The Hon Michelle Rowland MP

Attorney-General
Federal Member for Greenway

Reference: MS26-000155

Senator the Hon Sue Lines
President of the Senate
Parliament House
CANBERRA ACT 2600

Dear President

I am writing in relation to the Senate Legal and Constitutional Affairs Legislation Committee report (report) on the Identity Verification Services Bill 2023 and the Identity Verification Services (Consequential Amendments) Bill 2023 (the Bills). I am pleased to confirm that the Government provided its response to the Committee's report on the Bills during debate in the Senate on 6 December 2023.

Senator the Hon Katy Gallagher provided the Government response to the report during debate in the Senate by tabling a supplementary explanatory memorandum, which directly addresses the Committee's recommendations.

All recommendations made in the Report were agreed to and implemented via amendments to the Bills. The relevant Hansard extract, supplementary explanatory memorandum and specific Parliamentary amendments evidencing the Government's response are enclosed for tabling.

I have copied Senator Jana Stewart, Chair of the Senate Legal and Constitutional Affairs Legislation Committee into this letter.

I trust this information is of assistance.

Yours sincerely

[redacted]

Michelle Rowland MP

11 / 3 /2026

Enc. *Extract from Hansard – Senate – 6 December 2023*
Supplementary Explanatory Memorandum
Parliamentary Amendments – Senate Debate

cc. Senator Jana Stewart, Chair, Senate Legal and Constitutional Affairs Legislation Committee

The Hon Michelle Rowland MP
PO Box 6022, Parliament House Canberra
Suite 101C, 130 Main Street, Blacktown NSW 2148 | (02) 9671 4780

The TEMPORARY CHAIR (Senator Chandler) (18:33): I will now deal with the amendment circulated by the opposition.

The CHAIR (18:33): The question is that the amendment on sheet 2286 be agreed to.

Opposition's circulated amendment—

(1) Schedule 1, item 5, page 25 (after line 25), at the end of Subdivision CA, add:

80.2N Review of this Subdivision

(1) The Minister must cause a review of the operation of this Subdivision to be undertaken as soon as possible after the end of 2 years after the commencement of this section.

(2) The person undertaking the review must give the Minister a written report of the review.

(3) The Minister must cause a copy of the report of the review to be tabled in each House of the Parliament within 15 sitting days of that House after the report is given to the Minister.

The committee divided. [18:36]

(The Chair—Senator McLachlan)

Ayes 21
Noes 27
Majority.....6

AYES

Antic, A.	Askew, W.	Babet, R.
Canavan, M. J.	Cash, M. C.	Chandler, C.
Davey, P. M.	Duniam, J. R.	Fawcett, D. J.
Hughes, H. A.	Kovacic, M.	Lambie, J.
McDonald, S. E.	McLachlan, A. L.	O'Sullivan, M. A. (Teller)
Rennick, G.	Reynolds, L. K.	Ruston, A.
Scarr, P. M.	Sharma, D. N.	Tyrrell, T. M.

NOES

Allman-Payne, P. J.	Ayres, T.	Bilyk, C. L.
Chisholm, A.	Gallagher, K. R.	Green, N. L.
Grogan, K.	Hanson-Young, S. C.	Lines, S.
McCarthy, M.	McKim, N. J.	O'Neill, D. M.
Payman, F.	Pocock, B.	Pocock, D. W.
Polley, H.	Pratt, L. C. (Teller)	Rice, J. E.
Sheldon, A. V.	Shoebridge, D.	Smith, M. F.
Sterle, G.	Stewart, J. N. A.	Urquhart, A. E.
Walsh, J. C.	Waters, L. J.	Whish-Wilson, P. S.

Question negatived.

Bill agreed to.

Bill reported without amendments; report adopted.

Third Reading

The DEPUTY PRESIDENT (18:38): The question now is that the remaining stages of the bill be agreed to and the bill be now passed.

Question agreed to.

Bill read a third time.

Identity Verification Services Bill 2023
Identity Verification Services (Consequential Amendments) Bill 2023

Second Reading

Consideration resumed of the motion:

That these bills be now read a second time.

Senator CASH (Western Australia—Deputy Leader of the Opposition in the Senate) (18:39): I rise to speak on the Identity Verification Services Bill 2023 and the Identity Verification Services (Consequential Amendments) Bill 2023. This legislation came forward in strange circumstances and was rushed into this place without warning. No-one knew it was coming, and certainly a major stakeholder in this area, that I had spoken to some time ago, was not aware that this legislation was coming; it was a shock to them. And it left many questions unanswered. But what it does do is deal with something very fundamental: the Document Verification Service that underpins the operation of many of our anti-money-laundering and counterterrorism-financing laws, and it also deals with like services.

As we made clear in the other place, we have no fundamental objection to putting those services onto a statutory footing. Let's go through, though, what those services are.

The Document Verification Service has been in operation since at least 2009 and open to the private sector since 2014. It is used by the Commonwealth, by state and territory government agencies and by the private sector to confirm that the details on a person's identity document, such as a driver's licence or passport, match the original record held by the government. The Face Verification Service allows a person's face to be biometrically matched to their driver's licence or passport photo. The Face Verification Service is currently in use and only used by Commonwealth agencies—for example, to set up a myGov account. The Face Identification Service will be a service which enhances law enforcement—in particular, in relation to undercover police—and will crossmatch photos biometrically against driver's licence photos to find potential matches. The Face Identification Service will be used solely to protect lawfully assumed identities. The driver's licence photos are provided by states and territories through a database called the National Driver Licence Facial Recognition Solution.

As I have already indicated, the coalition has never had an in-principle concern with putting these services on a legislative basis. The coalition is now in a position where we, on this side, can support the legislation, because of the very significant concessions that have been made by the government.

In that regard, I want to particularly call out the work of Senator Scarr. Senator Scarr led the coalition efforts in the inquiry into this bill, and his excoriating additional comments make clear that, as it was presented to the parliament, there were very significant shortfalls in the bill that the Attorney-General of Australia wanted us to agree to. Senator Scarr called for the bill to be rewritten to address his significant concerns.

I am pleased that the government has taken up Senator Scarr's work and has seen it as a wake-up call to indeed remedy the deficiencies that were in the bill that were initially presented to the parliament. In fact, in the wake of Senator Scarr's work, the Attorney-General's office reached out to engage with us on the passage of this bill. The approach was certainly late, but it was welcome. The Attorney-General and I have since exchanged letters about the basis upon which this bill should proceed. The Attorney-General has agreed to implement, as Senator Scarr had set out in his dissenting report, every one of the 11 substantive recommendations in the committee report. The Attorney-General has also agreed to the further changes that the coalition, both Senator Scarr and I, have requested.

The many changes that have been agreed, and the supporting work around the edges, have improved this legislation. The legislation is now in a position where the coalition can support it.

Senator SHOEBRIDGE (New South Wales) (18:44): The Identity Verification Services Bill 2023 and the Identity Verification Services (Consequential Amendments) Bill 2023 were rushed through by the government, for reasons that they have still not come clean about. The conclusion that pretty much every stakeholder has drawn is that the current identity verification services procedure is unlawful, and, in the absence of any statutory underpinning, is open to legal challenge. Unless that's is resolved rapidly by the government, they face, potentially, significant civil damages claims—potentially aggravated by the fact that they continue to operate a service knowing full well that it is unlawful, and in breach of, amongst other matters, the privacy laws. It would be useful, in terms of a frank exchange with the government if they would tell us, and also tell the Australian public. That kind of frankness should be expected from the government, particularly for service that's used some 120-odd million times a year and which involves the intimate personal details of pretty much every adult Australian. But we don't have that degree of transparency and clarity from the government, and I think that that's unfortunate, to say the least.

I commend the various stakeholders who engaged with the Senate inquiry into the Identity Verification Services Bill 2023 and who spent countless hours pointing out the deficiencies in the government's initial draft—the huge privacy gaps in the initial draft and the deeply problematic nature of its drafting. There were things as obvious as allowing implied consent when, on any valid privacy principle, if you're talking about sharing your biometric or other personal data, clearly, express consent is needed. There were things like ensuring clarity of drafting. There were very real and significant concerns about the bill, as drafted by the Attorney-General, and initially introduced into the parliament. That's why there were some 12 recommendations by the Legal and Constitutional Affairs Legislation Committee, ranging from ensuring that breaches of participation agreements can be dealt with properly through to ensuring that something as obvious as participation agreements be privacy-enhancing and consistent with

Australia's privacy principles; ensuring that an entity's legal obligations under privacy laws can't be watered down by agreements entered into under the scheme; ensuring that there are rule-making powers to actually enhance the privacy elements in the bill; and ensuring that there be an interim review—an urgent interim review—within 12 months of operation.

When dealing with such important issues as the private details of millions and millions of Australian citizens—details which are essential for obtaining financial services or for accessing the many essential services we now require through online activity, it's remarkable that the bill, as initially drafted, failed to deal with all of that. We had the benefit of incredibly detailed submissions from entities such as UNSW's Allen's Hub for Technology; Digital Rights Watch—and I particularly want to highlight the clarity of the evidence from Ms Lizzie O'Shea; the Law Council of Australia; the Australian Human Rights Commission; and the Human Technology Institute at UTS. It would also be wrong not to give a shout-out to Professor Ed Santow for the help he gave to the committee in his evidence.

The government having received not just the majority report but the excellent dissenting report from Senator Paul Scarr—which, I have to say, grappled with the complex evidentiary and legal issues and set out a roadmap for reform of the bill—and evidence from critical stakeholders, thankfully we now see a raft of amendments from the government that make this bill passable. It's far from perfect but probably, on balance, it's passable.

But that's not what the sector wants. It may be what the financial sector, the Australian Banking Association and the Attorney want, but it's not what the engaged stakeholders in the privacy space want. What they want is consistency in privacy laws. What they want is a set of privacy laws that will stand the test of time. One of the most extraordinary things about this little legislative venture from the Attorney-General was that, whilst the Identity Verification Services Bill 2023 was working through one track with very inadequate privacy protections in it—no doubt they would have been cutting-edge in 1983 but they don't cut the mustard in 2023—the draft Digital ID Bill 2023, which had substantially higher privacy protections, was going through under another minister. There was a draft digital ID bill out on public exhibition with substantially higher privacy protections. They were much closer to what you'd expect in 2023 in the draft Digital ID Bill, which was out on consultation at the same time as the government was trying to force through the Identity Verification Services Bill. The stakeholders said to do them together—do them once and make them coherent. For that reason, we have a second reading amendment that aims to do just that—to defer this bill until we can have a coherent set of privacy reforms and do the two bills together as core business in the first half of next year. If that doesn't succeed, then we will with some reluctance support the bill, but only because of the very significant amendments that have been drafted.

I raise one significant issue that we would normally address in committee but that, given the guillotine motion that's been moved today, there won't be an opportunity for—that is, the Greens amendments to prohibit the identity verification system from collecting or disseminating protected information. Protected information is information about an individual's health, criminal record, membership of a professional or trade association, membership of a trade union, racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, sexual orientation or practices, or disability status. For the Greens, this is a critical amendment. Information of this nature should never find its way into a federal database about us. We'll be moving amendments to expressly prohibit this information being captured or disseminated through the identity verification services process, and we would expect wholehearted cross-party support for those amendments.

We understand that the government won't support them, because they say that there's a policy in place, that they don't collect this stuff about us now, and that this bill isn't really about limiting what information we can use; it's just about making it happen. That bells the cat for us. That raises concerns for us. There should be clear legal constraints preventing critical information, which we've outlined in our amendments, ever being collected under this system, held by the government and distributed under this system.

We would urge members in this chamber to have close regard to those amendments and think, 'Do I want the next government to be collecting this information about us?' Do you want to have the protections just founded under policy which can be changed from Attorney-General to Attorney-General? Why not make it clear in black and white that this is information the government should not be collecting about us, should not be storing about us and should not be disseminating about us. I note the time, and I know other senators have contributions, so I'll conclude my observations there. I move a second reading amendment:

Omit all words after "that", substitute "further consideration of this bill be postponed until the Government's comprehensive privacy reforms are available to ensure the best possible privacy protections are in place for personal information".

Senator SCARR (Queensland—Deputy Opposition Whip in the Senate) (18:55): I will speak very briefly on the Identity Verification Services Bill 2023 because I know other senators want to speak, and there's not much time to speak. I will make three points.

The first point is in relation to timing of the process. The Law Council of Australia said:

It is troubling that such a short reporting period has been imposed on this inquiry, providing a little over two weeks for stakeholders to make submissions about a proposed legislative framework for identity verification services …

… … …

The Law Council is concerned that the timeframe for this inquiry does not reasonably enable the Committee to carefully scrutinise whether the Bills strike the correct balance.

It is very disturbing when the Law Council of Australia makes that comment with respect to a process.

The second point I will make is again a quote from the Law Council of Australia. I think the government needs to reflect on this as it takes forward its review of the Privacy Act and also of the Digital ID Bill. The Law Council said:

As a general comment, the fragmented approach to privacy and data reform that is illustrated by these bills is not conducive to promoting harmonisation and clarity across Australia's digital identity, privacy and identity verification frameworks. The Law Council reiterates its call for a roadmap of the harmonisation of Australia's privacy and data laws to ensure the development of a national privacy framework that is consistent, clear and accessible.

The government would do well to heed those words. My colleague Senator Shoebridge, who makes an outstanding contribution on the Legal and Constitutional Affairs committees on which I serve with him, raised the issue of consent. Can I just say that expressed consent is one thing, but it also can't be Hobson's choice. It's got to be a real choice for people with respect to these matters.

The last point is to thank the members of the Attorney-General's Department for their work in relation to the bill. There were a lot of amendments that had to be made in a short period of time, and it was a pleasure to engage with them through the committee process, so thank you very much. I acknowledge Senator Anita Green for her chairing of the Legal and Constitutional Affairs Legislation Committee. We have robust debate, but she always chairs it very well. Lastly, I would like to acknowledge the input from Ms Shohini Sengupta, of the University of New South Wales Allens Hub for Technology, Law and Innovation, and also Ms Olga Ganopolsky, the chair of the Privacy Law Committee of the Business Law Section of the Law Council of Australia.

Senator ROBERTS (Queensland) (18:58): One Nation strongly opposes the Identity Verification Services Bill 2023. Here's why. The Albanese government's great mate, Blackrock boss Larry Fink, and predatory billionaires at the World Economic Forum are fond of the phrase 'you will own nothing and be happy'. What they really mean is that they will own everything and you will comply. Why would people voluntarily enslave themselves, give up their homes, cars and household goods and lose the right to travel freely, I hear you ask. The answer is that people will not be given a choice. They will be coerced—forced into it. That's the purpose of this government's triad of tyranny. First is the Identity Verification Services Bill 2023, which will normalise and allow the use of biometric data to locate and track citizens. Second is the Digital ID Bill 2023, which will force every Australian into having a digital ID. Third is the Misinformation and Disinformation Bill 2023, which will ensure media and social media only carry government sanctioned opinions; the government will be exempted and can be free to spread misinformation and disinformation.

Biometric data is your face turned into a data file based on your physical characteristics. It allows for faster and more accurate identification. They will capture your face. The national drivers licence database is being upgraded to become the repository of your master identification record, which is already used to establish your identity with a paper check. Now it will have a facial scan.

Australians do not need to consent in a meaningful manner. The bill currently uses the word 'consent' without definition. Consent can be implied. Here's an example. If a person sees a video of themselves on a self-service check-out at the supermarket and uses the check-out anyway, it's considered implied consent. The government has accepted that implied consent is no consent at all and has upgraded the reference to 'consent' in their amendment on sheet UD100 to 'explicit consent'. That isn't good enough either. Explicit consent can be provided as blanket consent. An example would be MasterCard changing their terms and conditions to allow for facial recognition whenever their card is used. Once the card owner gets the email saying, 'We have updated our terms and conditions. Click here to approve,' and people click without reading it, one of those new terms could be permission for facial recognition. Did you give consent? No.

Banks currently record the image of anyone using their ATMs and then use that in the case of a fraudulent transaction. Banks will update their terms and conditions to give themselves the right to run your biometric verification on each occasion before allowing access to your account. Refusing the new permission gives your bank or card company the right to refuse service. It's that simple. It's blackmail. This is why the government suggesting a digital ID or biometric data check will be voluntary is a complete lie. It's compulsory, because not agreeing means

you lose your bank account or payment card or service—just as those voluntary COVID injections were compulsory if you wanted to keep your job and your house and feed your family.

I foreshadow an amendment in the committee stage on sheet 2327 to change the definition of 'explicit' to 'active', meaning on each occasion your face is to be scanned they must ask permission before they scan it and make sure they get your permission each time. That's active consent. This should be supported, because the government already says Australians will have to consent to their biometric data being used—unless, of course, that was misinformation.

This bill does not offer a direct link between the authentication action at a check-out, office, airport et cetera and the master file. A government hub receives a request and pulls the master file, meaning only the government has access to the master file. This seems to look acceptable, yet it means there's a master file with 17 million records containing name, address, telephone, date of birth, drivers licence number, passport number and a biometric identification file all sitting in the same database. That's all the information necessary to steal someone's ID and impersonate them online—a hacker's paradise.

