraph it is stated that restricted attributes such as health information about the individual, an identifier of the individual that has been issued or assigned by or on behalf of; commonwealth or an authority or agency of the commonwealth, a state or territory can be collected and input into the digital registration listed as a restricted attribute of an individual. Now this is directly aligning with vaccination status and trying to collect information from the individual that's linked to Medicare or MyGOV. It is not hard to see what this bill is trying to encompass and direct society to. I OBJECT TO THE BILL as this will cause discrimination and segregation within our communities. Adding in the TFN as an identifier also suggests the plan to

link this within the workplace. I OBJECT TO THE BILL as this is all personal information and taking things too far!

Further on page 13, Fit and proper considerations are mentioned and state, 'in having regard to whether an entity is a fit and proper person for the purposes of this Act'. Again, does this mean you will be excluding those who do not wish to participate in the 'system' which in turn proposes that you will be banishing them from being an active member in society if they do not conform and provide all the information required, based all around their 'medical status' aka being vaccinated or not.

On page 36, 'holding digital identity information outside Australia', why would anyone overseas need to access this kind of information? If it is meant to be so positive and help Australia's economy, then why is it being branched out overseas? This seems to raise alarm bells and suggests that there is another hidden agenda riding on this bill.

The use of the term 'civil penalty units' and suggesting there will be punishment for both the individual and business (on page 46) continues to raise more flags as this is not merely just a Bill that captures personal identity and information to drive the Australian economy, but it is suggesting a civil social credit system by which individuals and businesses will be credited and uncredited in order to control their interactions and behaviour. This then suggests that there will be a credit ranking system in place that removes certain privileges. I OBJECT TO THE BILL AS WE ARE NOT A COMMUNIST COUNTRY! WE LIVE IN DEMONCRACY AND THIS BILL VIOLATES THIS TO THE CORE!

Additional concerns that the draft bill does not address properly:

5.1 **Providing Legislative Authority for Expansion.** Rather ambiguous – expansion into what? We already have our details in the MyGov system for medical, Centrelink and tax purposes. Most Australians' health records are available to governments as well, along with their banking details. How much more of our lives does the government need to control? I do not believe it is necessary to expand the government's control further

5.2 **Strengthening Privacy and Consumer Protections.** This sounds like government-speak to do just the opposite. Tell me how you are protecting my privacy by taking it? Data breaches are a regular occurrence as no system is 100% secure. I do not trust government, or any other system, which promises absolute protection. It has never been possible and I doubt it ever will be. People need to have multi-layered protection themselves. That is the responsible and democratic way.

5.3 **Establishing Governance Arrangements.** This is a statement that assumes you already have the Digital ID in place. No government or third-party entities can guarantee absolute privacy. Additionally, no government has a right to my life or my privacy.

7.3 **Two Voluntary Schemes.** Will this be voluntary the way that COVID vaccination is voluntary? In other words you comply or miss out? That is called coercion. This is a move towards totalitarianism – I am not convinced this will be voluntary for long. I do not believe any scheme that involves putting all of a person's private data in one place, or controlling it via one entity or third-party, is safe. I do not believe that governments need to know everything about a person. That is not their role. They are to govern, serve and protect – full stop. This proposal is beyond protection – it is enslavement.

I firmly believe this type of ''digital identity'' in the government's hands – any government – is not necessary, nor do I believe it will be used appropriately – not now and not in the future. Only a fool could believe that. I think the writing is on the wall if you introduce this type of ID.

I absolutely reject that any government needs this much power over - and information about - the good people it is supposed to serve. No amount of convenience or cost savings is worth a person's freedom – of choice, of conscience, to assemble, to speak. This will be the end of a free Australia.

No matter how virtuous you may think this is on paper, in reality it will be quite the opposite.

Concerns previously highlighted by Digital Rights Watch in their Phase 2 submission:

- Digital Rights Watch (https://digitalrightswatch.org.au/wp-content/uploads/2021/07/Submission_-DTA-Digital-Identity-Legislation-Position-Paper-July-2021.pdf) in their submission to the Stage 2 Consultation highlights a range of issues, including but not limited to:
  - Case studies of digital infrastructure systems intended to improve service accessibility and quality of life which failed in their objective and ultimately led to discrimination of marginalised groups and increased social controls (https://www.accessnow.org/supreme-court-of-india-rules-to-restrict-worlds-largest-digital-identity-framework-aadhaar-but-debate-continues/; https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=25156)
  - Lack of public distrust in government services, as evidenced by the opt-out rate of the My Health Record scheme
  - Australia's insufficient cybersecurity capacity to provide adequate protections
  - Privacy risks including identity theft and fraud, data security and breaches, and digital services, including social media sites
  - Among their recommendations for Phase 3 are:

