Company's Name	**: Privy ID**
Subject	**: Privy's Suggestion for Digital ID Bill**
Date	**: 3 October 2023**

- Cybersecurity Issues & Privacy protection within Interoperable Systems

  As with any system that holds a lot of sensitive information centrally, such a centralised database that runs interoperable systems could be the major target of hackers and result in a data breach. Cyber security controls and proper system risk management must be the priority.

  Further, as the system would be the central database for all sensitive data under Commonwealth, state, and territory, the government needs to have a proper internal management system to differentiate the source of data (from Commonwealth, state, and territory) where within all government levels involved it will implement best security practice for all the agencies. We also need a clear distinction of liability to operate, thus when a problem arises, we can identify which part needs to be mended and who is the point of contact to be responsible/escalated to solve the matters.

- Clear Roles and Responsibilities for the System Operation

  The government must set out clear policies in relation to how the government will utilise the sensitive information contained in the database. This is to prevent malicious conduct by the internal government towards such database (i.e. if the government is going to think it is a great data set to train AI models on, without realising the implications).

  Further, there should be a clear data sharing arrangements between the government and private sectors (e.g. clear agreement setting our roles and responsibilities in place). Both institutions need to share information to prevent fraudulent use of identity following a data breach. Information sharing will also be required to support the vision of harmonious sharing, updating and management of credentials.

  In the long run, there should also exist an initiative that could cater to a change of identity within the record database. For instance, if there is a change of name and/or gender in the long run birth certificates or immigration records are not always linked to change of identity processes. This initiative will explore updating identity records for life events, making myGovID/AGDIS have a strong database.

- Readiness of ACCC

  As the legislation will initially appoint the ACCC as Digital ID Regulator to regulate accredited Digital ID providers and the Australian Government Digital ID System (ADGIS), the independent institution needs to be ready to cater to every concern relating to Digital ID, and make sure that not only private sectors that need to comply with the standards set out under Digital ID Bill, but public sectors as well.

  Further, as the government will be reliant on the biometric techniques widely available in mobile phone handsets (e.g. facial recognition, thumbprints), we suggest that the Digital ID systems remain flexible, as we may see the development of biometric verification from time to time.

- Involvement of other stakeholders

We understand that one of the main purposes of Digital ID Bill is to enable more choice of which entity the user would want to create a Digital ID with and where the user can use it (e.g. choose to use a state or territory Digital ID, verify your ID with banks, real estate agents, telecommunications companies).

In implementing the above purpose, there will be many stakeholders that would be involved. Therefore, we suggest that the regulation put the implementable and feasible privacy, security, and fraud control standards for those stakeholders to comply with, in order to avoid a potential data breach occurring by such stakeholders.

Further, the industry and government should implement and promote best practices for deterring and responding to data breaches, including actively coordinating efforts to improve awareness, secure cyber practices, and support services.

- Exemption towards penalties in the event that the company has complied with Digital ID Bill and Privacy Act standards and requirements.

  Digital ID Bill should have a clear accountability and liability clause. As the company would initially try its best effort to meet all standards and requirements set out under Digital ID Bill and Privacy Act, therefore, we suggest that the Bill give an equal opportunity to the company to present its case to justify the data breach (in the event that it occurs within the company), beyond the company's control.

  Therefore, the penalty could be exempted or at least be reduced based on the company's effort to comply with Digital ID Bill and Privacy Act and be fully enforced and put the full liability towards the breach to the main perpetrator.

- Rights of data subject

  As the registration of Digital ID is voluntary, therefore, if the user chooses to register, it is also the user's choice to be able to exercise their rights (i.e. to update details of their personal information), in the application which such users choose. Therefore, there should be no single "one-stop shop" interface – rather credentials maintained in multiple systems can be updated through any one of those systems and Digital ID Bill should provide equal opportunity and services to every platform both public and private sectors to cater to this matter.