Australia's Digital ID System

Key questions on the Digital ID legislation and Digital ID Rules

[redacted]

Page # of guide	Question	Your response
14	What other types of Digital ID service should be included in the legislation, either now or in future?	The introduction of the Digital ID will have significant and far reaching effect on the lives of each and everyone of us in Australia. We cannot even envisage all the potential consequences and outcomes from such a massive undertaking. We are rolling into unknown from which we might find it extremely difficult, if not even impossible, to back out. The 2023 Digital ID Legislation Exposure Draft consultation process for the public is open for less than a month (22 days – from 19/09/2023 to 10/10/2023). The consultation process covers in many details hundreds of pages of rules and exposure draft. Many news, and other online communication means, reference in great extent the Voice, the departure of the Victorian Premier Daniel Andrews, the COVID-19 inquiry, amongst many noteworthy stories but there is hardly a whisper about the Digital ID consultation process. I found out by chance. It feels as if there is no interest to hear from as many as possible. This raises concern.

Page # of guide	Question	Your response
		I have through this process realised that the Privacy Act 1988 is going through an update, and that a consultation process was undertaken earlier this year. I have had no idea that this was happening. Public responses to the review indicate that the survey was difficult to find. We are introducing and changing legislations without substantial input from the public that does not seem to have been duly informed. Any relaxation of privacy rules will have significant effect on the Australian community. Some such examples are Proposal 14.1 to permit broad consent for research; enhanced emergency declaration powers under Proposals 5.3, 5.4, 5.5 that will facilitate enhanced information sharing in certain circumstances; Proposal 28.4 allows sharing of information in case of eligible data breach. https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report The consultation process and introduction of the Digital ID needs to be significantly expanded. The Australian public should be transparently and comprehensively informed about the process and outcomes. In its current state, I cannot see that we are ready to go forward with the AGDIS.
14	Does the Minister's rule-making power to include new services over time provide appropriate flexibility to add new types of Digital ID services? If not, why not?	There is potential that the Minister has too much power. *-- Draft Digital ID Rules* *Part 3 section 10 Holding etc. information outside Australia* *Subsection (5) On application by an entity mentioned in sub rule (1) , the Minister may grant, in writing, the entity an exemption in respect of the holding, storage, handling or transferring of the system information at a specified place outside Australia.* We should not allow foreign locations. *-- Exposure Draft* *Chapter 9 Section 159 Rules – requirement to consult*

Page # of guide	Question	Your response
		Subsection (4) Exception if imminent threat etc. Ensure this applies only if stricter controls are considered i.e. privacy rights and voluntary use are not downgraded in any way. These rights though, as is presented in the draft, should be tightened before the legislation goes forward.
16	Is the Regulator's power to impose conditions on accreditation an appropriate mechanism to balance the need to provide for unique characteristics of accredited entities with the need for a consistent set of Rules for the Accreditation Scheme? If not, how can the Regulator's power to impose conditions on accreditation be improved?	There is potential that the Digital ID Regulator has too much power. *-- Exposure Draft* *Chapter 5 Part 2 Section 87 Powers of the Digital ID Regulator* *The Digital ID Regulator has power to do all things necessary or convenient to be done for or in connection with the performance of the Regulator's functions under this Act.* How broad is the interpretation of section 87? How much power is actually given?
16	Is the application for accreditation process appropriate, or should other matters be included or some excluded?	Government entities should be included only. We should not be considering private entities now.
17	Are the maximum penalties for failure to meet accreditation requirements sufficient to deter accredited entities from not meeting their obligations? If not, what maximum penalties would be an appropriate deterrent?	Start small. Start with government agencies only. Review frequently. Involve the Australian community in best practice identification. Private corporations should not have involvement until we are confident that we understand well how we can align in practice implementations with accreditation requirements and best fit guides. This will allow us to review penalties for maximum benefit. I feel that we are rushing through to introduce the Digital ID, as if we are going to miss out in case we don't start 'now'. The opposite will actually work better in the long run. We need to build our trust in the system. It takes time to gain trust and it is easily lost. The Robodebt scheme is an example of negative outcomes when solutions are rushed.
21	Are the additional privacy safeguards	There are too many exceptions!

