Senate Economics Legislation Committee

Inquiry into Digital ID Bill 2023 and the Digital ID (Transitional and Consequential Provisions) Bill 2023

Department of Finance

Response to Question on Notice

Hearing of 9 February 2024

Question on Notice 1 (Proof Hansard page 31 – Senator Walsh)

Topic: Law Enforcement access to digital ID data.

CHAIR: …How can law enforcement access the digital ID data, and how has that changed from the exposure draft through consultation? You would have noted from submitters today that concerns remain about access by law enforcement to the data. How have you arrived, through consultation, to the position that the bill reflects now?

Response

The Digital ID Bill 2023 (the Digital ID Bill) has restrictions on accredited entities disclosing personal information to law enforcement bodies that go beyond those in the *Privacy Act 1988.*

Clause 54 provides that *personal information* may only be disclosed to law enforcement bodies in certain circumstances, which include:

- if the disclosure is required or authorised under warrant; or
- if the individual gives express consent and the disclosure is for the purpose of verifying the individual's ID or investigating or prosecuting an offence; or
- if an enforcement body has commenced proceedings against a person for an offence against a law or breach of law imposing a penalty.

The Digital ID Bill provides stronger restrictions over the disclosure of *biometric information*. Clause 49 provides that biometric information may only be disclosed to a law enforcement body:

- if disclosure is required or authorised under warrant; or
- if the individual gives express consent and the disclosure is for the purpose of verifying the individual's ID or investigating or prosecuting an offence against a law.

These provisions of the Digital ID Bill seek to strike a balance between:

- current legal frameworks
- stronger safeguards on the disclosure of Digital ID information to law enforcement than what applies to information on ID documents when used outside of the Digital ID system; and
- ensuring that law enforcement can investigate and prosecute criminal behaviour, including identity crime.

Access to this information by law enforcement agencies is considered essential to protect Australia's Digital ID system from malicious actors, protect the privacy of individuals and respond appropriately to criminal behaviour. For example, the Australian Federal Police (AFP) may require access to personal or biometric information to investigate Commonwealth offences, such as identity fraud, where a malicious actor seeks to exploit a person's Digital ID for financial gain or to obfuscate other criminal activity.

When reaching a position on law enforcement access to digital ID data, a number of competing views were taken into account. These include:

- current Commonwealth policies and legal frameworks in relation to accessing data (such as the *Privacy Act 1988* and the *Crimes Act 1914*);
- the views of human rights and privacy advocates who suggest that strong restrictions on law enforcement are crucial to building trust in the Digital ID system;
- the views of state and territory governments on the needs of their law enforcement agencies, including the ways that those agencies view or access a digital driver licence;
- examples of how law enforcement access to this data could lead to improvements in safety (such as in cases of kidnapping and family violence); and
- independent advice from the Minister's Digital ID Expert Panel.

Following the Exposure Draft consultation, the Bill was amended to remove a provision which enabled accredited Digital ID providers to disclose personal information where an enforcement body reasonably suspected that an offence had occurred (retaining those in clause 54 above).

During consultations on the exposure draft legislation, some stakeholders also suggested limiting access to only certain types of crimes (for example crimes of a more serious nature, or fraud or cyber security incidents directly related to the Digital ID system). The reasons for not adopting suggested restrictions are outlined below:

- There is already a well-established legislative framework governing law enforcement access to personal information under warrants. There are specific procedures and certain criteria that need to be met in order to obtain a warrant. These safeguards help ensure that any warrants issued are specific in their purpose, preventing them being used to access information for mass surveillance.

- If law enforcement access to personal information in the Digital ID system were to be limited only to 'serious offences' (offences with a maximum penalty of 7 years or more), this would become too inconsistent with existing legal frameworks that allow law enforcement to obtain the same information outside of the Digital ID system. For example, the AFP routinely uses warrants under section 3E of the *Crimes* Act 1914 (Cth) to obtain information required for an investigation. When necessary, this will include warrants for sensitive information such as health records or biometric information.

- Increasing the minimum threshold to offences that carry a maximum penalty of 7 years or more would significantly impact the ability of law enforcement agencies to protect the community. At the start of an investigation it may not always be apparent whether an offence will be a serious offence. Moreover, offences with lower penalties still have a significant impact on an individual and the community (e.g. possession or control of data with intent to commit a computer offence (478.3 of the *Criminal Code Act 1995*).

- Limiting the disclosure of information to serious criminal fraud and cyber security incidents directly related to the use of accredited Digital ID services would be challenging to implement, acknowledging the number of ways in which a Digital ID could be misused to commit an offence.