Robodebt proved that our bureaucrats are incapable of even a simple one-to-one database match, and now they're being trusted to pull this off. It's impossible without a high level of compulsion and without completely ignoring victims of software or data-matching errors. If the look-up fails, then your purchase, travel, document, signing or whatever other use fails. If the purchase was for petrol, your family could be stranded late at night. We might as well start the royal commission now.

Downstream from the big government database are what I call intermediaries or entities with participating agreements. There are 20 of these so far. Their role is to take a request for authentication from a bank or card processor, solicitor, real estate agent, airline—anyone needing you to prove you are who you say you are—and submit that to the national drivers licence database hub to run past the master database. In the original bill there were no effective checks and balances on those businesses. The government's amendment of its own bill has added a few checks and balances to ensure that intermediaries must delete data received as part of the verification process. Thank you, Minister Gallagher. That, taken together with my amendment to make the level of consent clear, takes some of the potential abuse out of the bill. A clear privacy statement would have helped. The government have promised they will do that later. There are trust issues around that promise.

Questions remain around the New South Wales government's comment that this bill will allow them to verify that every person detected driving a car past a surveillance camera has a drivers licence. The only way this can be achieved is if every driver is scanned every time they pass a detection camera and their image is compared to the national database. Does this mean those cameras going up around Australia are just the right height to scan the driver's face and that the cameras will be used to scan and verify your identity each time you pass one? Yes, it does. Before they work out who you are and whether you have a licence, they have to scan and verify your biometrics. It's the only explanation for the New South Wales government's comment.

For those listening to this with incredulity, I remind you that this is exactly the system now in place in London, with Lord Mayor Khan's ULEZ, Ultra Low Emission Zone, and in Birmingham, Manchester and other cities in Britain. It's really the World Economic Forum's 15-minute cities happening right now. Residents are locked into their zone and can only leave a certain number of times a year. This is happening in Britain. That depends on the make and model of the car you drive. If you drive a car they don't like, you can't move. Rich people who can afford electric cars can, of course, come and go as they please. Everyday citizens are locked in or, when they leave, the cameras detect them leaving and fine them on the spot. It's a fine of 180 pounds a week for leaving over seven days. That's in Britain now. Already it has raised hundreds of millions of pounds because people will pay for freedom. Look it up. Don't just trust me: look it up. There are fines for not registering with the system and fines for breaching the 15-minute limits. It's a virtual fence. It's like an electric dog collar. It's the foundation for a social credit system to completely control people's lives. So don't tell me this is a conspiracy theory. It's real and it's happening now in our mother country.

Cash is necessary to ensure these measures are ameliorated as much as possible, which is why the globalist wing of the Liberal Party tried to ban cash in the last parliament, which One Nation defeated. It should be obvious that predatory, parasitic billionaires and some of their lackeys in the Labor and Liberal Party are getting their ducks in a row because they want to be ready for the full implementation of their globalist masters' control agenda, exactly as they promised. It's not like they're hiding any of this. When they tell us what they're going to do, listen.

Remember this government's triad of tyranny. Already entered into parliament is the Identity Verification Services Bill 2023 to normalise and allow the use of biometric data to locate and track citizens. Here it is. There's the Digital ID Bill 2023 to force every Australian into having a digital ID. There's the misinformation and disinformation bill 2023, which will ensure media and social media only carry government sanctioned opinions,

and the government is exempted. I implore the Senate to vote against this bill and to reject this bill. This is the first of three bills necessary to turn Australia into the world's first World Economic Forum digital prison.

Senator CANAVAN (Queensland) (19:08): Senator Roberts has rightly outlined the serious concerns with privacy in the Identity Verification Services Bill 2023 that were similarly outlined to the Senate committee on this bill. Digital rights campaigners are aghast at the government, which is proceeding with this massive expansion of a surveillance state without introducing related reforms to the Privacy Act that would protect people's data when it's centralised with a government that will be unaccountable now because of these changes.

Nothing demonstrates more why we should oppose this bill tonight than that the government has allotted the sum total of 30 minutes for debate. One of the most significant pieces of legislation to come before our parliament this year, massively expanding the amount of power and surveillance the state has over Australian citizens and individuals, has been given the sum total of 30 minutes for debate. I will not get to make the normal 15-minute contribution here because I rose with just one minute left on the clock. The government is trying to gag any opposition to this bill because it cannot defend why it needs to collect so much data on law-abiding Australian citizens in this country.

The ACTING DEPUTY PRESIDENT (Senator Walsh): Senators, in accordance with the resolution agreed to earlier today, the time for consideration of the Identity Verification Services Bill 2023 and a related bill has expired. After I have put the question before the chair, I will then put the questions on the remaining stages of the bills. The question is that the second reading amendment on sheet 2158, moved by Senator Shoebridge, be agreed to.

Question negatived.

Senator SHOEBRIDGE (New South Wales) (19:10): by leave—We don't want a division on this, but we want our position recorded.

Senator ROBERTS (Queensland) (19:10): by leave—Could I have my name recorded as supporting the Greens' amendment on sheet 2158 please.

The ACTING DEPUTY PRESIDENT (Senator Walsh): The question now is that these bills be now read a second time.

Question agreed to.

Bills read a second time.

The ACTING DEPUTY PRESIDENT (Senator Walsh): I will now deal with the Committee of the Whole amendments, starting with the amendments circulated by the government. I understand the minister has documents to table.

Senator GALLAGHER (Australian Capital Territory—Minister for the Public Service, Minister for Finance, Minister for Women, Manager of Government Business in the Senate and Vice-President of the Executive Council) (19:11): I table a supplementary explanatory memorandum relating to the government amendments to the bill.

The ACTING DEPUTY PRESIDENT (Senator Walsh): I will first deal with the Committee of the Whole amendments to the Identity Verification Services (Consequential Amendments) Bill 2023 on sheet UD100. The Australian Greens have circulated amendments to government amendments (31) and (35). The question is that the Australian Greens amendments on sheet 2326 to government amendments (31) and (35) be agreed to.

Australian Greens' circulated amendments—

(1) Amendment (31), omit the amendment, substitute:

"(31) Clause 36, page 41 (lines 16 to 18), omit "A review of the operation of this Act and the provision of identity verification services must be started within 2 years. A report of the review must be tabled in Parliament.", substitute "An interim review and review of this Act must be conducted."."

(2) Amendment (35), subclause 43(1A), omit "as soon as practicable after 12 months, and before the end of 2 years,", substitute "within 12 months".

(3) Amendment (35), after paragraph 43(1B)(a), insert:

(aa) any other law of the Commonwealth that regulates privacy, facial recognition or biometric data, to the extent that the other law is relevant to this operation of this Act; and

Question negatived.

The ACTING DEPUTY PRESIDENT: Pauline Hanson's One Nation have circulated amendments to government amendments (8) and (27). The question is that the Pauline Hanson's One Nation amendments on sheet 2327 to government amendments (8) and (27) be agreed to.

Pauline Hanson's One Nation's circulated amendments—

(1) Amendment (8), omit the amendment, substitute:

"(8) Clause 9, page 16 (line 32), omit "consent to", substitute "active express consent to each instance of"."

(2) Amendment (27), omit the amendment, substitute:

"(27) Clause 35, page 39 (line 20), omit "consented to", substitute "actively and expressly consented to each instance of"."

The Senate divided. [19:16]

(The Acting Deputy President—Senator Walsh)

Ayes 6
Noes 33
Majority.....27

AYES

Antic, A.	Babet, R.	Canavan, M. J.
Hanson, P. L.	Rennick, G.	Roberts, M. I. (Teller)

NOES

Allman-Payne, P. J.	Ayres, T.	Bilyk, C. L.
Cash, M. C.	Chisholm, A.	Gallagher, K. R.
Green, N. L.	Grogan, K.	Hanson-Young, S. C.
Henderson, S. M.	Lambie, J.	McCarthy, M.
McGrath, J.	McKim, N. J.	O'Neill, D. M.
O'Sullivan, M. A. (Teller)	Payman, F.	Pocock, B.
Pocock, D. W.	Polley, H.	Pratt, L. C.
Rice, J. E.	Scarr, P. M.	Sheldon, A. V.
Shoebridge, D.	Smith, M. F.	Sterle, G.
Stewart, J. N. A.	Tyrrell, T. M.	Urquhart, A. E.
Walsh, J. C.	Waters, L. J.	Whish-Wilson, P. S.

Question negatived.

The ACTING DEPUTY PRESIDENT (Senator Walsh) (19:18): The question now is that the government amendments on sheet UD100 be agreed to.

Government's circulated amendments—

(1) Clause 2, page 2 (lines 2 to 9), omit subclause (1), substitute:

(1) Each provision of this Act specified in column 1 of the table commences, or is taken to have commenced, in accordance with column 2 of the table. Any other statement in column 2 has effect according to its terms.

Commencement information

Column 1	**Column 2**	**Column 3**
Provisions	**Commencement**	**Date/Details**
1. Sections 1 to 14 and anything in this Act not elsewhere covered by this table	The day after this Act receives the Royal Assent.	
2. Sections 15 to 41	The earlier of: (a) the commencement of rules made under section 44 of this Act; and (b) the start of the day after the end of the period of 6 months beginning on the day this Act receives the Royal Assent.	
3. Section 42	The day after this Act receives the Royal Assent.	
4. Section 43	At the same time as the provisions covered by table item 2.	
5. Section 44	The day after this Act receives the Royal Assent.	

Note: This table relates only to the provisions of this Act as originally enacted. It will not be amended to deal with any later amendments of this Act.

(2) Clause 3, page 3 (after line 4), at the end of the clause, add:

Note: The objects in paragraphs 3(a), (b) and (d) are authorised and provided for by Parts 2, 3 and 5. In accordance with the object in paragraph 3(c), Part 4 prohibits the use or disclosure of, or access to, identification information, unless it is in accordance with the objects of this Act or in other limited circumstances.

(3) Clause 4, page 4 (after line 21), after the paragraph beginning "Those requests", insert:

Part 4 of this Act prohibits the use or disclosure of, or access to, identification information, unless it is in accordance with the objects of this Act or in other limited circumstances.

(4) Clause 5, page 8 (lines 9 to 12), omit the definition of ***IGIS official***.

(5) Clause 5, page 9 (lines 9 to 13), omit the definition of ***Ombudsman official***.

(6) Clause 6, page 14 (after line 6), at the end of the clause, add:

Identification information taken to be personal information

(6) Identification information is taken to be personal information for the purposes of the *Privacy Act 1988*.

(7) Clause 7, page 15 (line 9), omit "consent", substitute "express consent".

(8) Clause 9, page 16 (line 32), omit "consent", substitute "express consent".

(9) Clause 9, page 17 (line 7), omit "consent", substitute "express consent".

(10) Clause 9, page 17 (line 23), at the end of subclause (2), add:

; and (g) the Department to notify each party to the agreement that is relevant to, or impacted by, a data breach of which the Information Commissioner is informed under paragraph (f); and

(h) each party notified under paragraph (g) of a data breach, that is impacted by that breach, to take reasonable steps to notify each individual to whom the identification information relates.

(11) Clause 9, page 17 (line 25), omit "consent", substitute "express consent".

(12) Clause 9, page 18 (after line 9), at the end of the clause, add:

(4) A participation agreement must provide that a party to the agreement is not authorised to use or disclose identification information obtained for the purposes of requesting or providing identity verification services for the purposes of any of the following:

(a) engaging in activities that would allow the party to create a data profile of the person whose identity is being verified (including where it would allow the person's behaviour to be tracked (whether or not online));

(b) offering to supply goods or services;

(c) advertising or promoting goods or services;

(d) enabling another person or entity to offer to supply goods or services;

(e) enabling another person or entity to advertise or promote goods or services;

(f) market research.

(13) Clause 10, page 18 (after line 33), after paragraph (2)(a), insert:

(aa) if the identity verification service is an FVS—to take reasonable steps to destroy each facial image of an individual that is created, for the purposes of the request, by the party requesting the service, as soon as reasonably practicable after the image is no longer required for the purposes of the request, unless the image is:

(i) a Commonwealth record (within the meaning of the *Archives Act 1983*); or

(ii) required by a law of the Commonwealth, a State or a Territory, or by an order of a court or tribunal, to be retained; and

(14) Page 19 (after line 12), after clause 10, insert:

10A Failure to comply with participation agreements

(1) This section applies if:

(a) a party to a participation agreement is subject to the *Privacy Act 1988*; and

(b) an act or practice of the party, relating to personal information about an individual, does not comply with a requirement of:

(i) the agreement in relation to a matter covered by section 9 or 10 (other than paragraph 10(1)(b)) of this Act; or

(ii) rules prescribed for the purposes of subsection 44(1A) of this Act.

(2) For the purposes of the *Privacy Act 1988*, the act or practice is taken to be:

(a) an interference with the privacy of the individual; and

(b) covered by sections 13 and 13G of that Act.

(15) Clause 12, page 19 (line 29), after "agreement", insert ", rules made for the purposes of subsection 44(1A),".

(16) Clause 12, page 19 (after line 30), at the end of the clause, add:

Note: Under subsection 44(1A), the rules may prescribe requirements relating to privacy with which a party to a participation agreement must comply.

(17) Clause 15, page 24 (line 6), omit "12 months", substitute "the period specified by subsection (3)".

(18) Clause 15, page 24 (after line 11), at the end of the clause, add:

(3) For the purposes of subsection (2), the period is:

(a) 12 months; or

(b) if the rules prescribe a longer period of up to 18 months for the purposes of this paragraph—that longer period.

(19) Clause 23, page 30 (line 5), omit "The Department", substitute "In accordance with the object of this Act covered by paragraph 3(a), the Department".

(20) Clause 26, page 31 (line 5), omit "The Department", substitute "In accordance with the object of this Act covered by paragraph 3(b), the Department".

(21) Clause 29, page 35 (before line 4), before the paragraph beginning "Current and former", insert:

An object of this Act is to protect identification information communicated to approved identity verification facilities, and certain other information relating to the use or security of those facilities.

This Act does this by prohibiting the use or disclosure of, or access to, identification information, unless it is in accordance with the objects of this Act or in other limited circumstances.

(22) Clause 29, page 35 (lines 20 and 21), omit "an IGIS official or Ombudsman official", substitute "an official of an integrity agency".

(23) Clause 29, page 35 (line 22), omit "consent", substitute "express consent".

(24) Heading to Division 2, page 36 (lines 1 and 2), omit the heading, substitute:

Division 2—Prohibition on recording or disclosure of, or access to, information by entrusted persons

(25) Heading to clause 30, page 36 (line 3), omit the heading, substitute:

30 Prohibition on recording or disclosure of, or access to, information by entrusted persons

(26) Clauses 33 and 34, page 39 (lines 1 to 15), omit the clauses, substitute:

33 Information communicated etc. to integrity agencies

(1) An entrusted person may disclose protected information if:

(a) the disclosure is to any of the following persons:

(i) the Inspector-General of Intelligence and Security, or a person covered by subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986*;

(ii) the Commonwealth Ombudsman, or another officer (within the meaning of subsection 35(1) of the *Ombudsman Act 1976*);

(iii) the Information Commissioner, a member of the staff of the Office of the Information Commissioner, or a consultant engaged under the *Australian Information Commissioner Act 2010*;

(iv) the National Anti-Corruption Commissioner, or another staff member of the NACC (within the meaning of the *National Anti-Corruption Commission Act 2022*);

(v) the Inspector of the National Anti-Corruption Commission, or a person assisting the Inspector (within the meaning of the *National Anti-Corruption Commission Act 2022*); and

(b) the disclosure is for the purpose of that person exercising a power, or performing a function or duty.

(2) An entrusted person may make a record of or access protected information for the purpose of disclosing the protected information under subsection (1).

(27) Clause 35, page 39 (line 20), omit "consented", substitute "expressly consented".

(28) Clause 35, page 39 (line 30), omit "consents", substitute "expressly consents".

(29) Clause 36, page 41 (before line 4), before the paragraph beginning "The Secretary may delegate", insert:

An object of this Act is to provide for oversight and scrutiny of the operation and management of the approved identity verification facilities. This Part provides for that oversight and scrutiny, as well as dealing with other miscellaneous matters.

(30) Clause 36, page 41 (lines 10 and 11), omit "the operation and management of".

(31) Clause 36, page 41 (lines 16 to 18), omit "A review of the operation of this Act and the provision of identity verification services must be started within 2 years. A report of the review must be tabled in Parliament.", substitute "An interim review and review of this Act must be conducted, both of which must be started within 2 years of the commencement of section 43 of this Act.".

(32) Clause 40, page 43 (lines 13 to 15), omit paragraph (1)(a), substitute:

(a) assessing the approved identity verification facilities in relation to any act or practice of the Department during the financial year;

(33) Clause 40, page 43 (lines 17 to 22), omit subclauses (2) and (3), substitute:

(2) For the purposes of the *Privacy Act 1988*, an assessment under subsection (1) of this section is taken to be an assessment under paragraph 33C(1)(a) of that Act.