Page # of guide	Question	Your response
	sufficiently robust, clear and practical?	<u>Privacy Act</u> Privacy Act 1988 (Cth) – we have seen the Privacy Act bypassed during emergency acts of power. Any mention of the Privacy Act was ignored by employers when they were gathering personal medical vaccination status information, some of these are still in place. Similarly the public was not allowed to attend many places such as stores and venues without providing their private medical information to 'anyone and everyone'. As an example, 14 year old and younger children could not go to local ice skating without intrusion into their health matters or parents could not visit schools. Any APP-equivalent agreement needs to have at least the same or higher restrictions as the Privacy Act 1988 and any additional restrictions that come out of the Digital ID Legislation. These restrictions cannot be reduced in any manner of form in the future regardless of potential future updates to the Privacy Act or this legislation or any external influences. This should be set by law. Please provide exact details of an APP-equivalent agreement with the Commonwealth for our review before any legislation is put in place. We need to put into legislation that the privacy of users cannot under any circumstances be bypassed. The privacy of the user has to be at the forefront of every single step of the process. <u>Exceptions</u> All exceptions should be removed. Looking at all these exceptions in the draft Bill significantly erodes confidence in the AGDIS.

Page # of guide	Question	Your response
		The only exception that I could think might be allowable to a very limited extent is for Digital ID fraud investigation and even then users should be notified and consent provided unless the user itself has hacked/tampered with or in other way directly tried to manipulate the Digital ID system. For testing purposes, a user always needs to be provided with clear and full information about the extent of involvement, potential consequences and outcomes. The user always needs to provide consent on an opt-in basis. The consent approval should not be hidden as we can see nowadays on websites that ask you to accept cookies or software that seeks acceptance for terms and conditions you can't modify and with so much information that many users are hardly able to or have the time to understand the context and details. <u>Consent</u> We need to ensure that people are not mislead or enforced to provide consent. Consent should apply to any user information. There should be no opt-outs. There should only be opt-ins. These clearly indicate to the user that a choice needs to be made and if one isn't done, the default will not inadvertently expose private user data. Breaches can happen throughout the flow from the provider of the digital ID to the entity that seeks the use of a digital ID. The first and greatest need before implementation of any Digital ID is to have in place clear and straightforward procedures and processes that allow Australians to access government and private services without the need to go online. I can't nowadays, for example, even buy an antivirus software without getting a subscription and having to provide my credit card details online, even if I go to a store and buy a pre-paid card. Until recently, I did not have to provide any

Page # of guide	Question	Your response
		such details. I unfortunately expect this practice will expand requirements following the introduction of AGDIS. I have seen online a large government agency advising users that they need to use a digital ID – myGovID - to be able to access their portal. The web site does not have any advice on how a user can provide information without using a digital ID. I could not see easily either how to remove the digital ID. This practice seems misleading since many users would assume that this is their only option. It goes in direct contradiction to the indicated use per the Digital ID legislation. How do we ensure that the Digital ID is not being pushed onto Australians when I have not seen anywhere any information provided about potential consequences of its use – there is always for and against. *-- Exposure Draft* *Chapter 3 Privacy* *Section 28 – Digital IDs must be deactivated on request* A maximum timeframe needs to be set by legislation for deactivation of digital IDs upon user request, i.e. 1 week. A user needs to be able to access a simple request process for deactivation of the user's digital ID. Templates and processes for such requests need to be provided and should be in place by accredited entities. What happens to backed up information that is stored through regular backups. How do we ensure that none is retrieved after a digital ID is deactivated? Do we ensure that any backups are automatically cleaned for any reference to a deactivated ID? Can this even be done? Or do we store backups in a way that will not allow us to read entries unless a key or else is enabled, which gets disabled by deactivation. *-- Exposure Draft*