- *Prioritise an update to the Privacy Act and the precedent it may set for privacy. Given the topical overlap and potential for new privacy reforms to fundamentally change the way data protection and ownership is viewed in Australian legislation, it should remain a priority to anticipate an updated Privacy Act before proceeding with any other fundamental changes to the way that personal data of Australians is treated.*
- *Do not integrate biometric data into the Trusted Digital Identity Framework in order to minimise risks to the individual and reduce the cybersecurity threat to the infrastructure.*
- *Ensure that the digital identity framework remains truly voluntary. Individuals should have a choice to opt into the scheme whether they are interacting with government services or private entities. All accredited private participants must accommodate alternative ways to interact with individuals who do not wish to use the scheme.*
- *Maintain analogue pathways for individuals to interact with, and use, services. There are many valid reasons due to which individuals may be unable to interact with the digital identity framework. Connectivity and network affordability may be one, digital literacy another. No services should be denied to them because of that.*
- *Ensure that there are easy ways to alter consent, and delete or alter data. Consent can be a complex issue, especially when individuals have no ability to choose between services or meaningfully opt out. The digital identity framework must allow for consent to be withdrawn (data to be deleted on the TDIF or accredited partner side), and simple pathways to delete or alter data if the individual wishes to do so.*
- *Prohibit use of digital identity data for enforcement purposes. Law enforcement agencies should be explicitly prohibited from accessing the data in the TDIF or identity data held by the accredited partners.*

<u>The system is unnecessary, creates potential for abuse of power and becomes a potential hacking target for sensitive information</u>

The Regulatory Impact Statement (RIS) captures the significant community concerns with providing personal information including biometric information to a government agency.

"A majority (66%) of Australians were found to be reluctant to provide biometric information to a business, organisation or government agency (source: Office of the Australian Information Commissioner 2020, Australian Community Attitudes to Privacy Survey 2020). This wariness is not limited to potential commercialisation of personal data. OAIC's survey also found that only

36% of Australians are comfortable with their personal information being shared between government entities, and only 13% are comfortable with businesses sharing their information with other organisations (source: Office of the Australian Information Commissioner 2020, Australian Community Attitudes to Privacy Survey 2020)

...In this context, Australia's growing concern with privacy and the security of personal data could significantly impact the uptake of Digital Identity, which requires sharing of personal data, including biometrics. (Internal DTA Program research has validated the high priority that individuals place on

1. *Reassurance that their information is safe and secure, and*
2. *Proactive security monitoring.)*

If the System is to retain public trust whilst it expands across the economy, enabling the realisation of whole-of-economy benefits, public concerns over data privacy and security need to be decisively and permanently addressed".

The stated benefits in the RIS for individuals are:

- *improved speed of interaction with a wider range of Australian Government, state, territory and local government entities, as well as private sector businesses*
- *greater choice and flexibility in interactions with identity providers, appealing to individuals 'varying preferences*
- *reduced risk of information or data loss and identity fraud, encouraging greater confidence in Digital Identity*
- *strong levels of autonomy and control compared with other emerging 'de facto' identity solutions which are increasingly used to transact with private companies online.*

The World Economic Forum publication *A Blueprint for Digital Identity* (https://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf) suggests that the benefits of such a system would accrue primarily toward institutions (financial, government, and regulators), identity providers and "Relying parties" (entities that accept attestations from identity providers about user identity to allow users to access their services) (from p.75 onward). While the benefits for the individual are stated as privacy and control, security, convenience and transparency, however this document suggests that institutions, identity providers and relying parties would benefit most from such a system.

Digital rights are human rights (https://digitalfreedomfund.org/digital-rights-are-human-rights/). Such a system centralising vital personal information poses significant risks to personal freedoms; mores in Australia than internationally, as there is no Bill of Rights in Australia.

COVID-19 contact tracing apps were developed in contravention to the *Privacy Act 1988*, and have neither provided assurances or evidence that the information would be used only for the purposes for which it was collection (for contract tracing associated with COVID-19 cases). One such example was a breach of the data by WA police (https://www.9news.com.au/national/wa-police-stand-by-decision-to-use-safewa-contact-tracing-app-in-nick-martin-murder-investigation/9250eb64-b523-46ea-810d-bf09521f1e1f). However noble the reasons (this instance cites collection of evidence for a murder case), who becomes the arbiter of what is an "exceptional circumstance" to breach privacy laws and use information for a purpose outside the scope of the data collection? The use of 'loopholes' cited create a slippery slope, and are a breach of the public's trust and personal liberties.

The authorisation lockdown measures, have breached human rights across the states and territories and most notably in Melbourne and Sydney. Melbourne, despite having some protections through the *Victorian Charter of Human Rights & Responsibilities Act 2006(Vic).* The Victorian Ombudsman's finding that the Public Housing tower lockdown is one such example of breaches of the human rights charter *(*https://assets.ombudsman.vic.gov.au/assets/Reports/Parliamentary-Reports/Public-housing-tower-lockdown/English-Summary-of-investigation-into-public-housing-tower-lockdown.pdf*).*

This example highlights a further recent example of how despite having legal protections in place does not guarantee the protection of human rights and how the public have reason to distrust that Government will act in the best interests of the people they serve.