(34) Heading to clause 43, page 46 (lines 18 and 19), omit the heading, substitute:

43 Interim review, and review of this Act and provision of identity verification services

(35) Clause 43, page 46 (before line 20), before subclause (1), insert:

Interim review

(1A) The Minister must cause an interim review to be started as soon as practicable after 12 months, and before the end of 2 years, of the commencement of this section.

(1B) The interim review must consider the adequacy and operation of:

(a) the privacy protections contained in this Act; and

(b) the security requirements and obligations contained in this Act; and

(c) the penalties for non-compliance with obligations set out in participation agreements, including considering whether civil penalties should apply.

Review of Act and provision of identity verification services

(36) Clause 43, page 46 (before line 23), before subclause (2), insert:

Consultation, preparation and tabling of reports

(2A) The President of the Australian Human Rights Commission, the Human Rights Commissioner appointed under section 8B of the *Australian Human Rights Commission Act 1986*, and the Information Commissioner, must be consulted in relation to a review under subsection (1A) or (1).

(37) Clause 44, page 47 (after line 4), after subclause (1), insert:

(1A) Without limiting subsection (1), the rules may prescribe requirements relating to privacy with which a party to a participation agreement must comply.

Consultation on draft rules

(1B) Before making or amending any rules under subsection (1), the Minister must:

(a) cause to be published on the Department's website a notice:

(i) setting out the draft rules or amendments; and

(ii) inviting persons to make submissions to the Minister about the draft rules or amendments within the period specified in the notice (which must be at least 28 days after the notice is published); and

(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; and

(c) consider any submissions received within the specified period.

(1C) The Minister may consider any submissions received after the specified period if the Minister considers it appropriate to do so.

Limitation on rules

(38) Clause 44, page 47 (before line 14), before subclause (3), insert:

Disallowance and sunsetting of rules

Question agreed to.

The ACTING DEPUTY PRESIDENT: I will now deal with the amendments circulated by the Australian Greens. The question is that the amendments on sheet 2157 revised be agreed to.

Australian Greens' circulated amendments—

(1) Clause 5, page 9 (after line 19), after the definition of ***protected information***, insert:

restricted information of an individual means:

(a) health information (within the meaning of the *Privacy Act 1988*) about the individual; or

(b) information or an opinion about the individual's criminal record; or

(c) information or an opinion about the individual's membership of a professional or trade association; or

(d) information or an opinion about the individual's membership of a trade union; or

(e) other information or opinion that is associated with an individual and is prescribed by the rules; or

(f) information or an opinion about the individual's:

(i) racial or ethnic origin; or

(ii) political opinions; or

(iii) membership of a political association; or

(iv) religious beliefs or affiliations; or

(v) philosophical beliefs; or

(vi) sexual orientation or practices; or

(vii) disability status.

(2) Clause 23, page 30 (after line 11), at the end of the clause, add:

However, the Department must not collect, use or disclose restricted information of an individual in developing, operating and maintaining approved identity verification facilities.

(3) Clause 25, page 30 (line 27), at the end of the clause, add:

; and (c) not collect, use or disclose information that is restricted information of an individual.

(4) Clause 26, page 31 (after line 18), at the end of the clause, add:

However, the Department must not collect, use or disclose identification information that is restricted information of an individual for any of those purposes.

(5) Page 34 (after line 12), at the end of Division 2, add:

28A Collection, use and disclosure of restricted information of individuals

Despite sections 27 and 28, the Department must not collect, use or disclose identification information that is restricted information of an individual.

The Senate divided. [19:20]

(The Acting Deputy President—Senator Walsh)

Ayes 8
Noes 30
Majority.....22

AYES

Allman-Payne, P. J.	Hanson-Young, S. C.	McKim, N. J. (Teller)
Pocock, B.	Rice, J. E.	Shoebridge, D.
Waters, L. J.	Whish-Wilson, P. S.	

NOES

Antic, A.	Ayres, T.	Babet, R.
Bilyk, C. L.	Canavan, M. J.	Cash, M. C.
Chisholm, A.	Gallagher, K. R.	Green, N. L.
Grogan, K.	Hanson, P. L.	Henderson, S. M.
Lambie, J.	McCarthy, M.	McGrath, J.
O'Neill, D. M.	O'Sullivan, M. A. (Teller)	Payman, F.
Pocock, D. W.	Polley, H.	Pratt, L. C.
Roberts, M. I.	Scarr, P. M.	Sheldon, A. V.
Smith, M. F.	Sterle, G.	Stewart, J. N. A.
Tyrrell, T. M.	Urquhart, A. E.	Walsh, J. C.

Question negatived.

The ACTING DEPUTY PRESIDENT (Senator Walsh) (19:22): I will now deal with the government amendment to the Identity Verification Services (Consequential Amendments) Bill 2023. The question is that the amendment on sheet UD102 be agreed to.

Government's circulated amendment—

(1) Clause 2, page 2 (table item 1), after "commencement of", insert "section 24 of".

Question agreed to.

Third Reading

The ACTING DEPUTY PRESIDENT (Senator Walsh) (19:23): The question now is that the remaining stages of the bills be agreed to and the bills be now passed.

The Senate divided. [19:24]

(The Acting Deputy President—Senator Walsh)

Ayes 32
Noes 6
Majority.....26

AYES

Allman-Payne, P. J.	Ayres, T.	Bilyk, C. L.
Cash, M. C.	Chisholm, A.	Gallagher, K. R.
Green, N. L.	Grogan, K.	Hanson-Young, S. C.
Henderson, S. M.	Lambie, J.	McCarthy, M.
McKim, N. J.	O'Neill, D. M.	O'Sullivan, M. A.
Payman, F.	Pocock, B.	Pocock, D. W.
Polley, H.	Pratt, L. C. (Teller)	Rice, J. E.
Scarr, P. M.	Sheldon, A. V.	Shoebridge, D.
Smith, M. F.	Sterle, G.	Stewart, J. N. A.
Tyrrell, T. M.	Urquhart, A. E.	Walsh, J. C.
Waters, L. J.	Whish-Wilson, P. S.	

NOES

Antic, A.	Babet, R. (Teller)	Canavan, M. J.
Hanson, P. L.	Rennick, G.	Roberts, M. I.

Question agreed to.

Bills read a third time.

Interactive Gambling Amendment (Credit and Other Measures) Bill 2023

Second Reading

Consideration resumed of the motion:

That this bill be now read a second time.

The ACTING DEPUTY PRESIDENT (Senator Walsh) (19:26): I will now put the questions on the remaining stages of the Interactive Gambling Amendment (Credit and Other Measures) Bill 2023.

Senator HENDERSON (Victoria) (19:27): I seek leave to have my speech incorporated into *Hansard*.

Leave not granted.

The ACTING DEPUTY PRESIDENT (Senator Walsh) (19:27): I will first deal with the second reading amendment circulated by Senator David Pocock. The question is that the second reading amendment on sheet 2259 be agreed to.

Senator David Pocock's circulated amendment—

At the end of the motion, add ", but the Senate:

(a) commits to diminishing the political influence of the online wagering industry, in the interests of protecting Australians and harm reduction strategies from industry influence; and

(b) calls on all politicians and all political parties to stop accepting political donations from the online wagering industry and revoke any passes that they have sponsored for members of the industry, and their agents, to access Parliament House".

The Senate divided. [19:28]

(The Acting Deputy President—Senator Walsh)

Ayes 11
Noes 24
Majority.....13

2022-2023

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

SENATE

IDENTITY VERIFICATION SERVICES BILL 2023

IDENTITY VERIFICATION SERVICES (CONSEQUENTIAL AMENDMENTS) BILL 2023

SUPPLEMENTARY EXPLANATORY MEMORANDUM

Amendments to be Moved on Behalf of the Government

(Circulated by authority of the

Attorney-General, the Hon Mark Dreyfus KC MP)

GLOSSARY

The following abbreviations and acronyms are used throughout this Explanatory Memorandum.

Abbreviation	***Definition***
AHRC Act	*Australian Human Rights Commission 1986* (Cth)
APP	Australian Privacy Principle
Bill	Identity Verification Services Bill 2023
Consequential Amendments Bill	Identity Verification Services (Consequential Amendments) Bill 2023
Crimes Act	*Crimes Act 1914*
Criminal Code	*Criminal Code Act 1995*
Department	the department responsible for administering the Act to be established by the Bill
DVS	Document Verification Service
FIS	Face Identification Service
FVS	Face Verification Service
ICCPR	International Covenant on Civil and Political Rights
Information Commissioner	Australian Information Commissioner
NACC	National Anti-Corruption Commission
NDLFRS	National Drivers Licence Facial Recognition Solution
OAIC	Office of the Australian Information Commissioner
Ombudsman Act	*Ombudsman Act 1976*
Privacy Act	*Privacy Act 1988*
Senate Committee	Senate Standing Committee on Legal and Constitutional Affairs Legislation Committee

AMENDMENTS TO THE IDENTITY VERIFICATION SERVICES BILL 2023 AND IDENTITY VERIFICATION SERVICES (CONSEQUENTIAL AMENDMENTS) BILL 2023 (Government)

GENERAL OUTLINE

1. The purpose of the amendments to the Identity Verification Services Bill 2023 is to implement the Government's response to recommendations from the Senate Legal and Constitutional Affairs Legislation Committee's inquiry into the Bill and the Identity Verification Services (Consequential Amendments) Bill. The Senate Committee handed down the report of its inquiry on 9 November 2023. The amendments will also address issues raised by stakeholders, including during the Committee's inquiry.

2. The amendments will enhance existing privacy safeguards, oversight and transparency arrangements, including by clarifying the application of the Privacy Act and the role of the Information Commissioner, by:

    - ensuring that the annual assessment at clause 40 aligns with, and leverages, the Information Commissioner's existing assessment functions and powers in the Privacy Act

    - better aligning the requirements that must be set out in participation agreements regarding data breaches with the requirements in the Notifiable Data Breaches scheme under Part IIIC of the Privacy Act

    - requiring express consent, rather than allowing for implied consent

    - specifying the acts or practices of a party to a participation agreement which constitutes an 'interference with privacy of the individual' for the purposes of the Privacy Act

    - clarifying that identification information, as defined in clause 6 of the Bill, is personal information for the purposes of the Privacy Act

    - requiring parties to a participation agreement to take reasonable steps to destroy a facial image that was collected to request the use of the Face Verification Service if it is no longer required for that purposes, unless the image is a Commonwealth record, or is required by law or court or tribunal

    - ensuring that entrusted persons are authorised to disclose protected information to Commonwealth integrity agencies, including the Information Commissioner, and the National Anti-Corruption Commissioner, for the purpose of such agencies exercising a power or performing a function or duty

    - clarifying that Departmental officials and other entrusted persons are prohibited from recording, disclosing or accessing protected information unless authorised to do so

    - requiring the Minister to cause an interim review of the Act to commence as soon as practicable after 12 months after commencement

    - requiring the President of the Australian Human Rights Commission, the Human Rights Commissioner and the Information Commissioner to be consulted on the interim review and the existing statutory review at subclause 43(1)

    - requiring the Minister to consult with the public and the Information Commissioner before making rules under the Bill

- empowering the Minister to make rules to further delay the requirement for participation agreements to be in place for the use and provision of the Document Verification Service

- empowering the Minister to make rules to prescribe additional privacy obligations that must be met by parties to participation agreements

- preventing identification information, obtained for the purpose of requesting or providing identity verification services, from being used for data profiling, online tracking or marketing, and

- delaying commencement of the operative provisions of the IVS Bill until rules are made to support the operation and function of the identity verification services, or 6 months after the Act receives Royal Assent.

3. The amendments will also empower the Minister to make rules to extend the transitional period for users of the Document Verification Service to transition onto a participation agreement. The current period is 12 months, and the Minister will be able to make rules to extend this period by 6 months, allowing for up to a total transitional period of 18 months.

4. The amendment to the Consequential Amendments Bill reflects the amendment to the commencement of the Bill.

FINANCIAL IMPACT

5. There are no financial impacts associated with these amendments.

STATEMENT OF COMPATIBILITY WITH HUMAN RIGHTS

Identity Verification Services Bill 2023

1. The amendments to the Bill are compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview of the amendments

2. The purpose of these amendments to the Identity Verification Services Bill 2023 is to enhance the existing privacy protections and oversight arrangements in the Bill, including by implementing the Government's response to recommendations from the Senate Standing Committee on Legal and Constitutional Affairs' majority report into the Bill and the Identity Verification Services (Consequential Amendments) Bill, which was tabled on 9 November 2023.

3. The amendments enhance existing privacy safeguards and oversight arrangements in the Bill, including by:

    - ensuring that the annual assessment at clause 40 aligns with, and leverages, the Information Commissioner's existing assessment functions and powers in the Privacy Act

    - better aligning the requirements that must be set out in participation agreements regarding data breaches with the requirements in the Notifiable Data Breaches scheme under Part IIIC of the Privacy Act

    - requiring express consent, rather than allowing for implied consent

    - specifying the acts or practices of a party to a participation agreement which constitutes an 'interference with privacy of the individual' for the purposes of the Privacy Act

    - clarifying that identification information, as defined in clause 6 of the Bill, is personal information for the purposes of the Privacy Act

    - ensuring that entrusted persons are authorised to disclose protected information to Commonwealth integrity agencies, including the Information Commissioner, and the National Anti-Corruption Commissioner, for the purpose of such agencies exercising a power or performing a function or duty

    - requiring an interim review of the Act to commence as soon as practicable after 12 months after commencement, which must consider the adequacy and operation of the privacy protections, security requirements and obligations, and the penalties for non-compliance with obligations set out in participation agreements, including whether civil penalties should apply

    - requiring that the Information Commissioner, President of the Australian Human Rights Commission, and Human Rights Commissioner all be consulted during the course of the interim review and the 2 year statutory review

    - requiring the Minister to consult with the public and the Information Commissioner before making rules under the Bill, and

    - empowering the Minister to make rules to prescribe additional privacy obligations that must be met by parties to participation agreements

- clarifying that entrusted person are prohibited from dealing with protected information other than for the purposes provided for in the Bill, and

- imposing additional requirements on parties to participation agreements to destroy facial images collected for the purpose of the FVS where the images are no longer required.

Human rights implications

The right to freedom of expression contained in Article 19 of the ICCPR

4. Article 19 of the ICCPR provides that everyone shall have the right to freedom of expression, including the freedom to seek, receive and impart information and ideas of all kinds.

5. Article 19(3) of the ICCPR provides that this right may be limited on grounds including respect for the rights of others, or the protection of national security or public order. Any limitations must be prescribed by legislation and be reasonable, necessary, and proportionate to achieve the desired purpose.

6. The Bill engages the right to freedom of expression by making it an offence for an entrusted person (as defined in clause 30(4)) to make a record of, disclose, or access protected information (see clause 30). The amendments also put beyond doubt that the department responsible for administering the Act to be established by the Bill is prohibited from recording, disclosing or accessing identity verification information unless it is in accordance with the objects of the Bill or in other limited circumstances.

7. The purpose of the limitation on this right is to protect the privacy rights of individuals whose personal information is used in the provision of identification verification.

8. Entrusted persons will have significant access to protected information, as part of their role and it is necessary to limit their freedom of expression to disclose, record, or access this protected information unless authorised. An ***entrusted person*** means:

    - the Secretary of the department responsible for administering the Act to be established by the Bill
    - APS employees (as defined in section 7 of the *Public Service Act 1999*) in the Department
    - a person whose services are made available to the Department who is:
        - an employee of an Agency as defined in the *Public Service Act 1999*
        - or an officer or employee of a State or Territory
        - an officer or employee of a government authority (defined in clause 5 to mean an authority of the Commonwealth, state or territory but <u>not</u> a local government authority)
        - an officer or employee of the government of a foreign country or an authority of a foreign country,
        - or an officer or employee of a public international organisation as defined in section 70.1 of the Criminal Code (for example multilateral international organisations such as the World Bank, World Trade Organization and International Monetary Fund)
    - a contractor engaged to provide services to the Department in connection with an approved identity verification facility (whether the contractor is engaged directly or as a subcontractor), or

- an officer or employee of such a contractor whose duties relate wholly or partly to an approved identity verification facility.

9. ***Protected information*** means any of the following:

    - information obtained by an entrusted person from electronic communications to or from an approved identity verification facility, or from the NDLFRS
    - information about the making, content or addressing of an electronic communication to or from an identity verification facility that was obtained by an entrusted person in their capacity as an entrusted person
    - information about identification information relating to a particular individual held in, or generated using, the NDLFRS, that was obtained by an entrusted person in their capacity as an entrusted person, and
    - information obtained by an entrusted person in their capacity as an entrusted person that would enable access to the Document Verification Service hub, Face Matching Services hub or the NDLFRS.

10. There is a rational connection between the limitation of this right by making it an offence for an entrusted person to make a record of, disclose or access protected information and the objective of protecting the privacy rights of individuals about whom protected information may be disclosed.

11. The offences only limit the right to freedom of expression to the extent necessary and reasonable to protect the rights and reputation of the individuals whose personal information is protected information.