Page # of guide	Question	Your response
		Chapter 3 Part 2 Division 2 Additional privacy safeguards *Section 41 Collection etc. of certain attributes of individuals is prohibited* Details to be provided for unintentional collections – case scenarios and what are procedures to follow. It will provide service entities greater understanding of what needs to be done. There is so much mention of fraud controls, management and responses that it makes me feel uneasy. We are painfully aware that frauds and breaches will happen. The centralisation of identity data exposes us to much greater consequences in such cases. A user should not by default have to agree to the use of personal information for activities such as fraud by an accredited entity.
21	Is the rule making power to allow disclosure of biometric information to enable sharing of verifiable credentials (under specified circumstances) an appropriate exception to the restriction on disclosure of biometric information?	*-- Exposure Draft* *Chapter 3 Part 2 Division 2* *Sections 44 Restricting the disclosure of unique identifiers* *Subsection (4) – Subsections (2) and (3) do not apply if...* *and Section 46 Authorised collection, use and disclosure of biometric information of individuals – general rules* *Subsection (3) An accredited entity is authorised to disclose biometric information of an individual to a law enforcement agency...* The exception that allows disclosure of the unique identifier should be removed. We need to ensure that identifiers and logs can link paths of usage without connecting to a person. Any notification to a user should not expose the unique digital ID or other personal information to any third party. There should NEVER be a case to use a personal ID of a person that could put them in harm's way because a person has taken up a digital ID in the first place. Exceptions break the first rule of keeping personal identifying information

Page # of guide	Question	Your response
		private. Biometric information should never be disclosed. Another exception! Reading through the consultation papers, it appears as if we are setting up Australians on the path of track and trace - where have you been, what have you done? Why would for example a tribunal have any access whatsoever? Destroy the biometric information immediately after the verification is complete – contra to keeping for 14 days for fraud and testing. *-- Draft Exposure* *Chapter 3 Part 2 Section 48 Destruction of biometric information of individuals* *Subsection (4) ...preventing investigating digital ID fraud incidents...* Please update wording "(about preventing investigating digital ID fraud incidents)" - are we preventing investigation? – likely not. *-- Exposure Draft* *Chapter 3 Part 2 Division 2 Section 50 Data profiling to track online behaviour is prohibited* *Subsection (3)* Online data profiling and tracking of online behaviour using the Digital ID should always be prohibited. The clauses are being watered down. I can see extremely limited use for IT services, users should in any such cases be de-identified. All other cases to be withdrawn from legislation. *-- Exposure Draft* *Chapter 3 Part 2 Division 2 Section 51 Personal information must not be used or disclosed for prohibited enforcement purposes.* Remove ALL exceptions. Remove wording 'prohibited'. Exceptions actually

Page # of guide	Question	Your response
		provide 'approval' for trace and tracking using a Digital ID. The legislation needs to be written in such a way that these entries cannot be added in a later amendment either. These sections significantly reduce confidence that the Digital ID legislation will be primarily in the interest of Australians. Instead it appears as a tool for the government. Review fraud particulars. *--Exposure Draft* *Chapter 3 Part 2 Division 2 Section 52 Personal information must not be used or disclosed for prohibited marketing purposes* *Subsection (2) Subsection (1) does not apply to the disclosure of personal information about an individual if...* Individual's consent should not be sought through misleading activities such as not providing clear information about the ability to 'not accept'. Consent as we are seeing can be generated in many ways i.e. you are forced as otherwise you get less or no service or simply by accessing the provider you allow advertising etc. The default should be no advertising. There should be clear and easily accessible means to provide consent, if this is what the user wants, and to later have the consent removed without the need to go through many pages i.e. terms and conditions or trying to call the provided phone number that then tells you they have too many high volume calls and you should try later (as was the case I had today trying to follow up on my potential voice print activity).
21	Is the maximum penalty for a breach of a privacy safeguard sufficient to deter accredited entities from interfering with a person's privacy? If not, what maximum penalty would be an appropriate deterrent?	Is 300 penalty units per individual breach or for the whole scope i.e. single 300 unit across multiple individuals (i.e. 100,000 individuals) for the same breach action? It should be at least scaled if multiple users have had their information breached. Large corporations can easily manage 300 penalty units, there should be further penalties as they can also easier implement rules and have