The Queensland Premier was also referred to the Human Rights Commissioner to investigate the allegation of a human rights breach by the Palaszcuk Government regarding border restrictions that are denying Queenslanders their right to lawfully return to Queensland (https://www.sydneycriminallawyers.com.au/blog/queensland-premier-referred-to-human-right-commissioner/). This double standards granting exemptions for entering Queensland, with sports stars and celebrities favoured over Queensland residents demonstrates the enormous abuse of power of a leader acting for political opportunism and popularity, demonstrating an inability to act in the interests of the people she was elected to lead.

The risks of centralising a significant volume of personal information in the hands of Government, who have done little to demonstrate that they should be trusted by the public do not outweigh the benefits to the individual stated in the RIS.

In addition to the above concerns, the following objections are raised:

- It is not essential and digital infrastructure in place is currently sufficient to service current and future digital needs.
- There is enormous potential for abuse of power, discrimination and privacy of the individual.
- Centralising such a volume of digital information in one location would pose an enormous threat to safety of private information, with greater potential for a centralised digital system to be hacked by malicious actors. The safer option to counter this threat would be to hold sensitive information in multiple locations.
- The digitisation of identities would 'lock out' or marginalise at risk groups including elderly citizens who lack computer literacy.

<u>A pre-curser to the Chinese social credit system</u>

The stated purposes of the legislation are to:

- enable the expansion of the Australian Government Digital Identity System, specifically to enable greater participation by state and territory governments and the private sector
- enshrine in law various privacy and consumer protections, so that Australians can have confidence in the System and know that their personal information is safe and secure establish permanent governance arrangements and a strong regulatory regime.

The RIS states that the system should be based on the principles include:

- *Choice – ensuring that creation and use of a digital identity is voluntary at whatever Identity Proofing Level a person chooses to have, and that individuals also have the option to select from multiple identity providers.*
- *Consent – requiring consent at multiple occasions when an individual interacts with the System, and the ability for that individual to withdraw consent at any time through an easily-understood process*
- *Privacy – safeguarding the personal information of individuals is the single most important design feature of the System, with privacy-enhancing principles embedded in its design and architecture*

- *Security – including specific security requirements which participants must comply with to become and remain accredited, and otherwise embedding security protocols in the System design*
- *Integrity – ensuring that an appropriate governance structure is in place, with an Oversight Authority responsible for operational System assurance, as well as safety, reliability and efficient operation of the System.*

Despite these principles, including the voluntary nature outlined, this legislation sets the framework which could enable a mandatory social credit system, like that which is currently in place in China. China's social credit systems provides an alarming case study of both government overreach and the overwhelming control that government has over its citizens and their quality of life. This NBC news feature (https://youtu.be/0cGB8dCDf3c) highlights the features and operation of the social credit system, which should be considered alarming to anyone who believes in and cherishes the democratic way of life in Australia. Among the key elements highlighted were:

- The system completely monitors the citizen through omnipresent cameras in the urban environment and assigns social credit based on lifestyle choices from the major to the most minute of actions.
- Through this system an individual starts with 1000 points and can lose points for things like jaywalking, littering or even spreading rumours.
- Posters are placed around the urban environment showing the ways an individual can gain or lose points and a nightly news program shows highlights of surveillance during the day.
- Citizens are paid as "information collector" enforcers who walk around and document the deeds of neighbours to inform their social credit.
- If you have bad social credit or are put on a social credit blacklist this will significantly impact on an individual's quality of life. Being discredited makes it hard for an individual to get a job, loan, a hotel room, or put children in certain schools. Additionally, there is public shaming through apps or online galleries of discredited people.
- The above news feature highlights an example, of an individual on a social credit blacklist who could not buy an airplane or train tickets. When attempting to do so, a message appeared stating that the individual was discredited. The feature indicates that in a year, 23 million people were blocked from booking flights.
- The algorithmic surveillance allows for the collection of data to build detailed profiles of people especially those who are identified as being "not loyal to the Government", which is augmented by Artificial Intelligence.

The Chinese social credit system is instructive and highlights the Orwellian trajectory this Bill is travelling on.

INDICATION OF MASS OBJECTION TO THE DIGITAL ID PROPOSAL

The total subscribers and follows of the Concerned Lawyers Network exceeds 25,000 and we have had volumes of people express their objection to the proposed bill. 100% of the feedback has been AGAINST any form of Digital ID whether it be voluntary or or not. In summary, a digital identity for each Australian does not meet the needs of the community and is not supported.

For the abovementioned reasons in this submission, Concerned Lawyers Network and myself and the subscribers of the Concerned Lawyers Network object to this Bill in the strongest possible way and urge you to maintain the status quo (i.e. no regulatory action taken) and abandon the proposed legislation**.**

27.10.21

Maria Rigoli *B.A. LLB. (Melbourne University) Acc.Spec (Fam)*

Concerned Lawyers Network

Concerned Lawyers Network