12. The offences will only apply to entrusted persons, which is limited to officers who are working, in some capacity, in the Department. It will not apply to any other persons. This is an appropriate limitation, given such persons will have chosen to take on such roles and received training and induction about the sensitivity of the information and services that they are dealing with, and the application of the offences. The offences also only apply to protected information as defined in subclause 30(4). This is limited to information held or generated using an approved identity verification facility, or that would enable access to such facilities. This information is sensitive and needs to be protected in order to ensure the security of the facilities and support the privacy safeguards set out in the Bill.

13. The limitation on this right through the imposition of this offence is also reasonable, necessary and proportionate due to the safeguards provided in the Bill and in the introduction of the further exceptions to the offence at Amendment 26. The exceptions to the offences in subclauses 30(1) and 30(2) of the Bill are contained in clauses 31 to 35 of the Bill. Amendment 26 would extend the defences available to entrusted persons by expanding the list of persons to whom entrusted persons may disclose protected information. Amendment 26 would achieve this by:

    - omitting clause 33, which permitted entrusted persons to disclose protected information to an IGIS official for the purpose of the IGIS official exercising a power, or performing a duty, as an IGIS official
    - omitting clause 34, which permitted entrusted persons to disclose protected information to an Ombudsman official for the purpose of the Ombudsman official exercising a power, or performing a function or duty, as an Ombudsman official

- inserting a new clause 33 that:
    - permits the disclosure of protected information by entrusted persons to a person in their capacity as an official of a Commonwealth integrity agency for the purpose of that person exercising a power, or performing a function or duty, namely:
        - the Inspector-General of Intelligence and Security, or a person covered by subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986*
        - the Commonwealth Ombudsman, or another officer within the meaning of subsection 35(1) of the *Ombudsman Act 1976*
        - the Information Commissioner, a member of the staff of the OAIC, or a consultant engaged under the *Australian Information Commissioner Act 2010*
        - the National Anti-Corruption Commissioner or another staff member of the NACC (within the meaning of the *National Anti-Corruption Commission Act 2022*), or
        - the Inspector of the NACC or a person assisting the Inspector (within the meaning of the *National Anti-Corruption Commission Act 2022*), and
    - permits an entrusted person to make a record of or access protected information for the purpose of disclosing the protected information to any of the persons set out above.

14. Amendment 26 provides that an entrusted person may disclose protected information to the IGIS or another IGIS official for the purpose of that official exercising a power, or performing a function or duty in their capacity as an IGIS official. Amendment 26 is intended to enable the Inspector-General of Intelligence and Security to obtain information on the use of the identity verification services by ASIO and ASIS, to assist in carrying out the Inspector-General's oversight duties and functions in relation to those agencies as provided in the *Inspector-General of Intelligence and Security Act 1986*. This information may include records of transactions held in the Face Matching Services hub, which are records that will not contain facial images, biometric templates or any other identification information about an individual. Amendment 4 omits the definition of ***IGIS official*** from clause 5, as this definition is not required following the insertion of new subparagraph 33(1)(a)(i) as a result of Amendment 26.

15. Amendment 26 provides that an entrusted person may disclose protected information to the Commonwealth Ombudsman or another officer within the meaning of subsection 35(1) of the *Ombudsman Act 1976* for the purpose of the Ombudsman official exercising a power, or performing a function or duty, as an Ombudsman official. This amendment is intended to support the Commonwealth Ombudsman to perform its functions under the Ombudsman Act, including investigating complaints, as well as other functions conferred on the Ombudsman by the Ombudsman Act or any other Commonwealth Act, or any regulations made under those Acts. Amendment 5 omits the definition of ***Ombudsman official*** from clause 5, as the definition of an Ombudsman official is not required following the insertion of new subparagraph 33(1)(a)(ii)as a result of Amendment 26.

16. Amendment 26 ensures that an entrusted person may disclose protected information to the Information Commissioner, or to an official of the OAIC, for the purpose of that official exercising a power, or performing a function or duty as an official of the OAIC. As defined in Amendment 26, an official of the OAIC includes the Information Commissioner, a member of the

staff of the OAIC, or a consultant engaged under the *Australian Information Commissioner Act 2010*. Amendment 26 is intended to support the Information Commissioner to perform its functions as the independent national privacy regulator, including its investigation, enforcement and oversight functions under the Privacy Act in relation to the Bill. In particular, Amendment 26 would support the Information Commissioner in performing the annual assessment of the approved identity verification facilities required by clause 40, as amended by Amendments 30, 32, and 33. Amendment 26 would assist the Information Commissioner in undertaking this assessment by ensuring that an entrusted person can disclose protected information to the Information Commissioner (or OAIC staff) for this purpose.

17. Amendment 26 also provides that an entrusted person may disclose protected information to the National Anti-Corruption Commissioner, or another staff member of the NACC, for the purpose of the National Anti-Corruption Commissioner exercising a power, or performing a function or duty in their capacity as NACC official. Amendment 26 is intended to enable the NACC to obtain relevant information in order to perform its functions under the *National Anti-Corruption Commission Act 2022*, including to detect corrupt conduct and to undertake investigations into serious or systemic corrupt conduct within the Commonwealth public sector, as well as other functions conferred by the NACC Act and other Acts. Similarly, the clause would enable the Inspector of the NACC to obtain relevant information in order to perform its functions under the NACC Act, including oversight functions and detecting and investigating corrupt conduct within and relating to the NACC. This recognises the functions of the Commissioner and Inspector as part of the broader Commonwealth integrity framework, and their role in supporting the proper enforcement of the law.

18. The exceptions in Amendment 26 ensure that an entrusted person will not be inappropriately subject to criminal liability for their conduct where the disclosure is made to the officials of the relevant Commonwealth integrity agencies for the purpose of performing a function or duty, or exercising a power in their capacity as an official of that integrity agency. Amendment 26 will promote the right to freedom of expression by expanding the range of Commonwealth integrity agencies to which entrusted persons can lawfully disclose protected information. It could also be said to further promote the right to freedom of expression by ensuring Commonwealth integrity agencies can appropriately perform their integrity functions, including the OAIC's function under the Bill to undertaken an annual assessment of the approved identity verification facilities.

19. Therefore Amendment 26 would further mitigate any limitation on the right to freedom of expression that may be considered to result from the offences in subclauses 30(1) and 30(2) of the Bill. The purpose of this limitation is reasonable and necessary given the sensitive nature of the information to which entrusted persons will have access, and implications for an individual if their identification information is unnecessarily disclosed. The limitation is proportionate to protect the privacy of individuals, and is one of the key privacy safeguards built into the Bill.

The right to the presumption of innocence contained in Article 14(2) of the ICCPR

20. Article 14(2) of the ICCPR provides that anyone charged with a criminal offence shall have the right to be presumed innocent until proven guilty according to law. It imposes on the prosecution the burden of proving a criminal charge and guarantees that no guilt can be presumed until the charge has been proved beyond reasonable doubt.

21. Amendment 26 and the Bill engages the right to the presumption of innocence under article 14(2) of the ICCPR. This is because Amendment 26 and the Bill provide that a defendant bears an evidential burden in relation to certain offence-specific defences.

22. The offences in subclauses 30(1) and (2) that require a defendant to bear an evidential burden in relation to an applicable defence in the Bill, including the exceptions amended by Amendment 26, may amount to a limitation on the right to be presumed innocent. This includes provisions where

an evidential burden is created by expressing a matter to be a defence or exception to an offence or providing that the defendant must adduce or point to evidence suggesting a reasonable possibility of the matter. Requiring the defendant to bear the evidential burden in this way may limit article 14(2) of the ICCPR, as a defendant's failure to discharge the burden may permit their conviction despite reasonable doubt as to their guilt. However, under international human rights law, a requirement for a defendant to bear an evidential burden will not necessarily limit the presumption of innocence provided that the law is not unreasonable in the circumstances and maintains the rights of the accused. The purpose of the reverse onus provision is relevant in determining its justification.

23. Subclauses 30(1) and (2) of the Bill and offence-specific defences in clauses 31 to 35 of the Bill (including as amended by Amendment 26, 27 and 28) serve the legitimate objective of protecting personal information by creating criminal offences applying to current and former entrusted persons, such as current and former Departmental employees, who record, disclose or access protected information (including personal information). The maximum penalty for the offences would be 2 years' imprisonment. This penalty reflects the serious consequences that may arise from the relevant conduct, given that a breach of the obligations of entrusted persons may place a person's life or safety at risk, in particular shielded persons.

24. The offence-specific exceptions to these offences, for which the defendant will bear the evidential burden, ensure that an entrusted person will not be inappropriately subject to criminal liability for their conduct where the recording, disclosure or access was:

    - authorised by a law of the Commonwealth or of a state or territory (provided for in paragraph 30(3)(a))

    - in compliance with a requirement under a law of the Commonwealth or of a state or territory (provided for in paragraph 30(3)(b))

    - for the purposes of the Act (as authorised by clause 31 of the Bill)

    - in exercising powers, or performing functions or duties, relating to an approved identity verification facility (as authorised by clause 31 of the Bill)

    - for the purpose of lessening or preventing a serious and imminent threat to human life or health (as authorised by clause 32 of the Bill)

    - for the purpose of an official of a Commonwealth integrity agency exercising a power, or performing a function or duty in their capacity as an official of that integrity agency (as authorised by clause 33 provided for in Amendment 26), or

    - with the express consent of the person to whom the information recorded, disclosed or accessed relates (as authorised by subclause 35(1) as amended by Amendment 27), or with the express consent of the state or territory authority that supplied the information in relation to the NDLFRS (as authorised by subclause 35(2) as amended by Amendment 28).

25. There is a rational connection between the limitation on the right to the presumption of innocence through the imposition of defences that have a reverse burden of proof and protecting entrusted persons from criminal prosecution for conduct undertaken as a legitimate part of the exercise of their duties and function.

26. It is reasonable and necessary for a defendant to bear an evidential burden where the facts in relation to the defence are peculiarly within the knowledge of the defendant, and where it would be significantly more difficult and costly for the prosecution to prove (see the Attorney-General's

Department's *Guide to Framing Commonwealth Offences, Infringement Notices and Enforcement Powers*). In accordance with the principle at paragraph 4.3.1 of the Guide, a matter should only be included in an offence-specific defence, as opposed to being specified as an element of the offence, where:

- it is peculiarly within the knowledge of the defendant, and
- it would be significantly more difficult and costly for the prosecution to disprove than for the defendant to establish the matter.

27. It will be peculiarly within the defendant's knowledge as to the basis on which they believed they were authorised to do so, for the following reasons.

    - There are a vast range of legitimate circumstances in which entrusted persons will need to access, make a record of, or disclose protected information in performing their duties. Every time they do so, they will need to be sure that they have appropriate authorisation under the Bill.
    - The offences in clause 30 will only apply to entrusted persons, which is defined in subclause 30(4) to be limited to persons employed by, or contractors engaged to provide services to, the Department. It will not apply to the general public or persons outside the Department. Entrusted officers will have received training and on-the-job supervision and oversight, and it is reasonable to expect that they will understand their obligations under the Bill when dealing with protected information. Internal guidance policies and procedures will also be in place in order to ensure that entrusted persons understand the need to, and are supported to make, case by case decisions about whether they are authorised to access, make a record of, or disclose protected information before they take such action.

28. In addition, it will be significantly more difficult and costly for the prosecution to prove, beyond a reasonable doubt, that the entrusted person was not authorised to access, make a record of, or disclose protected information, To do this, it would be necessary to negative a significant number of facts – including that the protected information was not disclosed for the purposes of the Act or in the course of the entrusted person performing their functions or duties (as provided for in the exception in clause 31) as well as the fact that there was authority for the person's actions in any Commonwealth, state or territory law (as provided for in subclause 30(3)(a)). This would be in addition to negativing the application of all of the other exceptions set out at clauses 32 to 35 of the Bill. In practice, given the range of laws that might authorise such actions, and the number of actions that might be performed for the purposes of the Act, it may be impossible for the prosecution to disprove all of these matters. At best, it would be extremely costly and burdensome.

29. In contrast, if an entrusted person had a particular reason for thinking that their conduct was authorised in line with the Bill then it would not be difficult for them to describe where they thought that authority arose. This is particularly the case given entrusted persons will be employees of, or contractors with, the Department, and will have received appropriate training and supervision in how to appropriately handle protected information. In line with subsection 13.3(6) of the *Criminal Code Act 1995*, the entrusted person would only need to adduce or point to evidence suggesting a reasonable possibility that their access to, or recording or disclosure of, protected information was authorised by one of the exceptions in the Bill in order to discharge the evidential burden.

30. For these reasons, the offence-specific exceptions in the Bill are reasonable and necessary, as they are consistent with the two-limb test set out in paragraph 4.3.1 of the Guide. They are matters that are peculiarly within the knowledge of the defendant, and would be significantly more difficult

and costly for the prosecution to disprove than for the defendant to establish. Therefore it is reasonable that a defendant bears an evidential burden in relation to certain offence-specific defences.

31. The exceptions set out in the Bill (including as amended by Amendments 26, 27 and 28) are proportionate because, consistent with section 13.3 of the Criminal Code, the evidential burden requires the defendant to adduce or point to evidence that suggests a reasonable possibility that a particular matter exists or does not exist. It does not require the defendant to prove those matters beyond reasonable doubt. Further, if the defendant discharges an evidential burden, the prosecution will also be required to disprove those matters beyond reasonable doubt. The reversed evidential burden provisions in the Bill, including as provided for in Amendments 26, 27 and 28, are also proportionate because they create offence-specific defences that operate in addition to, not instead of, the general defences available at criminal law.

Protection against arbitrary or unlawful interference with privacy contained in Article 17 of the ICCPR

32. Article 17 of the ICCPR prohibits arbitrary or unlawful interference with a person's privacy, family, home or correspondence and unlawful attacks on a person's honour or reputation. It also provides that everyone has the right to the protection of the law against such interference or attacks.

33. The right to privacy articulated in Article 17 may be subject to permissible limitations that are authorised by law, are not arbitrary, pursue a legitimate objective, are necessary to achieve that objective, and are a proportionate means of achieving it. In order for an interference with the right to privacy not to be arbitrary, the interference must be for a reason consistent with the provisions, aims and objectives of the ICCPR and be reasonable in the particular circumstances. The United Nations Human Rights Committee has interpreted 'reasonableness' in this context to mean that 'any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case'.[1]

34. The Bill engages Article 17 by authorising the Department to collect, use and disclose personal or sensitive information covered by the definition of identification information for the purposes of providing the identity verification services. The privacy, accountability and transparency measures contained in the Bill provide appropriate safeguards against any limitations on the right to privacy as a result of the identity verification services provided for by the Bill. This ensures that privacy is an ongoing and primary consideration in the implementation of the Bill and the identity verification services.

35. The amendments to the Bill set out below may be considered to engage the right to privacy. The amendments either seek to enhance the existing privacy protections contained in the Bill, or introduce new privacy protections into the Bill's framework. These measures ensure that privacy is an ongoing and primary consideration in the implementation of the Bill and the identity verification services. Accordingly, the measures further ensure that any limitation on the right to privacy under the Bill are proportionate to the legitimate objective of promoting privacy rights.

36. The following amendments may be considered to engage the right to privacy:

    - Amendment 6 – providing that 'identification information' under the Bill is 'personal information' for the purposes of the Privacy Act

[1] United Nations Human Rights Committee, *The right to privacy in the digital age*, UN Doc A/HRC/27/37, 30 June 2014, paragraph 21, quoting United Nations Human Rights Committee, *Toonan v. Australia*, Communication No. 488/1992, paragraph 8.3.

- Amendment 12 – which would explicitly prohibit the use or disclosure of identification information obtained for the purpose of requesting or providing identity verification services being used for data profiling, online tracking or marketing.

- Amendments 14, 15 and 16 – providing that non-compliance with a requirement of a participation agreement or privacy related rules will be taken to be an 'interference with the privacy of an individual' under the Privacy Act, and can also result in suspension or termination of the ability of a party to the agreement to request identity verification services

- Amendments 7, 8, 9, 11, 23, 27 and 28 – requiring express consent

- Amendment 10 – requiring the Department to notify those parties to a participation agreement that are relevant to, or impacted by, a data breach reported to the Information Commissioner under subclause 9(2)(f), and requiring the party directly impacted by the data breach to take reasonable steps to notify each individual to whom the relevant identification information relates

- Amendments 30, 32 and 33 – providing that the annual assessment of the approved identify verification facilities by the Information Commissioner is taken to be an assessment under paragraph 33C(1)(a) of the Privacy Act

- Amendments 31, 34, 35 and 36, – requiring the Minister to undertake an interim review of the operation of the Bill, including its privacy protections, and

- Amendment 37 – empowering the Minister to make Rules in relation to privacy obligations that must be met by parties to participation agreements and requiring the Minister to consult with the public on all rules and the Information Commissioner on rules related to privacy.

- Amendment 13 – requiring that where a requesting entity no longer needs a facial image that was collected for the purpose of requesting an FVS, the entity must take reasonable steps to destroy the facial image after the purpose for which it is collected is satisfied.

37. All of the above amendments seek to enhance the existing privacy protections contained in the Bill. Accordingly, these measures can be considered to promote, and not limit, the right to privacy as discussed below.