Page # of guide	Question	Your response
		the potential to squeeze out smaller entities. Users should be compensated when their information is breached. Compensation should not be just in terms of a monetary value lost but also the appropriate value for the exposure of private user's information that has the potential to cause psychological, social, financial and other harm. How easy is it to withdraw consent and confirm that biometric (and other) data has actually been destroyed? Data in backups should also be destroyed or at least access cancelled. User consent needs to be on an opt-in basis to a provider to allow biometric data to remain for 14 days for testing.
23	What is the appropriate age at which a young person should be able to create their Digital ID? What factors should be considered?	A young person should be **at least 18 years old** to be able to create a Digital ID. These systems are in the infancy phase. A young person does not have well developed capability to understand risks and consequences and would have very little experience in dealing with services that use confidential private information. My experience with young people as a parent has definitely presented the need to support them into adulthood. There is nothing wrong in using alternate means to access services when the need arises. We should not present these as old fashioned in order to nudge young people into thinking that they will be 'cool' using Digital IDs. We should not speed up the digitised process. We MUST have parallel services available outside of the Digital ID space. I had to in the past go through 'hoops' just to be able to get into contact for support with an actual person for the Medicare government service. I was continuously being pushed online but the online facility did not have solutions for my specific case. It was almost impossible to get a person to talk with. We need to have direct types of support readily available but there is very little happening in this space. I am seeing these services steadily being reduced

Page # of guide	Question	Your response
		and removed.
25	What other steps could the Government consider taking to ensure the AGDIS is ready for use by private sector relying parties and accredited entities?	We should not rush into the use of AGDIS by any party. Actions and the pre-requisites to be implemented before any use of AGDIS: 1. allow people to access government and private sites and services in a manner that does not and will not enforce them to go via a digital id now or in the future. 2. ensure that infrastructure, procedures and controls are in place that enable and enforce number 1 above. 3. ensure that number 1 cannot be changed by legislation i.e. people will always have the option to not use a digital ID. Alternative means need to be clearly and readily provided while a user should not need to go out of their way to try to identify options that are available. We are already seeing the push to go digital. An example is: - the use by ATO where, when I called 2 different numbers, I was advised on each call that a highly secure and faster way was introduced to access my information and that my call will be recorded to improve services and create my unique voice print, which may be used to verify my identity. I was not asked for permission for a voice print and identification, or provided with any suitable alternative, or provided with any explanation, or had the possibility to remove the recording. I did not have the option to simply say no to the process. The whole phone interaction was very uncomfortable and I felt I had no choice but to abruptly end the call. How do we ensure that we do not have a digital ID pushed regardless of the voluntary nature proposed? I am against the involvement of the private sector, especially foreign entities and corporations.

Page # of guide	Question	Your response
25	What factors should the responsible Minister consider prior to deciding to approve the AGDIS expanding into another phase?	The Australian public needs to be fully aware of the Digital ID implementation, including both positives and negatives, without being exposed to ads and other narratives that glorify the system and have the potential to mislead. We need to have open, robust and transparent discussions, prototyping and incremental implementations. It is too early to even consider private entities.
26	How would phasing the rollout of the ADGIS affect the wider Digital ID services market in Australia?	The broader the implementation the higher the risk for privacy exposure and mandated use. Imagine the setback if the system is hacked in its early phase of development.
27	Is the balance between voluntary use and the exceptions to voluntary use right? Are any additional exceptions appropriate?	There should be NO exceptions or exemptions. *-- Draft Exposure* *Division 4 Section 71 Creating and using a digital ID is voluntary* Remove Exception under subsection (3) and Exemptions – There should never be a requirement to access a service only by means of a Digital ID. We cannot start this process until we have in place controls that ensure voluntary use. This is a very watered down section. The Digital ID Regulator has great power. The voluntary subsection (1) has been overwhelmed by other subsections that override it. Options should be clearly specified and easily accessible that allow use of alternatives to the Digital ID process. 'Creating and using a digital ID is voluntary', under Section 71, has so many exceptions and exemptions that it sounds like an oxymoron. Are we going towards seemingly allowing people the right to not use a digital ID but finding ways to actually enforce the use of digital IDs? We have similar happenings with cash – I heard from a food outlet I recently visited that as per advice from the Reserve Bank "It is OK to not allow cash purchases as long as you visibly display 'no cash accepted'". Banks are increasingly removing cash and ATMs, and closing or reducing branch activities, as I have experienced first hand and as can also be seen

