NSW GOVERNMENT

Statement of Public Interest
Tabled by... Ms. Tachas
...
for Clerk of the Parliaments
25/6/25

IDENTITY PROTECTION AND RECOVERY BILL 2025

STATEMENT OF PUBLIC INTEREST

Need: Why is the policy needed based on factual evidence and stakeholder input?

ID Support NSW (**IDS**) is a business unit within the NSW Department of Customer Service (**DCS**) that was established in 2021 as a specialised NSW Government service provider dedicated to supporting individuals, public sector agencies (**Agencies**), and private entities following a data compromise involving personal information, including government-issued identity documents.

Data compromises are a growing problem. The Australian Community Attitudes to Privacy Survey, completed by the Office of the Australian Information Commissioner in 2023, found that 47% of respondents had been notified by an organisation that their data was involved in a data breach in the year prior.

When individuals are impacted by a data compromise, particularly if their identity documents have been compromised, they are at risk of identity misuse. The Australian Institute of Criminology report 'Counting the costs of identity crime and misuse in Australia, 2018-19' found that identity crime cost Australia $3.1 billion that year, in direct and indirect costs, experienced by individual victims, businesses and Government.

IDS' services help to reduce these costs, by supporting Agencies and private entities that have experienced a compromise to respond quickly and appropriately, as well as helping individuals impacted by a data compromise to reduce the risk that their identity will be misused.

The current IDS operating model has been successful and is continuing to provide world-class support to Agencies, private sector entities and individuals. This has been reflected in the feedback received from entities that have utilised IDS's services as well as individuals who IDS has assisted.

Privacy legislation (such as the *Privacy and Personal Information Protection Act 1998* (**PPIP Act**), *Health Records and Information Privacy Act 2002* (**HRIP Act**)) and other secrecy provisions) generally prevent NSW Agencies from collecting, storing, using and disclosing personal and health information without consent of the individual to whom the information relates.

IDS has been operating under the ID Support NSW Privacy Code of Practice – identity remediation services (**Privacy Code**) since June 2022. The Privacy Code provides limited exemptions to some of the restrictions in the PPIP Act to allow IDS to provide identity protection and recovery services for the most part, to NSW Agencies.

However, the Privacy Code was only intended to be an interim measure until legislation could be enacted, as it is best practice to ensure that long-term functions that impact privacy and personal information protection are authorised by legislation. There were also some limitations in terms of what IDS can do under the Privacy Code, for example, in relation to the services that IDS can provide to private entities.

The *Identity Protection and Recovery Bill 2025* (the **Bill**) overcomes these limitations and broadens IDS' functions to include certain fraud control functions.

From November 2024 to January 2025, DCS consulted NSW Government agencies, relevant Commonwealth Government agencies and subject matter experts in privacy, security and inclusion.

There was a clear theme from the submissions, that is, IDS is an extremely important function that provides significant value to the people of NSW.

Objectives: What is the policy's objective couched in terms of the public interest?

The Bill establishes IDS as the core government provider of identity protection and recovery services and certain fraud control services within NSW; and provides statutory exemptions from the PPIP Act, HRIP Act, and other secrecy provisions that are necessary for these services.

The Bill does three key things:

1. Confers the identity protection functions on the Secretary of the Department administering the Bill (proposed to be DCS, with functions delegated to IDS staff). These functions enable IDS to advise and make recommendations to mitigate the risks of personal data compromise and assist organisations and individuals to respond to data compromises, including by assisting organisations to notify impacted individuals.

   The functions also enable IDS to establish a Compromised ID Register (the **Register**) and add identity documents that have or may have been compromised to the Register. Under the Bill, entities can then apply to be a 'fraud check user', enabling them to make queries with IDS about whether an identity document is on the Register or regarding the life status of an identity document holder (i.e. whether the person is known to have died).

2. Provides legislative authority for IDS to work with Agencies and other entities to exercise the identity protection functions, by providing:

   a. necessary exemptions from laws such as the PPIP Act, HRIP Act and secrecy provisions, and

   b. civil, criminal and disciplinary liability protections for disclosures that are made consistent with the Bill and, where necessary, a written agreement with IDS.