The definition of identification information

38. Amendment 6 inserts new subclause 6(6) to provide that ***identification information***, as defined in clause 6 of the Bill, is taken to be personal information for the purposes of the Privacy Act. Subsection 6(1) of the Privacy Act provides that personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

    - whether the information or opinion is true or not; and

    - whether the information or opinion is recorded in a material form or not.

39. Identification information includes certain types of 'sensitive information' (which is a type of personal information and defined at section 6 of the Privacy Act) and other types of personal identifiers which satisfies the definition of 'personal information' at subsection 6(1) of the Privacy Act.

40. New subclause 6(6) will only apply to parties to a participation agreement who are subject to the Privacy Act (entities covered by paragraph 9(1)(a) of the Bill). This provision is not intended to apply to other parties who may be subject to participation agreements (entities covered by paragraphs 9(1)(b) to 9(1)(e) of the Bill).

41. Amendment 6 puts beyond doubt that, when dealing with identification information, parties to the participation agreement covered by paragraph 9(1)(a) of the Bill, must comply with the requirements in the Privacy Act, including the Australian Privacy Principles, which regulates the handling of personal information. For example, this includes APP 11 which requires APP entities to take active measures to ensure the security of personal information they hold and to actively consider whether they are permitted to retain this personal information. Further, amending the definition of ***identification information*** in this way promotes the right to privacy by engaging the privacy safeguards contained within the Privacy Act relating to personal information, in particular, where there has been an 'interference with privacy' in relation to an APP entity's dealing with identification information. An 'interference with privacy' is defined in section 13 of the Privacy Act, and is a breach of that Act or of a privacy-related provision in certain other legislation.

42. The Privacy Act confers a range of regulatory powers on the Information Commissioner, including investigation and enforcement powers. Where the Information Commissioner has identified an interference with privacy, there are a number of regulatory powers available to the Commissioner to work with an entity to facilitate compliance with legal obligations and best practice privacy practice. In more serious cases, this includes the civil penalty provision at section 13G of the Privacy Act in cases of serious or repeated interference with privacy by an APP entity.

Interference with privacy of an individual

43. Amendment 14 would add a new clause 10A, which would provide that non-compliance with a participation agreement constitutes an 'interference with the privacy of an individual' for the purposes of section 13 of the Privacy Act. This would apply to a party to a participation agreement who is subject to the Privacy Act if the party does not comply with:

    - privacy-related aspects of the participation agreement, which are those matters provided for in clause 9 and 10 of the Bill (except for paragraph 10(1)(b) which is specific to access policies), or

    - rules prescribed for the purposes of subsection 44(1A) (as provided for in Amendment 37).

44. Access policies (as provided for in clause 14 of the Bill) are intended to be used by the Department to set contemporary standards to protect the security of identity verification services, and ensure they are only used for appropriate purposes. A breach of access policies will not always constitute an interference with the privacy of an individual, and therefore paragraph 10(1)(b) is excluded as set out above.

45. This amendment would clarify the application of the Privacy Act and more directly enliven the Information Commissioner's regulatory powers under Parts IV and V of the Privacy Act where there has been a privacy-related breach of a participation agreement. For example, this provides for an individual to complain to the Information Commissioner under section 36 of the Privacy Act about an act or practice that may be an interference with privacy of the individual. This amendment clarifies the intention that participation agreements are privacy-enhancing and consistent with the APPs. In particular, the compliance obligations under the Bill do not alter a party to a participation agreement's obligations under the Privacy Act.

46. Amendment 14 also expands the consequences for non-compliance with the privacy obligations for a party to a participation agreement that is subject to the Privacy Act, beyond the suspension or termination of the participation agreement in accordance with clause 12. This better protects the privacy rights of individuals whose personal information is dealt with by a party to a participation agreement (that is subject to the Privacy Act) by clarifying that the regulatory powers of the Information Commissioner apply for non-compliance with privacy obligations under the agreement.

Prohibiting the use or disclosure of identification information for particular purposes

47. Amendment 12 would insert new subclause 9(4) into the Bill to require that a participation agreement must provide that a party to the agreement is not authorised to use or disclose identification information obtained for the purpose of requesting and providing identity verification services for the purposes of any of the following:

    - engaging in activities that would allow the entity to create a data profile of the person whose identity is being verified, including where it would allow their behaviour (whether online or offline) to be tracked
    - offering to supply goods or services
    - advertising or promoting goods or services
    - enabling another entity to offer to supply goods or services
    - enabling another entity to advertise or promote goods or services
    - market research.

48. This amendment would prevent the identity verification services from being used for data profiling, online tracking or marketing. It makes it clear that this applies to both parties who request identity verification services, as well as the Department, in its role providing the identity verification services.

49. Non-compliance with the explicit prohibition in new subclause 9(4) could result in suspension or termination of the ability of a party to the agreement to request identity verification services, in accordance with clause 12.

50. For a party subject to the Privacy Act (which includes the Department), non-compliance with the explicit prohibition in new subclause 9(4) may also enliven the regulatory powers of the Information Commissioner under Part IV and V of the Privacy Act. For example, an individual may complain to the Information Commissioner under section 36 of the Privacy Act about an act or practice that may be an interference with privacy of the individual. This is made clear through Amendments 6 and 14. Under Amendment 6, identification information is taken to be personal information for the purposes of the Privacy Act. In accordance with Amendment 14, non-compliance with the new subclause 9(4) by a party to a participation agreement subject to the Privacy Act may be taken to be an interference with the privacy of an individual and covered by sections 13 and 13G of that Act. Accordingly, this amendment would promote the privacy rights of individuals who disclose information for identity verification purposes by further ensuring their personal information may only be used or disclosed by a party for the purpose of requesting or providing identity verification services.

Express consent

51. Amendments 7, 8, 9, 11, 23, 27 and 28 will replace any reference to 'consent' references to 'express consent'.

    - Clause 9 of the Bill contains the privacy obligations relating to participation agreements, and requires participation agreements to provide provisions for how a party to a participation agreement obtains an individual's consent to the collection, use and disclosure, for the purposes of requesting identity verification services, of identification information that relates to the individual included in such a request. Amendments 7, 8, 9 and 11 will require any consent in this context to be express consent; and

    - Clause 35 provides a general exception to the offences in clause 30 for entrusted persons who disclose protected information where the individual whose information is disclosed consents to the disclosure, or where the state or territory authority that supplied the information that is held in or generated using the NDLFRS consents to the recording, disclosure or access. Amendments 23, 27 and 28 will require any consent in these scenarios to be express consent.

52. The above amendments will promote the right to privacy by ensuring individuals whose personal information is proposed to be dealt within under the Bill expressly consent to their personal information being used for the purpose proposed. This will promote the privacy rights of those individuals by enhancing the transparency of how their personal information is proposed to be dealt with and ensures those individuals are able to make an informed decision whether to agree to their personal information being used for those purposes.

Notification of data breaches

53. Amendment 10 will expand the notification requirements relating to data breaches to align the notification requirements under the Bill with the with the Notifiable Data Breaches scheme under the Privacy Act. It will do this by requiring the Department to notify each party to a participation agreement that is relevant to, or impacted by, a data breach which is reported to the Information Commissioner under existing paragraph 9(2)(f). New paragraph 9(2)(h) will also impose obligations on such parties to take reasonable steps to notify each individual to whom the identification information subject to the data breach relates.

54. New paragraph 9(2)(g) in Amendment 10 will promote privacy rights by imposing a positive obligation on the Department to notify relevant parties to participation agreements of data breaches. This will enable notified entities to take measures to safeguard personal information held by them which may be susceptible to being accessed in data breaches relevant to them (for example, data breaches to a related government agency that is also party to a participation agreement). Similarly, new paragraph 9(2)(h) will promote the right to privacy of the individuals whose information is impacted by the data breach by ensuring those persons are informed of a breach in relation to their personal information and are able to take measures to mitigate any consequences that might arise from their personal information being the subject of a data breach.

Annual assessment of the approved identity verification facilities by the Information Commissioner

55. Clause 40 of the Bill requires the Information Commissioner to conduct an annual assessment of the operation and management of the approved identity verification service facilities. These facilities are the technical components that enable the department to provide the identity verification services. Amendments would amend clause 40 of the Bill to ensure the annual assessment aligns with, and leverages, the Information Commissioner's assessment functions and powers in the Privacy Act.

56. Amendment 30, 32 and 33 would amend clause 40 to require the Information Commissioner to undertake an annual assessment of the approved identity verification facilities in relation to any act or practice of the Department during the financial year. Amendment 33 will provide that the assessment made under clause 40 is taken to be an assessment under paragraph 33C(1)(a) of the Privacy Act. The amendments ensure that the Information Commissioner will not be limited in determining the scope of its assessment of the approved identity verification facilities. It is also intended to provide certainty that the Information Commissioner's annual assessment will be conducted in a manner consistent with existing privacy assessment function provided at paragraph 33C(1)(a) of the Privacy Act. Paragraph 33C(1)(a) of the Privacy Act provides the Information Commissioner with the power to conduct assessments of APP entities about whether personal information they hold is being maintained and handled in accordance with the APPs. This will promote the right to privacy by making it clear that the Information Commissioner can rely on its existing powers and enforcement mechanisms provided in the Privacy Act to support the conduct of the annual assessment. This includes powers to require APP entities to provide information or produce a document where the Commissioner has reason to believe that an entity being assessed has information or a document relevant to an assessment under section 33C of the Privacy Act. It also ensures that the Information Commissioner's assessment function under clause 40 aligns with the OAIC's *Guide to Privacy Regulatory Action.*[2]

57. Subsection 33C(8) of the Privacy Act provides that the Information Commissioner may publish the Information Commissioner's assessments on the OAIC website. As set out in the OAIC's *Guide to Privacy Regulatory Action*,[3] the OAIC recognise that there may be circumstances when it would be inappropriate to publish all or part of an assessment report due to statutory secrecy provisions or reasons of privacy, confidentiality, commercial sensitivity, security or privilege. The OAIC will take these factors into account when deciding whether to publish an assessment report in full or in an abridged version, and the OAIC would generally consult with the relevant target of the report before publication. This is an important factor which promotes transparency as well as the right to privacy, as it enables the OAIC to ensure that its assessments would not unduly release personal information through the publication of its assessment, or other sensitive information about the approved identity verification facilities.

Interim review

58. Amendments 31, 34, 35 and 36 amend clause 43 of the Bill to require the Minister to cause an interim review of the Act to commence as soon as practicable after 12 months of the commencement of clause 43. This interim review is to occur in addition to the requirement in clause 43 for the Minister to cause a review of the operation of the Act and the provision of the identity verification services to be started within 2 years of the commencement of clause 43.

59. The interim review will consider the adequacy and operation of:

- the privacy protections contained in the Act (new paragraph 43(1B)(a)), which may include, but is not limited to, consideration of:
    - the privacy obligations of parties to participation agreements (clauses 9 and 10 of the Bill), and
    - the data breach notification requirements in relation to the NDLFRS hosting agreement, which is provided at subclauses 13(3) and (4), and

---

[2] *Guide to Privacy Regulatory Action*, Chapter 9: Privacy Assessments, available at https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-9-privacy-assessments, published January 2023, accessed November 2023.
[3] *Guide to Privacy Regulatory Action*, Chapter 9: Privacy Assessments, at 9.68.

- the security requirements and obligations contained in the Act (new paragraph 43(1B)(b)), which may include, but is not limited to, consideration of:
    - the requirement for the Department to maintain the security of identification information included in a database in the NDLFRS, including by encrypting the information (paragraph 13(4)(a))
    - the requirement for the Department to maintain the security of electronic communications to and from the approved identity verification facilities, including by encrypting the information (paragraph 25(a)), and
    - the requirement for the Department to protect the information from unauthorised interference or unauthorised access (paragraph 25(b), and
- the penalties for non-compliance with obligations set out in participation agreements, including consideration of whether civil penalties should apply to any such non-compliance (new paragraph 43(1B)(c)), noting that the current penalty for non-compliance with a participation agreement is suspension or termination of the ability of a party to the agreement to request identity verification services (paragraph 12(c)).

60. Amendment 35 to the Bill further provides that the President of the Australian Human Rights Commission, the Human Rights Commissioner and the Information Commissioner, must be consulted in relation to the interim review. This will ensure that the interim review is informed by expert views on human rights, including privacy rights.

61. The interim review promotes the right to privacy by ensuring that there will be timely examination of the adequacy and operation of the privacy protections, security requirements and penalties for non-compliance with such obligations contained in the Act. It will provide the opportunity to identify and address any areas for improvement to further enhance the strong privacy and security protections in place.

Rules and consultation on the rules

62. Amendment 37 would expand the Minister's rule making power in clause 44 to provide that the Minister may make rules in relation to privacy obligations that must be met by parties to participation agreements.

63. Amendment 37 would require the Minister to consult with the public before making any rules under the Bill. Further, before the Minister makes any rules related to privacy, including any rules made in accordance with Amendment 37, the Minister must consult with the Information Commissioner.

64. The Minister's expanded rule making power to allow rules to be made in relation to the privacy obligations that must be met by parties to participation agreements will promote privacy rights. It will do this by ensuring the Minister has the ability to set additional privacy requirements or obligations that must be met by parties to participation agreements. For example, this power may be used to require a party to a participation agreement to put in place additional protections in response to the Information Commissioner's annual assessment of the approved identity verification facilities (clause 40), or to address operational issues identified through the annual reporting (clause 41) or the interim or 2 year review (clause 43) that may require further privacy safeguards for entities seeking to request the use of the identity verification services.

65. As one of the key functions of the Information Commissioner is to protect the privacy rights of individuals in accordance with the Privacy Act, the consultation requirement in Amendment 37 promotes the right to privacy by harnessing the expertise of the OAIC and enhancing oversight of

the privacy-related rules before they are made. The consultation requirement will help ensure any privacy-related rules made by the Minister align with, and promote, the objectives of the Privacy Act. The requirement to consult with the public similarly provides additional oversight and transparency about any rules that the Minister proposes to make before they are made, and provides other stakeholders with the opportunity to make submissions on privacy-related rules, or other rules.

66. The amendments to the commencement provisions of the Bill would also provide the Minister with sufficient opportunity to undertake the required consultation with the Information Commissioner and the public on any proposed rules that the Minister seeks to have in place upon commencement of the Bill, such as the fees for private sector entities. This will also provide greater opportunity to work with industry and state and territory government agencies to support the implementation of the Bill.

Destruction of facial images

67. Amendment 13 would insert an additional privacy obligation to be contained in participation agreements for parties that request an FVS. The new obligation would require parties who request an FVS to take reasonable steps to destroy a facial image that has been created by the party as soon as practicable after the image is no longer required.

68. The only exceptions to the general requirement to destroy facial images will be if the record is a Commonwealth record within the meaning of the *Archives Act 1983*, or a party is required to retain the record under a law of the Commonwealth, a state or a territory, or by order of a court or tribunal. Requesting parties who do not comply with this requirement may have their participation agreement cancelled or suspended. In addition, under new clause 10A, non-compliance with this obligation will be considered an interference with the privacy of an individual under the Privacy Act.

69. This additional obligation will promote the right to privacy by ensuring that entities requesting an FVS have a positive obligation to destroy facial images after they are no longer required by that entity for the purpose of identity verification. This will help ensure facial images are only collected and retained for the limited purpose, and for minimum time necessary, to verify a person's identity.

70. The amendment will further promote the privacy rights of persons whose facial images are collected by mitigating impacts of data breaches or other unlawful access to systems of requesting FVS entities where facial images are stored. This will reduce potential incidents of identity theft, fraud or other unlawful conduct that could result from access to facial images.

Conclusion

71. The proposed amendments are compatible with the applicable human rights and freedoms.

72. The Bill as amended is compatible with the applicable human rights and freedoms as provided for in the Explanatory Memorandum to the Bill. To the extent that it may limit human rights, particularly the right to privacy, those limitations are reasonable, necessary and proportionate to achieving that objective.

NOTES ON AMENDMENTS

Amendment 1—commencement

1. Amendment 1 amends clause 2 of the Bill to provide a new commencement table. The effect of this amendment is that only clauses 1 to 14, 42 and 44, rather than the whole Bill, will commence on the day after the Bill receives the Royal Assent. All other provisions in the Bill will commence on the earlier of:

    - the day rules made under the rule making power at clause 44 commence, and

    - the day after the end of the period of 6 months beginning on the day the Bill receives the Royal Assent.

2. Amendment 1 provides certainty that the provisions relating to the requesting or provision of the identity verification services will commence once rules that are critical to support the effective operation of the DVS, FVS and FIS have commenced, or on the day 6 months after the day after the Royal Assent.

3. The following rules that may be made by the Minister are critical to support the effective operation of the identity verification services:

    - rules prescribing a state or territory privacy law for the purposes of a participation agreement (paragraph 9(1)(b)) and the NDLFRS hosting agreement (subparagraph 13(2)(a)(ii)

    - rules prescribing a government authority of the purposes of a participation agreement (paragraph 9(1)(d)), and

    - rules prescribing the fees for requests for identity verification services or for connections to the approved identity verification facilities to allow the making of electronic communications to, and receipt of electronic communications from, those facilities (clause 42).