Page # of guide	Question	Your response
		through the Senate Banking Inquiry. With reference to the Exposure Draft example under subsection (2) – how are we going to enforce the availability of a local bank branch service or other ways to access banking services if a customer does not want to use the digitised system? How are we going to ensure that a customer will not be pressured? A pizza shop told us to go online and order even though we were physically in the shop. You either follow the direction or the business loses a customer. It can be difficult to manage the online maze. This was visible earlier this year when banks sought validation of users. The online option sought extra information that did not appear essential for the purpose. The form had questions that could not be bypassed. The alternate process in the branch was very simple and without intrusive privacy concerns. We are already seeing 'enforcement' to use digital IDs, examples are for Unique Student Identifier (USI) and Director ID. It is a matter of time before we see more private identifying data added and connected. What are processes in place that are very easily accessible for users to put in a complaint and will not put users in a difficult position with entity service providers? Systems and processes should be in place, before any implementation of ADGIS, that allow us access in different ways regardless of any Digital ID availability and use. Corporations should be fully aware of this obligation.
27	Are the exemptions to the interoperability principle appropriate? Are any additional exemptions appropriate?	Remove the ability to store any information outside Australia under any circumstances. Implement in legislation in a way that cannot be changed with future amendments. We cannot put the privacy and security of Australians in potential jeopardy. Do not allow the Digital ID Regulator such great powers to grant exemptions that could see private entities gain rights initially out of

Page # of guide	Question	Your response
		scope. The cost should not be the breaking point. We cannot allow foreign companies to store internationally any Australian private information used through the Digital ID. Online corporations are already trying to retrieve and relate our information on a daily basis. It has become so intensive that I would, and probably many others, appreciate if something can be done so that our data is not being exploited or constantly asked for. We should not be using a Digital ID with a foreign company regardless of any arrangements and rules in place. What would happen in case, for example, of a war? Agreements with a foreign entity could become void and data and infrastructure exposed. The exposure of a Digital ID will have far more reaching consequences than most of the cyber leaks we have seen so far. Needless to say how easy it is to link and correlate all personal data nowadays. We do want to have confidence in the system. Therefore, every step of the process needs to be meticulously determined and managed.
29	Are the protections for the Australian community within AGDIS appropriate, or are additional protections needed?	Of concern is the use of a personal device i.e. phone with an installed application that can be subject to hacks, viruses, out of date software, network downtime, non-individualised devices, 3rd party in person enforcements and much more. We need to legalise privacy principles for any device used for this purpose. How can this even be achieved with today's technology? I do NOT want us to get into a position where we as the user have a software on the device banned, or have to provide our device to a 3rd party for any purpose, or have the responsibility for a breach passed on due to our device settings and other personal matters etc.

Page # of guide	Question	Your response
		How do we ensure that private devices and accesses i.e. emails have the best interests of Australians? Software and hardware are easily updatable to corrupt and enable retrieval of information by 3rd parties. These are controlled in many cases by foreign corporations. We often don't even realise the extent of the software reach that we install for games, weather, school and so on. Additionally, we have to frequently agree to terms and conditions, without the ability to change any items and therefore few read those. We seem to be chasing our 'tails' with frequent security updates and another antivirus or other 'unknown' upgrade. Will the government supply the device i.e. phone (a device that will NEVER be privacy intrusive and a data gatherer) and guarantee the security and its availability? What happens while out of action for any reason (stolen, broken, misplaced, software error, repairers seeking admin access), especially considering all those exceptions proposed. What is the cost benefit when we take into consideration the ongoing maintenance cost including also activities to ensure regulation is followed, user and security flaws are identified and fixed. This is a large undertaking. How much do we expect it will cost the Australian tax payer? How can we ensure that the majority of infrastructure and other related budget remains in Australia? We need to take a step back. Even though there has been consultation in the past (that I have not noticed), the undertaking is so substantial that we cannot rush into broad use of Digital IDs until we have prepared the environment. We need to provide case scenarios including worst case ones, prototypes. We, Australians, need to know that we will not be discriminated against if we do not use a Digital ID. Non-digital systems for identity verification must