3. Provides the power to make regulations to support the functions established in the Bill, including to prescribe fees for the exercise of IDS' functions, and establishes an Identity Protection and Recovery Fund for payment of fees connected with IDS services.

There is a clear public interest in the Bill as it will allow IDS to support Agencies and private sector entities to respond to a data compromise, contributing to faster and more informative notifications to impacted individuals. This will help empower individuals to take action quickly to reduce their risks of identity misuse and financial harm. The Compromised ID Register and fraud checks will also help to reduce risks of identity misuse and financial harm to individuals, agencies and private entities.

Options: What alternative policies and mechanisms were considered in advance of the bill?

As an alternative to introducing legislation, the Government considered:

1. Continuing IDS' operation under the Privacy Code.

2. Private sector solutions to help organisations and individuals respond to data compromises.

Analysis: What were the pros/cons and benefits/costs of each option considered?

1. Continuing IDS' operation under the Privacy Code

IDS could continue operating in a limited manner under the Privacy Code.

Benefits

- The Privacy Code is in place and IDS has been operating under it since July 2022.

Costs

- The Privacy Code has significant limitations that prevent IDS from supporting Agencies, private entities and individuals:
  - The Privacy Code does not enable IDS to provide identity protection and recovery services where a data compromise is **suspected** but not yet confirmed to have occurred.
  - The Privacy Code does not enable fraud control services, such as the Register proposed in this Bill.
  - Privacy Codes are only able to modify the application of the Information Privacy Principles contained in the PPIP Act and cannot provide exemptions from other laws or liability protections. This means that IDS is unable to assist at the request of Agencies and private entities that hold health information under the HRIP Act or information subject to secrecy or confidentiality obligations.

These limitations have been addressed in the Bill.

2. Private sector solutions to help organisations and individuals respond to data compromises

There are some private sector service providers that offer support to organisations that have experienced a data compromise. These service providers include not-for-profit organisations and private consultancies, including law firms.

Benefits

- Could reduce the need for a Government service provider if there are enough affordable private sector providers to meet the growing demand for support and assistance following a data compromise.

Costs

- Private sector providers are limited in the assistance that they can provide, particularly as:
  - The PPIP Act, HRIP Act and other secrecy provisions may prevent Agencies from sharing personal and other sensitive information with private sector providers. Whereas, under this Bill, IDS can provide the same support to Agencies and private entities.
  - Private sector providers do not have the same access to other Agencies that play a critical role in responding to data compromises, such as Service NSW and Transport for NSW who provide updated contact information regarding impacted individuals, or NSW Police which has a partnership with IDS in responding to data compromises.
- Some private sector providers are reliant on government or community funding, creating uncertainty regarding ongoing availability of services. Whereas, the Bill allows regulations to establish a charging framework for services provided under the

Bill. This will ensure IDS is funded to provide its critical support to Agencies, private sector entities and individuals.

- Some private sector providers may be too costly for some organisations that experience a data compromise, for example small businesses and sole traders. This would limit the availability of identity protection and recovery and fraud control services for individuals impacted by a data compromise where an entity cannot afford to pay for private support services. Whereas IDS will ensure its charging framework is competitive and offers value-for-money. IDS will also continue to provide identity remediation and fraud control advice and education to the community and individuals impacted by a data compromise for free.

Pathway: What are the timetable and steps for the policy's rollout and who will administer it?

The Bill will commence on the date of assent and is proposed to be administered by the Minister for Customer Service and Digital Government.

The Bill enables regulations to be made. DCS will consult on draft regulations before they are made.

Consultation: Were the views of affected stakeholders sought and considered in making the policy?

DCS has engaged extensively with stakeholders on the Bill. From November 2024 to January 2025, DCS consulted NSW Agencies, relevant Commonwealth Government agencies and subject matter experts with expertise in privacy, security and inclusion, including the NSW Law Society and NSW Council for Civil Liberties.

DCS received and considered 23 written submissions on the Bill. Several changes were made to the Bill as a result of stakeholder feedback.