4. It is necessary for clauses 1 to 14, 42 and 44 to commence before the rest of the Bill in order to ensure that the Minister is empowered to make the above rules. Clauses 1 to 14 includes the definitions for the Bill, and the obligations for parties to participation agreements and the NDLFRS hosting agreement. Clause 42 provides that the Minister may make rules in relation to the imposition, collection and recovery of fees, which rely on these definitions. Clause 44 is a broad rule-making power which ensures there is authority to make such rules as are necessary to ensure the effective operation of the Act to be established by the Bill.

5. The commencement provisions in Amendment 1 also support Amendment 37 which implements the Government's response to Recommendation 9 of the Committee's report. The commencement provisions ensure there will be sufficient opportunity to consult with the Information Commissioner on the rules that need to be in place to support the effective operation of the identity verification services, insofar they relate to privacy, before they are made under clause 44. Amendment 1 will also allow for sufficient opportunity to undertake public consultation prior to any rules outlined above being made under clause 44.

Amendment 2, 3, 19, 20, 21, 24, 25, 29—prohibition on the recording, disclosing or access protected information

6. Amendment 2, 3, 19, 20, 21, 24, 25 and 29 would amend the Bill to put beyond doubt that an entrusted person (including a Departmental official) is prohibited from recording, disclosing or

accessing protected information unless it is in accordance with the objects of this Bill or in other limited circumstances.

7. Amendment 24 omits the heading to Division 2 (previously 'When protected information can be recorded, disclosed or accessed') and replaces it with a new heading of 'Prohibition on recording or disclosure of, or access to, information by entrusted persons'.

8. Amendment 25 omits the heading to clause 30 (previously 'Offences by entrusted persons') and replaces it with a new heading of 'Prohibition on recording or disclosure of, or access to, information by entrusted persons'.

9. The purpose of Amendments 24 and 25 is to better reflect the substantive content of clause 30 of the Bill. Clause 30 of the Bill prohibits the recording or disclosure of, or access to, protected information by:

    - creating two criminal offences in relation to entrusted persons where they make a record of, disclose or access protected information (subclauses 30(1) and (2)) – the maximum penalty for both these offences would be imprisonment for two years, and

    - providing exceptions to the two offences where the recording or disclosure of, or access to, protected information is for the purposes of the Act, in accordance with the objects of this Bill (clause 31), or in other limited circumstances (clauses 31 to 35).

10. The terms ***entrusted person*** and ***protected information*** are defined in subclause 30(4) of the Bill.

11. Amendment 2 would insert a note at the end of clause 3 to reflect the intent of Amendment 24 and 25 and to clarify that the existing prohibition provided by subclause 30(1) and (2) do not apply where an entrusted person's conduct is for the purposes of the Act, as set out in the objects set out in clause 3 of the Bill.

12. Clause 3 is an objects clause that outlines the purposes of the Bill and can be used to resolve uncertainty and ambiguity. Objects clauses may assist the courts and others in the interpretation of legislation.

13. The note clarifies that the objects referred to in paragraphs 3(a), (b) and (d) are authorised and provided for by Part 2 (Developing, operating and maintaining approved identity verification facilities), Part 3 (Authorising collection, use and disclosure of identification information) and Part 5 (Miscellaneous) respectively. The note also clarifies that in accordance with paragraph 3(c), Part 4 of the Bill prohibits the use or disclosure of, or access to, identity verification information, unless it is in accordance with the objects of this Bill or in other limited circumstances.

14. Amendment 3, 19, 20, 21 and 29 would amend relevant simplified outlines in the Bill to reflect the intent and purpose of Amendment 24 and 25. The simplified outline is included to assist readers to understand the substantive provisions of the Bill. The outline is not intended to be comprehensive. It is intended that readers should rely on the substantive provisions of the Bill.

15. Amendment 3 would insert additional information into the simplified outline of the Bill in clause 4. Clause 4 provides a simplified outline of the Bill, including an overview of the operation of the identity verification facilities and the services that are authorised to be conducted using those facilities.

16. Amendment 3 would insert an outline of Part 4 of the Bill (Protection of information) into the simplified outline at clause 4. The purpose of the amendment is to ensure that the simplified outline at clause 4 reflects that Part 4 of the Bill prohibits the use or disclosure of, or access to,

identity verification information, unless it is in accordance with the objects of this Bill or in other limited circumstances.

17. Amendment 19 would amend the simplified outline of Part 2 of the Bill (Developing, operating and maintaining approved identity verification facilities) at clause 23. The amendment would omit "The Department" at the beginning of the simplified outline of Part 2 and substitute "In accordance with the object of this Act covered by paragraph 3(a), the Department".

18. Paragraph 3(a) of the Bill provides that one of the objects of the Bill is to authorise the Department to develop, operate, and maintain the approved identity verification facilities. The purpose of the amendment is to ensure that the simplified outline of Part 2 reflects that the Department is required to develop, operate and maintain the approved identity verification facilities (the DVS hub, the Face Matching Service Hub and the NDLFRS) in accordance with the object of the Bill covered by paragraph 3(a) of the Bill.

19. Amendment 20 would amend the simplified outline of Part 3 of the Bill (Authorising collection, use and disclosure of identification information) at clause 26. The amendment would omit the words 'The Department' from the beginning of the simplified outline of Part 3 and substitute the words 'In accordance with the object of this Act covered by paragraph 3(b), the Department'.

20. Paragraph 3(b) of the Bill provides that one of the objects of the Bill is to authorise the Department, but not other persons or bodies, to collect, use and disclose identification information that has been communicated to an approved identity verification service, or generated using the NDLFRS, for purposes relating to:

    - the use of 1:1 matching services (the DVS and the FVS) for verifying the identity of an individual

    - the use of 1:many matching services (the FIS) for protecting shielded persons or someone else associated with a shielded person, or

    - the NDLFRS.

21. The purpose of the amendment is to ensure that the simplified outline reflects that the Department is required to collect, use and disclose identification information in accordance with the object of this Bill covered by paragraph 3(b) of the Bill.

22. Amendment 21 would amend the simplified outline of Part 4 of the Bill (Protection of information). The amendment would reflect in the simplified outline of Part 4 that:

    - an object of this Bill is to protect identification information communicated to approved identity verification facilities, and certain other information relating to the use or security of those facilities, and

    - the Bill does this by prohibiting the use or disclosure of, or access to, identity verification information, unless it is in accordance with the objects of this Bill or in other limited circumstances.

23. The aim of this amendment is to put beyond doubt that officials involved in providing the identity verification services are prohibited from recording, disclosing or accessing protected information unless it is in accordance with the objects of the Bill or in other limited circumstances.

24. Amendment 29 would amend the simplified outline of Part 5 of the Bill (Miscellaneous). This amendment would reflect in the simplified outline of Part 5 that an object of this Bill is to provide

oversight and scrutiny of the operation and management of the approved identity verification facilities, as provided in paragraph 3(d) of the Bill.

Amendments 4 and 5—disclosure to integrity agencies

25. Amendments 4 and 5 would omit the definition of ***IGIS official*** and ***Ombudsman official*** from clause 5. These definitions are no longer necessary because new clause 33 as provided in Amendment 26 incorporates on its face the definitions of the relevant persons in each integrity agency to whom an entrusted person may disclose protected information.

Amendment 6—identification information

26. Amendment 6 would implement the Government's response to Recommendation 2 of the Committee's report to provide that identification information, as defined in clause 6, is personal information for the purposes of the Privacy Act.

27. Amendment 6 would insert a new sub-heading and new subclause 6(6) to provide that ***identification information***, as defined in clause 6 of the Bill, is taken to be personal information for the purposes of the Privacy Act.

28. Subsection 6(1) of the Privacy Act provides that personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

    - whether the information or opinion is true or not; and

    - whether the information or opinion is recorded in a material form or not.

29. Identification information includes certain types of 'sensitive information' (which is a type of personal information and defined at subsection 6(1) of the Privacy Act) and other types of personal identifiers which satisfies the definition of 'personal information' at subsection 6(1) of the Privacy Act.

30. New subclause 6(6) would only apply to parties to a participation agreement who are subject to the Privacy Act (entities covered by paragraph 9(1)(a) of the Bill). This provision is not intended to apply to other parties who may be a party to a participation agreement (entities covered by paragraphs 9(1)(b) to 9(1)(e) of the Bill).

31. Amendment 6 puts beyond doubt that, when dealing with identification information, parties to the participation agreement, covered by paragraph 9(1)(a) of the Bill, must comply with the requirements in the Privacy Act, including the Australian Privacy Principles (APP), which regulates the handling of personal information. For example, this includes APP 11 which requires APP entities to take active measures to ensure the security of personal information they hold and to actively consider whether they are permitted to retain this personal information. To ensure compliance with the requirements in the Privacy Act, entities should consider the *Guide to Securing Personal Information* which provides guidance from the OAIC on the reasonable steps entities are required to take to protect personal information.

32. Amendment 6 would also enable the Information Commissioner to more easily determine whether there has been an 'interference with privacy' in relation to an entity's dealing with identification information. An 'interference with privacy' is defined in section 13 of the Privacy Act, and is a breach of that Act or of a privacy-related provision in certain other legislation.

33. Where the Information Commissioner has identified an interference with privacy, there are a number of enforcement powers available to the Commissioner. This includes the civil penalty

provision at section 13G of the Privacy Act in cases of serious or repeated interference with privacy by an entity.

Amendments 7, 8, 9, 11, 23, 27, 28—express consent

34. Amendments 7, 8, 9, 11, 23, 27, 28 would implement the Government's response to Recommendation 10 of the Committee's report to amend the Bill to only include express consent and not implied consent. The amendments implement this recommendation by replacing all references to 'consent' in the Bill with references to 'express consent'.

35. Subsection 6(1) of the Privacy Act provides that 'consent' means express consent or implied consent. *The Australian Privacy Principles Guidelines* from the OAIC provides guidance on the differences between express and implied consent:

    - Express consent is given explicitly, either orally or in writing. This could include a handwritten signature, an oral statement, or use of an electronic medium or voice signature to signify agreement.

    - Implied consent arises where consent may reasonably be inferred in the circumstances from the conduct of the individual and the APP entity.

36. The inclusion of express consent is intended to strengthen existing provisions in the Bill by ensuring consent is obtained 'explicitly.' This is a reasonable and necessary additional safeguard noting the Bill authorises for the collection, use and disclosure of an individual's 'identification information' (as defined at clause 6), which includes 'sensitive information' (as defined at subsection 6(1) of the Privacy Act). It also aligns with the *Australian Privacy Principles Guidelines* which notes that entities should 'generally seek express consent from an individual before handling the individual's sensitive information, given the greater privacy impact this could have.'

37. Amendment 7 would amend the simplified outline of Subdivision B of Division 2, to replace the reference to 'consent' with a reference to 'express consent'. The simplified outline is included to assist readers to understand the substantive provisions of the Bill and, in this case, reflects the substantive operation of paragraph 9(2)(b), as amended by Amendment 8.

38. Amendment 8 would amend paragraph 9(2)(b) to replace the reference to 'consent' with 'express consent' to clarify that participation agreements are required to provide for the obtaining of an individual's *express* consent to the collection, use and disclosure, for the purposes of requesting identity verification services, of identification information that relates to the individual included in such a request. This requirement will apply to all participation agreements (including government authorities, all private sector organisations and local government agencies). The only limited exception is set out in subparagraphs 9(2)(b)(i) and (ii) and applies to requests made by government authorities where the collection, use and disclosure of identification information for the purpose of protecting a shielded person, or someone else associated with a shielded person, are implicit in the functions conferred by law on the authority.

39. Amendment 9 would amend paragraph 9(2)(c) to replace the reference to 'consent' with 'express consent'. Paragraph 9(2)(c) requires a party to a participation agreement to provide, to an individual from whom consent is being sought, information about the matters listed in subclause 9(3). The effect of this amendment is to provide that this information must be provided to a person from whom *express* consent is being sought. This ensures the individual is provided with details about how their information will be used and is in a position to provide express consent.

40. Amendment 11 would amend paragraph 9(3)(a) to replace the reference to 'consent' with 'express consent'. Subclause 9(3) sets out the information that must be provided to a person from whom

express consent is being sought. Paragraph 9(3)(a) requires information to be provided about how the party seeking consent uses identity verification services. The effect of this amendment is to provide this information must be provided in relation to how a party seeking *express* consent will use the identity verification services.

41. Amendment 23 would amend the simplified outline of Part 4, to replace the reference to 'consent' with a reference to 'express consent'. The simplified outline is included to assist readers to understand the substantive provisions of the Bill and, in this case, reflects the substantive operation of clause 35, as amended by Amendments 27 and 28.

42. Amendment 27 would amend paragraph 35(1)(a) to replace the reference to 'consented' with 'expressly consented'. Clause 35 provides that an entrusted person may make a record of, disclose or access protected information if they have the consent of the person to whom it relates. The recording, disclosing or access must be done in accordance with that consent. The effect of this amendment is to provide that this authorisation only applies if the entrusted person has the *express* consent of the person to whom the protected information relates. In accordance with paragraph 35(1)(b), the recording, disclosing or access must be done in accordance with that *express* consent in order for the authorisation to apply.

43. Amendment 28 would amend subclause 35(2) to replace the references to 'consents' with 'expressly consents'. Subclause 35(2) of the Bill provides that an entrusted person may make a record of, disclose, or access protected information that was held in, or generated using the NDLFRS (paragraph (a)) and was supplied by an authority of a state or territory if that authority has consented to the recording, disclosure or access. The effect of this amendment is to provide that this authorisation only applies if the entrusted person has the *express* consent of the relevant authority to the recording, disclosure or access.

Amendment 10—notification of data breaches

44. Amendment 10 would implement the Government's response to Recommendation 7 of the Committee's report to amend the Bill to ensure that individuals are notified when there is a data breach that is likely to cause them serious harm.

45. Amendment 10 would insert new paragraph 9(2)(g) to require the Department to notify each party to a participation agreement that is relevant to, or impacted by, a data breach, where a data breach has been reported by the Department to the Information Commissioner in accordance with the requirement in paragraph 9(2)(f) of the Bill.

46. This amendment would more clearly align the notification requirements in the Bill with the notification requirements in the Notifiable Data Breaches scheme under Part IIIC of the Privacy Act.

47. The amendment would ensure that other relevant parties to a participation agreement are notified of a data breach in circumstances where:

    - a party to a participation agreement has reported a breach of security to the Department in accordance with the requirement in paragraph 9(2)(e) of the Bill, and

    - the Department has reported the breach of security to the Information Commissioner because it is a data breach that is reasonably likely to result in serious harm to an individual whose identification information is involved in the breach, in accordance with the requirement in paragraph 9(2)(f) of the Bill.

48. The purpose of the amendment is to ensure that all relevant parties to a participation agreement – not just the party that reported the security breach – are aware of such breaches and can take any

appropriate and necessary action to mitigate any consequential impacts to their entity's use of the identity verification services. For example, data hosting agencies may decide to limit the types of information available for identity verification purposes (in accordance with clause 11 of the Bill).

49. Amendment 10 would also insert new paragraph 9(2)(h) to require each party to a participation agreement that is impacted by a breach notified to the Information Commissioner under paragraph 9(2)(f) to take reasonable steps to notify each individual to whom the identification information relates. This approach aligns with the notification requirement in paragraph 13(3)(c) regarding the NDLFRS hosting agreement. It is also intended to align with the requirement in subsection 26WL(2) of the Privacy Act, which requires APP entities subject to a data breach to take reasonable steps to notify the individuals who are at risk from the breach.

50. Placing the notification requirement on entities impacted by the data breach seeks to ensure that individuals do not receive multiple notifications regarding the same breach. Where multiple parties to an agreement are involved in a data breach, the parties involved would be expected to take steps to ensure the individual does not receive multiple notifications about the same breach. For example, the parties involved could determine between them that one party would notify the affected individuals. This may be considered reasonable steps for the other parties involved for the purpose of the Bill. Furthermore, in practice, it is likely that only the information of customers of impacted entities – rather than customers of entities relevant to the data breach – would be at risk from the data breach.

51. Nothing in Amendment 10 is intended to exclude the operation of any state or territory notification requirements. This includes, for example, the mandatory data breach (information security incident) requirements on Victorian agencies under the Victorian Protective Data Security Framework and Standards. The Notifiable Data Breaches scheme under Part IIIC of the Privacy Act will also apply to those parties to a participation agreement that are subject to the Privacy Act.

52. Non-compliance with a participation agreement can lead to the agreement being suspended or terminated in accordance with clause 12 of the Bill. Further, if a non-compliant party is subject to the Privacy Act, new clause 10A (inserted by Amendment 14) would also be applicable. New clause 10A provides that privacy-related breaches of participation agreements by APP entities will constitute an interference with privacy under the Privacy Act.

Amendment 12—further limitations on use of identification information

53. Amendment 12 inserts new subclause 9(4) to require that a participation agreement must provide that a party to the agreement is not authorised to use or disclose identification information obtained for the purpose of requesting and providing identity verification services for the purposes of any of the following:

    - engaging in activities that would allow the party to create a data profile of the person whose identity is being verified (including where it would allow their behaviour to be tracked (whether or not online)) (paragraph 9(4)(a))

    - offering to supply goods or services (paragraph 9(4)(b))

    - advertising or promoting goods or services (paragraph 9(4)(c))

    - enabling another person or entity to offer to supply goods or services (paragraph 9(4)(d))

    - enabling another person or entity to advertise or promote goods or services (paragraph 9(4)(e))

- market research (paragraph 9(4)(f)).