Page # of guide	Question	Your response
		remain and be maintained. I could not see if and how Artificial Intelligence (AI) might be used and managed. We do not want runaway programs with complex algorithms where IT support and entities could potentially end up with very little understanding of what they do and how they work. *-- Draft Exposure* *Chapter 5 Part 2 Division 2 Section 90 Disclosing personal or commercially sensitive information to courts and tribunals etc. by entrusted persons* *Subsection (2) The bodies are a court, tribunal, authority or other person having power to require the production of documents or the answering of questions.* Very broad are bodies - court, tribunal, authority or other person - that have the power to require the production of documents or the answering of questions. We are opening the way for law enforcements for almost anything…. Remove any disclosure of sensitive information in section 90. *-- Draft Exposure* *Chapter 5 Part 2 Section 91 Advisory committees* Only Australians within the government and no commercial interest i.e. no conflict of interest. Does disclosure of interests deal with conflict of interest? What happens when disclosed interest shows great conflict of interests i.e. share holding in an entity? We need to be able to review and have the process under parliamentary scrutiny. *Section 153 Review of operation of Act* has under subsection (2) “no

Page # of guide	Question	Your response
		later than 2 years after the commencement of this Act" – change to no later than 1 year – and then yearly.
29	Are the protections for participants in the AGDIS appropriate, or are any additional protections needed?	*-- Draft Exposure* *Chapter 6 Part 3 Section 102 Application of the finance law etc.* Subject to public scrutiny. The Australian public needs to be well informed of the annual report availability to read through. *-- Draft Exposure* *Chapter 6 Part 3 Division 4 Section 110 Consultants* We need to ensure that any consultants will work for the best interest of Australia and not external or commercial interests. Will the same conflict of interests be disclosed as expected from the Advisory Committee? *-- Draft Exposure* *Chapter 8 Part 3 Section 130 – Destruction or de-identification of certain information* Remove under subsection (2) entries (c) and (d). This is yet another exception in the Exposure draft of the Digital ID Bill. *-- Draft Exposure* *Chapter 8 Part 6 Division 2 Section 142 Charging of fees by accredited entities in relation to the Australian Government Digital ID System* *(2) The Digital ID Rules may make provision in relation to the charging of fees by accredited entities for services provided in relation to Australian Government Digital ID System.* What is the expectation of the cost? Could it become exuberant? Especially now that we have increasingly struggling households with rising costs and

Page # of guide	Question	Your response
		inflation. *-- Draft Exposure* *Chapter 9 Section 144 Annual report by Digital ID Regulator* Include cost. Provide end user feedback. Include summary of complaints and resolutions. Results from survey provided to users and entities that include open ended comments. *-- Draft Exposure* *Chapter 9 Section 151 Protection from civil action* *Subsection (2) A person mentioned in subsection (1) is not liable to an action or other proceeding for damages for, or in relation to, an act done or omitted to be done in good faith by the person.* Define what in good faith means. *-- Draft Exposure* *Chapter 9 Section 153 Review of operation of Act* Review – external of the whole process and consultation with the public at regular periods. Update wording: Review to be done no later than 1 year after the commencement of this Act and then yearly. *-- Draft Exposure* *Chapter 9 Section 159 Rules – requirement to consult* *Subsection (1) (b) if the rules deal with matters that relate to the privacy functions (within the meaning of the Australian Information Commissioner Act 2010) – consult the Information Commissioner*

Page # of guide	Question	Your response
		What is this about “if the rules deal with matters that relate to the privacy functions”? There should be no reduction in privacy, only stricter rules can be implemented. *Subsection (4) Exception if imminent threat etc. - Subsection (1) does not apply if...* Do NOT take away or reduce privacy and voluntary rights for anything.
34	Noting the pace of technological change and the need for Digital IDs to stay protected by the latest developments, how can Data Standards provide an appropriate balance between certainty for accredited entities while maintaining currency?	Ensure upskilling is in place, continuous testing, incremental implementations, provide technological and other guidance where appropriate, utilisation of synthetic data and tools, ongoing workshops and reviews, enable a platform for easy feedback that is followed up, focus on complaints. Don’t forget the user. The best certainty will be guided by user voluntary uptake demand and close and ongoing understanding of user requirements.
34	What would be an appropriate model for the Australian Digital ID Standards Chair and are there lessons that can be learned from the Consumer Data Right model?	Do not have CDR enforced. Customers should not be disadvantaged or discriminated against in any way if they do not take up CDR.