Australian Government

Office of the Australian Information Commissioner

Law enforcement access to Digital ID information

November 2026



OAIC

Contents

Prohibition on handling information for enforcement and law enforcement purposes 2

Disclosure of personal information to enforcement bodies 2

Disclosure of biometric information to law enforcement agencies 3

Prohibition on handling information for enforcement and law enforcement purposes

The *Digital ID Act 2024* (the Digital ID Act) prohibits the use and disclosure of information, held by an accredited entity in connection to their accredited services for enforcement and law enforcement purposes unless one of a limited number of exceptions under the Digital ID Act apply. In contrast, the *Privacy Act 1988* (the Privacy Act) and Australian Privacy Principles (APPs) permit disclosures of personal and sensitive information to an enforcement body when it is reasonably necessary for an 'enforcement related activity'.[1] The Digital ID Act overrides the Privacy Act and the APPs to prohibit law enforcement access, with some exceptions. This prohibition applies despite section 86E of the *Crimes Act 1914* and any other law of the Commonwealth or a State or a Territory, whether enacted or made before or after the commencement of the Digital ID Act.

Disclosure of personal information to enforcement bodies

An 'enforcement body' has the same meaning as under the Privacy Act and includes Commonwealth and State or Territory government agencies responsible for administering certain laws. For example, the Australian Federal Police, State/Territory police forces, the Immigration Department and the Australian Prudential Regulation Authority. It has a broader meaning than 'law enforcement agencies' set out below.

Section 54 of the Digital ID Act outlines that an accredited entity must not use or disclose personal information of an individual for the purposes of enforcement related activities conducted by or on behalf of an enforcement body unless one of the following circumstances apply:

Circumstances where use or disclosure of personal information, that is not biometric information, for enforcement purposes is permitted:[2]
✓ a warrant issued under a law of the Commonwealth, State or Territory
✓ reporting a digital ID fraud or cyber security incident (suspected or actual)
✓ with express consent for verifying identity or investigating/prosecuting an offence
✓ complying with the Digital ID Act
✓ proceedings have commenced against a person (for a Commonwealth, State or Territory offence or a breach of a law imposing a penalty or sanction).

[1] s 20E and s 21G of the Privacy Act and APPs 3, 6, 8 and 9.

[2] s 54 of the Digital ID Act *2024*. These circumstances also apply in regard to subsection 47(4)(e).

Disclosure of biometric information to law enforcement agencies

'Law enforcement agencies' has the same meaning as under the *Australian Crime Commission Act 2002*. It has a narrower meaning than an 'enforcement body' as set out above and includes:

- the Australian Federal Police;
- State police forces; and
- any authority or person responsible for the enforcement of the laws of the Commonwealth or the States.

However, it also includes entities such as the Australian Taxation Office (ATO), the Australian Securities and Investment Commission (ASIC) and the Australian Border Force. For example, the ATO is a law enforcement agency because it can prosecute certain offences under the *Taxation Administration Act 1953* and ASIC is a law enforcement agency because it enforces the *Australian Securities and Investments Commission Act 2001* including certain conduct amounting to criminal offences.[3]

Section 48 and subsection 49(3) of the Digital ID Act outline that an accredited entity must not disclose biometric information, held by an accredited entity, to a law enforcement agency, unless the disclosure is in the following circumstances:

Circumstances where disclosure of biometric information to a law enforcement agency is permitted:[4]
✓ a warrant issued under a law of the Commonwealth, a State or a Territory
✓ with express consent for verifying identity or investigating/prosecuting an offence.

Example: ID4U is an accredited entity offering digital ID verification services. Enforcement Body A requests both personal information and biometric information of a user for an investigation into corrupt practices.

ID4U evaluates the request and determines they can disclose personal information to Enforcement Body A under section 54(1)(b)(vi) of the Digital ID Act with the express consent of the individual. However, they determine that they cannot disclose any biometric information. According to subsection 49(3), biometric information can only be disclosed to law enforcement agencies (not enforcement bodies), such as the AFP under certain limited circumstances.[5]

[3] *Australian Crime Commission v AA Pty Ltd* (2006) FCAFC 30.

[4] s 49(3) of the Digital ID Act.

[5] For this example, Enforcement Body A is not a law enforcement agency as per the *Australian Crime Commission Act 2002*.

ID4U requests the express consent of the individual to share their personal information for the purpose of investigating an offence against a law of a State. The individual provides their consent.

Therefore, ID4U informs Enforcement Body A that they will provide the requested personal information but must decline the request for biometric information, adhering to the legal restrictions on such disclosures.