54. New subclause 9(4) will apply to:

    - a party to a participation agreement requesting identity verification services, and

    - the Department in its role as a party to a participation agreement that provides the identity verification services.

55. Non-compliance with the requirements of new subclause 9(4) could result in suspension or termination of the ability of a party to the agreement to request identity verification services, in accordance with clause 12.

56. For a party subject to the Privacy Act (which includes the Department), non-compliance with the explicit prohibition in new subclause 9(4) may also enliven the regulatory powers of the Information Commissioner under Part IV and V of the Privacy Act. For example, an individual may complain to the Information Commissioner under section 36 of the Privacy Act about an act or practice that may be an interference with privacy of the individual. This is made clear through Amendments 6 and 14. Under Amendment 6, identification information is taken to be personal information for the purposes of the Privacy Act. In accordance with Amendment 14, non-compliance with the new subclause 9(4) by a party to a participation agreement subject to the Privacy Act may be taken to be an interference with the privacy of an individual and covered by sections 13 and 13G of that Act.

Amendment 13—destruction of facial images

57. Amendment 13 will amend Clause 10 (Extra privacy obligations of parties to participation agreement that request services) to insert new paragraph 10(2)(aa).

58. New paragraph 10(2)(aa) will require parties to a participation agreement to take reasonable steps to destroy each facial image of an individual that is created for the purposes of making a request for the FVS as soon as reasonably practicable after the image is no longer required for the purposes of the request. This new obligation will only apply to parties that make requests for an FVS.

59. Facial image is defined in clause 5 of the Bill and means a digital still image of an individual's face (whether or not including the shoulders).

60. For example, this provision is intended to apply in circumstances where an individual has taken a digital photo of themselves, for identity verification purposes, on a mobile application provided by a party to participation agreement. After obtaining express consent, the party would use the digital image created on their platform to verify that person's identity.

61. Amendment 13 is drafted to be consistent with Australian Privacy Principle 11.2, which sets out requirements for entities subject to the Privacy Act to take reasonable steps to destroy or de-identify the personal information it holds. In line with APP 11.2, new paragraph 10(2)(aa) will not apply if the image:

    - a Commonwealth record within the meaning of section 3 of the *Archives Act 1983* (Cth) (subparagraph 10(2)(aa)(i)), or

    - required by a law of the Commonwealth, a State or a Territory, or by an order of a court or tribunal, to be retained (subparagraph 10(2)(aa)(ii)).

62. Non-compliance with new paragraph 10(2)(aa) will be considered to be non-compliance with a participation agreement and may lead to the suspension or termination of access to the FVS. Non-compliance with a participation agreement can lead to the agreement being suspended or terminated in accordance with clause 12 of the Bill. Further, if a non-compliant party is subject to the Privacy Act, new clause 10A (inserted by Amendment 14) would also be applicable. New clause 10A provides that privacy-related breaches of participation agreements by APP entities will constitute an interference with privacy under the Privacy Act.

Amendment 14—failure to comply with participation agreements

63. Amendment 14 would implement the Government's response to Recommendation 3 of the Committee's report to amend the Bill to provide that a breach of a participation agreement that relates to a privacy matter by an APP entity constitutes an interference with privacy under the Privacy Act.

64. Amendment 14 would insert new clause 10A. Clause 10A would provide that if an act or practice of a party to a participation agreement, relating to personal information about an individual, does not comply with a requirement of:

    - clauses 9 and 10 of the Bill (other than paragraph 10(1)(b)) which set out the privacy obligations and requirements for participation agreements (defined at clause 8 of the Bill) (subparagraph (i)), or

    - rules prescribed for the purposes of new subclause 44(1A) as provided for in Amendment 37, namely rules relating to privacy with which a party to a participation agreement must comply

    then the act or practice is taken to be an 'interference with privacy of the individual' for the purposes of the Privacy Act, and would be covered by sections 13 and 13G of that Act.

65. New paragraph 10A(1)(a) limits the application of this clause to parties to a participation agreement that are subject to the Privacy Act and, in practice, covered by paragraph 9(1)(a) of the Bill. In general terms, the Privacy Act applies to Ministers, Departments, a range of Commonwealth agencies, and organisations with an annual turnover of less than $3,000,000 (see sections 6, 6C and 6D of the Privacy Act).

66. Clauses 9 and 10 provide important privacy safeguards which, among other things, governs how parties to participation agreements are authorised to collect, use and disclose identification information, and requires such entities to implement certain procedures and take action to protect the information of individuals when engaging with the identity verification services. ***Identification information*** is defined at clause 6 of the Bill and includes certain types of sensitive information (which is a type of personal information and defined at subsection 6(1) of the Privacy Act) and other types of personal identifiers which satisfies the definition of personal information at subsection 6(1) of the Privacy Act.

67. New clause 10A will not apply where a party to a participation agreement fails to comply with paragraph 10(1)(b) of the Bill which requires compliance with access policies for the identity verification services. Access policies (as provided for in clause 14 of the Bill) are intended to be used by the Department to set contemporary standards to protect the security of identity verification services, and ensure the services are only used for appropriate purposes. The requirements in access policies are often unrelated to privacy matters.

68. Rules prescribed for the purposes of new subclause 44(1A) are intended to provide further privacy obligations on parties to a participation agreement (in addition to those at clauses 9 and 10). For example, this rule making power could be relevant and relied upon should there be a need to

provide additional protections in response to the Information Commissioner's annual assessment (clause 40 of the Bill), or operational issues that may require further privacy safeguards for entities seeking to request the use of the identity verification services.

69. New subclause 10A(2) makes it clear that an act or practice of a party to a participation agreement that does not comply with privacy related requirements in a participation agreement is taken to be an interference with the privacy of the individual and, accordingly, is covered by sections 13 and 13G of the Privacy Act.

    - Section 13 of the Privacy Act sets out the acts and practices that may be an interference with the privacy of an individual, which includes a breach of an APP or a registered Australian Privacy Principle privacy code.

    - Section 13G of the Privacy Act is a civil penalty provision for cases of serious or repeated interference with privacy by an entity and operates in addition to the numerous other regulatory powers available to the Information Commissioner in relation to an interference with privacy.

70. The purpose and intent of new clause 10A is threefold.

    - Firstly, it provides certainty to entities subject to the Privacy Act, and the Australian community, that non-compliance with the privacy safeguards and obligations in participation agreements or prescribed in rules will constitute an interference with the privacy of an individual for the purposes of the Privacy Act.

    - Secondly, it better supports individuals by allowing them to make a complaint to the Information Commissioner (including under section 36 of the Privacy Act) in relation to an act or practice that may be an interference with privacy of the individual.

    - Thirdly, it will more directly enliven the Information Commissioner's functions and regulatory powers under Parts IV and V of the Privacy Act where there has been non-compliance with the relevant aspects of participation agreements or rules.

Amendments 15 and 16—rules relating to privacy

71. Paragraph 12(c) of the Bill currently requires participation agreements to provide for suspension or termination of the ability of a party to the agreement to request identity verification services if the party does not comply with the agreement or access policies for those services. Amendment 15 would amend paragraph 12(c) to add a reference to 'rules made for the purposes of subsection 44(1A)'.

72. New subclause 44(1A) will be inserted by Amendment 37, and will empower the Minister to make rules in order to provide further privacy requirements (in addition to those already in the Bill) to be met by a party to a participation agreement. It is essential that parties to participation agreements are required to comply with any privacy requirements that are set out in rules made under new subclause 44(1A) and that the participation agreement can be suspended or terminated in circumstances of non-compliance. The amendment to paragraph 12(c) achieves this outcome.

73. Amendment 16 would insert a note to clause 12 clarifying that under subsection 44(1A), the rules may prescribe requirements relating to privacy with which a party to a participation agreement must comply.

Amendments 17 and 18—timing of participation agreements for DVS

74. Amendment 17 and 18 would amend clause 15 to allow for a longer transition period for entities using and providing the DVS to move onto participation agreements.

75. Amendment 18 inserts new subsection 15(3) which provides that, for the purposes of subsection (2), certain requirements do not apply for a time period that is the longer of either:

    - 12 months (paragraph 15(3)(a)), or

    - up to 18 months if the rules prescribe it (paragraph 15(3)(b)).

76. Amendment 17 reflects this change by omitting '12 months' from subsection 15(2) and substituting the words 'the period specified by subsection (3).'

77. Currently, subsection 15(2) of the Bill provides that the requirements for the requesting entity and the document issuing body to be parties to a participation agreement do not apply in relation to the DVS within 12 months after the commencement of clause 15. The effect of Amendment 18 is that the Minister will be able to make rules (as provided by clause 44) to prescribe a longer period of up to 18 months.

78. Amendment 17 and 18 responds to concerns raised during the Committee's inquiry by providing industry with sufficient opportunity to consider and update current operations to comply with the obligations in participation agreements, without compromising their ability to use the DVS.

79. The DVS is a critical aspect of the day-to-day operations of government and business. It is a longstanding service which is currently used by over 2,700 government agencies and private sector organisations, matching against documents provided by more than 20 government agencies. These entities are party to memoranda of understanding (for government agencies) or contractual arrangements (for business users) outlining the terms of their participation of the services.

Amendments 22 and 26—disclosure to integrity agencies

80. Amendments 22 and 26 would further support the oversight and transparency functions of Commonwealth integrity agencies. The amendments would also implement the Government's response to Recommendation 8 of the Committee's report to allow entrusted persons to disclose protected information to the Information Commissioner or an OAIC staff member, for the purpose of the Commissioner or the OAIC exercising a power, or performing a function or duty.

81. Amendment 22 would amend the simplified outline of Part 4 in clause 29, to omit references to an IGIS official or Ombudsman official and substitute reference to 'an official of an integrity agency'. The simplified outline is included to assist readers to understand the substantive provisions of the Bill and, in this case, reflects the substantive operation of new clause 33, as inserted by amendment 26, and the removal of the definitions of ***IGIS official*** and ***Ombudsman official*** by amendments 4 and 5.

82. Amendment 26 omits the previous authorisations in clauses 33 and 34 allowing entrusted persons to disclose protected information to an IGIS official or an Ombudsman official. These clauses will be replaced by a new clause 33 that provides a more comprehensive authorisation allowing entrusted persons to disclose protected information to a Commonwealth integrity agency for the purpose of persons in those integrity agencies performing their functions or duties as officials of those agencies.

83. New clause 33 would permit the disclosure of protected information by entrusted persons to any of the following integrity agencies:

    - the Inspector-General of Intelligence and Security, or a person covered by subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986* (new subparagraph 33(1)(a)(i))

    - the Commonwealth Ombudsman, or another officer (within the meaning of subsection 35(1) of the *Ombudsman Act 1976*) (new subparagraph 33(1)(a)(ii))

    - the Information Commissioner, a member of the staff of the Office of the Information Commissioner, or a consultant engaged under the *Australian Information Commissioner Act 2010* (new subparagraph 33(1)(a)(iii))

    - the National Anti-Corruption Commissioner, or another staff member of the NACC (within the meaning of the *National Anti-Corruption Commission Act 2022*) (new subparagraph 33(1)(a)(iv)), or

    - the Inspector of the National Anti-Corruption Commission, or a person assisting the Inspector (within the meaning of the *National Anti-Corruption Commission Act 2022*) (new subparagraph 33(1)(a)(v)).

84. New paragraph 33(1)(b) requires that a disclosure under new paragraph 33(1)(a) must be for the purpose of that person exercising a power, or performing a function or duty. These officials are typically entitled to access any information in the course of performing their functions and duties, reflecting the paramount importance of effective oversight of the public service.

85. Subclauses 30(1) and (2) of the Bill protect personal information by creating criminal offences applying to current and former entrusted persons, such as current and former departmental employees, who record, disclose or access protected information (including personal information). Amendment 26 would provide exceptions to the offences provided for in clause 30. Amendment 26 adds new subclause 33(2) which makes clear that an entrusted person may make a record of, or access protected information for the purpose of disclosing the information to an integrity agency in accordance with new subclause 33(1).

86. The ability for entrusted persons to disclose protected information under new clause 33 is intended to achieve the following outcomes.

    - It will enable the Inspector-General or a person covered by subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986* to obtain information on the use of the identity verification services by ASIO and ASIS, to assist in carrying out their oversight duties and functions in relation to those agencies as provided in the Inspector-General of Intelligence and Security Act. This information may include records of transactions held in the Face Matching Services hub, which are records that will not contain facial images, biometric templates or any other identification information about an individual.

    - It will support the Commonwealth Ombudsman or another officer within the meaning of subsection 35(1) of the *Ombudsman Act 1976* to perform their functions under the Ombudsman Act, including investigating complaints, as well as other functions conferred on the Ombudsman by the Ombudsman Act or any other Commonwealth Act, or any regulations made under those Acts.

    - It will support the Information Commissioner to perform its functions as the independent national privacy regulator, including its investigation, enforcement and oversight

functions under the Privacy Act in relation to the Bill. In particular, Amendment 26 would support the Information Commissioner in performing the annual assessment of the department's operation and management of the approved identity verification facilities required by clause 40 as amended (see amendments 30, 32, and 33). This amendment implements a recommendation made by the OAIC in its submission to the Senate Committee's inquiry into the Bill and the Consequential Amendments Bill.

- It will enable the NACC to obtain relevant information in order to perform its functions under the *National Anti-Corruption Commission Act 2022*, including to detect corrupt conduct and to undertake investigations into serious or systemic corrupt conduct within the Commonwealth public sector, as well as other functions conferred by the NACC Act and other Acts. Similarly, new clause 33 is intended to enable the Inspector of the NACC to obtain relevant information in order to perform its functions under the NACC Act, including oversight functions and detecting and investigating corrupt conduct within and relating to the NACC. This recognises the Commissioner's and Inspector's functions as part of the broader Commonwealth integrity framework.

Amendments 30, 32 and 33—annual assessment by Information Commissioner

87. Amendments 30, 32, and 33 would implement the Government's response to Recommendation 6 of the Committee's report to amend the Bill to enliven the OAIC's existing assessment powers in subsection 33C(1) of the Privacy Act in relation to the annual assessment requirements in clause 40. Clause 40 of the Bill requires the Information Commissioner to conduct an annual assessment of the operation and management of the approved identity verification service facilities. These facilities are the technical components that enable the department to provide the identity verification services.

88. Amendment 30 would amend the simplified outline of Part 5 in clause 36, to omit references to the Information Commissioner assessing 'the operation and management' of the approved identity verification facilities. The simplified outline is included to assist readers to understand the substantive provisions of the Bill and, in this case, reflects the substantive operation of Amendment 32, which amends the provision that provides the Information Commissioner with the function of doing an annual assessment.

89. Amendments 32 and 33 would amend clause 40 of the Bill to ensure the annual assessment aligns with, and leverages, the Information Commissioner's assessment functions and powers in the Privacy Act, by:

    - omitting paragraph 40(1)(a) of the Bill which states that the Information Commissioner will assess the operation and management of the approved identity verification facilities by the Department in the financial year'

    - adding new paragraph 40(1)(a) to provide the Information Commissioner with the function of 'assessing the approved identity verification facilities in relation to any act or practice of the Department during the financial year', and

    - omitting subclauses 40(2) and 40(3) of the Bill and substituting new subclause 40(2) to provide that section 33C(1)(a) of the Privacy Act applies in relation to the annual assessment.

90. The annual assessment will only relate to the Department, and is not intended to extend to other parties to a participation agreement (for example, those entities requesting the use of the identity verification services).

91. New paragraph 40(1)(a), inserted by Amendment 32, ensures that the Information Commissioner will not be limited in determining the scope of its assessment of the approved identity verification facilities. New paragraph 40(1)(a) is intended to provide certainty that the Information Commissioner's annual assessment will be conducted in a manner consistent with existing privacy assessment function provided at subsection 33C(1) of the Privacy Act.

92. Subsection 33C(1)(a) of the Privacy Act empowers the Information Commissioner to conduct assessments of APP entities about whether personal information they hold is being maintained and handled in accordance with the APPs.

93. Amendment 33 omits previous subclauses 40(2) and (3), which required the Secretary of the Department to ensure there was in place an arrangement with the Information Commissioner for providing information to the Information Commissioner for making assessments under subclause 40(1). Previous subclause 40(3) provided that, to avoid doubt, an arrangement made under previous subclause 40(2) may have been made before, or on or after, the commencement of clause 40. This provision is no longer required following the removal of subclause 40(2).

94. New subclause 40(2), as inserted by Amendment 33, provides that an assessment under new subclause 40(1) is taken to be an assessment under paragraph 33C(1)(a) of the Privacy Act.

95. New subclause 40(2) of the Bill allows the Information Commissioner to rely on existing powers and enforcement mechanisms provided in the Privacy Act to support the conduct of the annual assessment. This includes powers to require APP entities to provide information or produce a document where the Commissioner has reason to believe that an entity being assessed has information or a document relevant to an assessment under section 33C of the Privacy Act. New subclause 40(2) would also ensure that the Information Commissioner's assessment function aligns with the OAIC's *Guide to Privacy Regulatory Action.*[4]

96. Subsection 33C(8) of the Privacy Act provides that the Information Commissioner may publish the Information Commissioner's assessments on the OAIC website. As set out in the OAIC's *Guide to Privacy Regulatory Action*,[5] the OAIC recognises that there may be circumstances when it would be inappropriate to publish all or part of an assessment report due to statutory secrecy provisions or reasons of privacy, confidentiality, commercial sensitivity, security or privilege. The OAIC will take these factors into account when deciding whether to publish an assessment report in full or in an abridged version, and the OAIC would generally consult with the relevant target of the report before publication.

Amendments 31, 34, 35 and 36—interim review

97. Amendments 31, 34, 35 and 36 would implement the Government's response to Recommendation 11 of the Committee's report to provide for an interim review of the Bill after 12 months which focuses on the adequacy of the privacy and security protections and whether there is merit in developing a civil penalties framework for the identity verification services.

98. Amendment 31 would amend the simplified outline of Part 5 of the Bill in clause 36 to omit reference to the requirements for a review of the operation of this Act and the provision of identity verification services to be started within 2 years and for the report to be tabled. Amendment 31 replaces this with a reference to an interim review and review of this Act being conducted, both of which must be started within 2 years of the commencement of clause 43 of the Bill. The simplified outline is included to assist readers to understand the substantive provisions

[4] *Guide to Privacy Regulatory Action*, Chapter 9: Privacy Assessments, available at https://www.oaic.gov.au/about-the-OAIC/our-regulatory-approach/guide-to-privacy-regulatory-action/chapter-9-privacy-assessments, published January 2023, accessed November 2023.
[5] *Guide to Privacy Regulatory Action*, Chapter 9: Privacy Assessments, at 9.68.

of the Bill and, in this case, reflects the substantive operation of amendments 34, 35 and 36, which establish the requirement for an interim review and a review of the Act.

99. Amendment 34 omits the heading to clause 43 (previously 'Review of operation of this Act and provision of identity verification services') and replaces it with a new heading reading 'Interim review, and review of this Act and provision of identity verification services.'

100. Amendment 35 amends clause 43 of the Bill to insert two new subclauses. New subclause 43(1A) will require the Minister to cause an interim review of the Act to be started as soon as practicable after 12 months and before the end of 2 years of the commencement of clause 43. Consistent with clause 2, as amended by Amendment 1, clause 43 will commence the earlier of the day rules made under clause 44 commence, and, the day after the end of the period of 6 month beginning on the day the Bill receives the Royal Assent).

101. The interim review will occur in addition to the requirement in clause 43 for the Minister to cause a review of the operation of the Act and the provision of the identity verification services to be started within 2 years of the commencement of clause 43. A 12-month period is appropriate for the interim review to be commenced as it will allow sufficient time for the relevant aspects of the Bill to be established and in operation for a meaningful period before the interim review is undertaken.

102. New subclause 43(1B) will require the interim review to consider the adequacy and operation of:

- the privacy protections contained in the Act (new paragraph 43(1B)(a)) – this may include, but would not be limited to, consideration of:
    - the privacy obligations of parties to participation agreements (clauses 9 and 10 of the Bill)
    - the data breach notification requirements in relation to the NDLFRS hosting agreement (provided at subclauses 13(3) and (4))
- the security requirements and obligations contained in the Act (new paragraph 43(1B)(b)) – this may include, but would not be limited to, consideration of:
    - the requirement for the Department to maintain the security of identification information included in a database in the NDLFRS, including by encrypting the information (paragraph 13(4)(a))
    - the requirement for the Department to maintain the security of electronic communications to and from the approved identity verification facilities, including by encrypting the information (paragraph 25(a))
    - the requirement for the Department to protect the information from unauthorised interference or unauthorised access (paragraph 25(b)), and
- the penalties for non-compliance with obligations set out in participation agreements, including consideration of whether civil penalties should apply to any such non-compliance (new paragraph 43(1B)(c))

103. Amendment 36 would insert a new subclause 43(2A) setting out consultation requirements for both the interim review (under subclause 43(1A)) and the 2 year review (under subclause 43(1)).

104. Under new subclause (2A), the following persons must be consulted in relation to the interim review and 2 year review:

- the President of the Australian Human Rights Commission appointed under section 8A of the AHRC Act
- the Human Rights Commissioner appointed under section 8B of the AHRC Act, and
- the Information Commissioner appointed under section 14 of the *Australian Information Commissioner Act 2010* (Cth).

105. This consultation requirement will provide an opportunity for the reviews to be informed by expert views about matters that relate to human rights, including the privacy.

106. Amendment 36 also ensures that the interim review will be subject to the same requirements for consultation, preparation and tabling as provided in subclauses 43(2) and (3) for the 2-year review. Subclauses 43(2) and (3) provide that the Minister must:

- cause a report of each review to be prepared and given to the Minister, and
- cause a copy of each report to be tabled in each House of the Parliament within 15 sitting days of that House after the Minister receives the report.

Amendments 37 and 38—rules relating to privacy

107. Amendment 37 would implement the Government's response to Recommendation 9 of the Committee's report to amend clause 44 of the Bill to require the Information Commissioner to be consulted on rules, as they relate to privacy, before they are made under clause 44.

108. Clause 44 currently allows the Minister to, by legislative instrument, make rules prescribing matters:

- required or permitted by this Bill to be prescribed by the rules, or
- necessary or convenient to be prescribed for carrying out or giving effect to the Bill.

109. Amendment 37 would amend clause 44 to insert new subclause 44(1A), which clarifies that, without limiting existing subclause 44(1), the rules may prescribe requirements relating to privacy with which a party to a participation agreement must comply (in addition to those already in the Bill). This ensures rules can be made to prescribe additional privacy requirements in response to an annual assessment by the Information Commissioner (conducted under clause 40 of the Bill), or to address operational issues that may require further privacy safeguards for entities seeking to request the use of the identity verification services.

110. Amendment 37 inserts new paragraph 44(1B)(a), which requires that, before making or amending any rules under subclause 44(1), the Minister must undertake public consultation on proposed rules with the public.

111. New subparagraphs 44(1B)(a)(i) and (ii) require the Minister to cause a notice to be published on the department's website:

- setting out the draft rules or amendments, and

- inviting persons to make submissions to the Minister about the draft rules or amendments within the period specified in the notice, which must be at least 28 days after the notice is published.

112. Amendment 37 also inserts new paragraph 44(1B)(b), which requires that any rules that deal with matters relating to privacy functions (within the meaning of the *Australian Information Commissioner Act 2010)* must be subject to consultation with the Information Commissioner. Under the Bill, as amended by Amendment 37, the Minister can make rules in relation to the following privacy matters:

- requirements relating to privacy within which a party to a participation agreement must comply (new subclause 44(1A) as inserted by Amendment 37)

- prescribing government authorities for the purposes of paragraph 9(1)(d)

- prescribing state or territory privacy laws for the purposes of becoming a party participation agreement under subparagraph 9(1)(b)(ii), and

- prescribing state or territory privacy laws for the purposes of becoming a party to the NDLFRS hosting agreement under subparagraph 12(2)(a)(ii).

113. Amendment 37 also inserts new paragraph 44(1B)(c) which requires the Minister to consider any submissions received within the period specified. This obliges the Minister to consider any submissions from the public on draft rules or amendments, as well as submissions from the Information Commissioner where the rules deal with matters relating to privacy functions. The Minister may also consider submissions received after the specified period if the Minister considers it appropriate to do so (new subclause 44(1C)).

114. The purpose of Amendment 37 is to establish a framework to support genuine and meaningful consultation with the public on any rules that are proposed to be made under subclause 44(1). The period of 28 days ensures the public are given a reasonable opportunity to consider and, if desired, make submissions in relation to, proposed rules or amendments. This will enable industry and other users of the identity verification services to provide input and scrutinise proposed rules to be made which may impact the operation of the services and fees charged to those entities that seek to request use of the services.

115. These amendments do not preclude or limit any other consultations undertaken to support the development of rules under the Bill. In particular, section 17 of the *Legislation Act 2003* (Cth) requires that, before making a legislative instrument, the instrument-maker must be satisfied that appropriate consultation, as is reasonably practicable, has been undertaken in relation to a proposed instrument.

116. Amendment 38 inserts a new sub-heading reading ‘Disallowance and sunsetting of rules’ before subclause 44(3), which serves to clarify that section 42 (disallowance) and Part 4 and Chapter 3 (sunsetting) of the *Legislation Act 2003* applies to the rules.

Identity Verification Services (Consequential Amendments) Bill 2023

Amendment 1—Commencement

1. Amendment 1 amends clause 2 of the Consequential Amendments Bill, which provides for the commencement of each provision in the Consequential Amendments Bill as set out in the table.

2. Amendment 1 amends clause 2 of the Consequential Amendments Bill (table item 1), by inserting in item (b) 'section 24 of' before 'the *Identity Verification Services Act 2023*'.

3. Amended item 1 of the table provides that the whole of the Consequential Amendments Bill will commence on the day that is the later of:

(a) the start of the day after the Bill receives Royal Assent, or

(b) the commencement of section 24 of the *Identity Verification Services Act 2023*.

4. Section 24 of the proposed *Identity Verification Services Act 2023* (the proposed Act) provides authority for the Department to develop, operate and maintain the approved identity verification facilities. This would provide authority for the Department to establish the information technology solutions for the approved identity verification facilities, operate them in accordance with the requirements of the proposed Act and maintain them on an ongoing basis. Therefore it is appropriate that the Consequential Amendments Bill does not commence unless section 24 of the proposed Act has commenced.

5. However, as noted in Item 1, the provisions in the Consequential Amendments Bill do not commence if section 24 of the proposed Act does not commence. This reflects that the amendment in the Consequential Amendments Bill is intended to support the operation of the identity verification services provided for in the proposed Act.

2022-2023

The Parliament of the
Commonwealth of Australia

THE SENATE

Identity Verification Services Bill 2023

(Government)

(1) Clause 2, page 2 (table item 1), omit "The day after this Act receives the Royal Assent", substitute "The day after the end of the period of 3 months beginning on the day this Act receives the Royal Assent".

[commencement]

(2) Clause 5, page 8 (lines 9 to 12), omit the definition of ***IGIS official***.

[disclosure to integrity agencies]

(3) Clause 5, page 9 (lines 9 to 13), omit the definition of ***Ombudsman official***.

[disclosure to integrity agencies]

(4) Clause 6, page 14 (after line 6), at the end of the clause, add:

Identification information taken to be personal information

(6) Identification information is taken to be personal information for the purposes of the *Privacy Act 1988*.

[identification information]

(5) Clause 7, page 15 (line 9), omit "consent", substitute "express consent".

[express consent]

(6) Clause 9, page 16 (line 32), omit "consent", substitute "express consent".

[express consent]

(7) Clause 9, page 17 (line 7), omit "consent", substitute "express consent".

[express consent]

(8) Clause 9, page 17 (line 23), at the end of subclause (2), add:

; and (g) the Department to notify each party to the agreement that is relevant to, or impacted by, a data breach of which the Information Commissioner is informed under paragraph (f); and

(h) each party notified under paragraph (g) of a data breach, that is impacted by that breach, to take reasonable steps to notify each individual to whom the identification information relates.

[notification of data breaches]

(9) Clause 9, page 17 (line 25), omit "consent", substitute "express consent".

[express consent]

(10) Clause 9, page 18 (after line 9), at the end of the clause, add:

(4) A participation agreement must provide that a party to the agreement is not authorised to use or disclose identification information obtained for the purposes of requesting or providing identity verification services for the purposes of any of the following:

(a) engaging in activities that would allow the party to create a data profile of the person whose identity is being verified (including where it would allow the person's behaviour to be tracked (whether or not online));

(b) offering to supply goods or services;

(c) advertising or promoting goods or services;

(d) enabling another person or entity to offer to supply goods or services;

(e) enabling another person or entity to advertise or promote goods or services;

(f) market research.

[further limitations on use of identification information]

(11) Page 19 (after line 12), after clause 10, insert:

10A Failure to comply with participation agreements

(1) This section applies if:

(a) a party to a participation agreement is subject to the *Privacy Act 1988*; and

(b) an act or practice of the party, relating to personal information about an individual, does not comply with a requirement of:

(i) the agreement in relation to a matter covered by section 9 or 10 (other than paragraph 10(1)(b)) of this Act; or

(ii) rules prescribed for the purposes of subsection 44(1A) of this Act.

(2) For the purposes of the *Privacy Act 1988*, the act or practice is taken to be:

(a) an interference with the privacy of the individual; and

(b) covered by sections 13 and 13G of that Act.

[failure to comply with participation agreements]

(12) Clause 12, page 19 (line 29), after "agreement", insert ", rules made for the purposes of subsection 44(1A),".

[rules]

(13) Clause 12, page 19 (after line 30), at the end of the clause, add:

Note: Under subsection 44(1A), the rules may prescribe requirements relating to privacy with which a party to a participation agreement must comply.

[rules]

(14) Clause 29, page 35 (lines 20 and 21), omit "an IGIS official or Ombudsman official", substitute "an official of an integrity agency".

[disclosure to integrity agencies]

(15) Clause 29, page 35 (line 22), omit "consent", substitute "express consent".

[express consent]

(16) Clauses 33 and 34, page 39 (lines 1 to 15), omit the clauses, substitute:

33 Information communicated etc. to integrity agencies

(1) An entrusted person may disclose protected information if:

(a) the disclosure is to any of the following persons:

(i) the Inspector-General of Intelligence and Security, or a person covered by subsection 32(1) of the *Inspector-General of Intelligence and Security Act 1986*;

(ii) the Commonwealth Ombudsman, or another officer (within the meaning of subsection 35(1) of the *Ombudsman Act 1976*);

(iii) the Information Commissioner, a member of the staff of the Office of the Information Commissioner, or a consultant engaged under the *Australian Information Commissioner Act 2010*;

(iv) the National Anti-Corruption Commissioner, or another staff member of the NACC (within the meaning of the *National Anti-Corruption Commission Act 2022*);

(v) the Inspector of the National Anti-Corruption Commission, or a person assisting the Inspector (within the meaning of the *National Anti-Corruption Commission Act 2022*); and

(b) the disclosure is for the purpose of that person exercising a power, or performing a function or duty.

(2) An entrusted person may make a record of or access protected information for the purpose of disclosing the protected information under subsection (1).

[disclosure to integrity agencies]

(17) Clause 35, page 39 (line 20), omit "consented", substitute "expressly consented".

[express consent]

(18) Clause 35, page 39 (line 30), omit "consents", substitute "expressly consents".

[express consent]

(19) Clause 36, page 41 (lines 10 and 11), omit "the operation and management of".

[annual assessment by Information Commissioner]

(20) Clause 36, page 41 (lines 16 to 18), omit "A review of the operation of this Act and the provision of identity verification services must be started within 2 years. A report of the review must be tabled in Parliament.", substitute "An interim review and review of this Act must be conducted, both of which must be started within 2 years of the commencement of this Act.".

[interim review]

(21) Clause 40, page 43 (lines 13 to 15), omit paragraph (1)(a), substitute:

(a) assessing the approved identity verification facilities in relation to any act or practice of the Department during the financial year;

[annual assessment by Information Commissioner]

(22) Clause 40, page 43 (lines 17 to 22), omit subclauses (2) and (3), substitute:

(2) For the purposes of the *Privacy Act 1988*, an assessment under subsection (1) of this section is taken to be an assessment under paragraph 33C(1)(a) of that Act.

[annual assessment by Information Commissioner]

(23) Heading to clause 43, page 46 (lines 18 and 19), omit "**Review of operation of this Act and provision of identity verification services**", substitute "**Interim review and review of this Act**".

[interim review]

(24) Clause 43, page 46 (before line 20), before subclause (1), insert:

(1A) The Minister must cause an interim review to be started as soon as practicable after 12 months, and before the end of 2 years, of the commencement of this section.

(1B) The interim review must consider the adequacy and operation of:

(a) the privacy protections contained in this Act; and

(b) the security requirements and obligations contained in this Act; and

(c) the penalties for non-compliance with obligations set out in participation agreements, including considering whether civil penalties should apply.

[interim review]

(25) Clause 43, page 46 (line 23), omit "the review", substitute "a review under subsection (1A) or (1)".

[interim review]

(26) Clause 44, page 47 (after line 4), after subclause (1), insert:

(1A) Without limiting subsection (1), the rules may prescribe requirements relating to privacy with which a party to a participation agreement must comply.

(1B) Before making or amending any rules under subsection (1), the Minister must:

(a) cause to be published on the Department's website a notice:

(i) setting out the draft rules or amendments; and

(ii) inviting persons to make submissions to the Minister about the draft rules or amendments within the period specified in the notice (which must be at least 28 days after the notice is published); and

(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; and

(c) consider any submissions received within the specified period.

(1C) The Minister may consider any submissions received after the specified period if the Minister considers it appropriate to do so.

[rules]