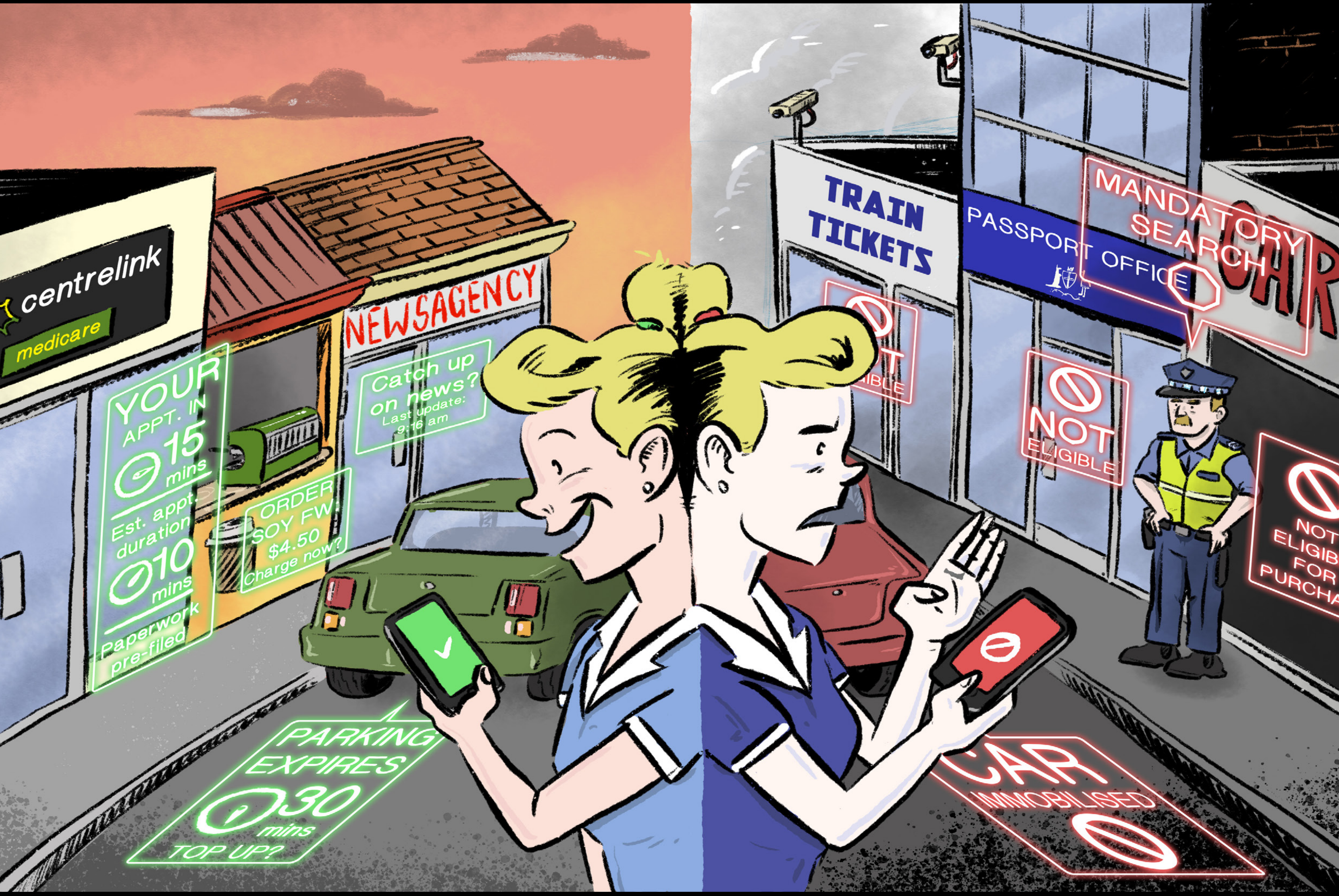
Embargoed until 11.59pm, 17 October 2018 AEST. Media may report 18 October 2018.

Preventing another Australia Card fail

Unlocking the potential of digital identity

Fergus Hanson



ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

Policy Brief
Report No. 9/2018

About the author

Fergus Hanson is the head of the ASPI International Cyber Policy Centre. He is the author of *Internet wars* and has published widely on a range of cyber and foreign policy topics. He was a visiting fellow at the Brookings Institution and a Professional Fulbright Scholar based at Georgetown University working on the uptake of new technologies by the US Government. He has worked for the UN, was a program director at the Lowy Institute and served as a diplomat at the Australian Embassy in The Hague. He has been a fellow at Cambridge University's Lauterpacht Research Centre for International Law and the Centre for Strategic and International Studies, Pacific Forum. He has published widely in Australian and international media.

What is ASPI?

The Australian Strategic Policy Institute (ASPI) was formed in 2001 as an independent, non-partisan think tank. Its core aim is to provide the Australian Government with fresh ideas on Australia's defence, security and strategic policy choices. ASPI is responsible for informing the public on a range of strategic issues, generating new thinking for government and harnessing strategic thinking internationally.

ASPI International Cyber Policy Centre

The ASPI International Cyber Policy Centre's mission is to shape debate, policy and understanding on cyber issues, informed by original research and close consultation with government, business and civil society.

It seeks to improve debate, policy and understanding on cyber issues by:

1. conducting applied, original empirical research
2. linking government, business and civil society
3. leading debates and influencing policy in Australia and the Asia–Pacific.

We thank all of those who contribute to the ICPC with their time, intellect and passion for the subject matter. The work of the ICPC would be impossible without the financial support of our various sponsors.

Important disclaimer

This publication is designed to provide accurate and authoritative information in relation to the subject matter covered. It is provided with the understanding that the publisher is not engaged in rendering any form of professional or other advice or services. No person should rely on the contents of this publication without first obtaining advice from a qualified professional person.

ASPI

Tel +61 2 6270 5100
Fax + 61 2 6273 9566
Email enquiries@aspi.org.au
www.aspi.org.au
www.aspistrategist.org.au
facebook.com/ASPI.org
@ASPI_ICPC
www.aspi.org.au/icpc/home

First published October 2018

Cover image: Illustration by Wes Mountain. ASPI ICPC and Wes Mountain allow this image to be republished under the Creative Commons License Attribution-Share Alike. Users of the image should use this sentence for image attribution: 'Illustration by Wes Mountain, commissioned by ASPI's International Cyber Policy Centre'.

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

Embargoed until 11.59pm, 17 October 2018 AEST. Media may report 18 October 2018.

Preventing another Australia Card fail

Unlocking the potential of digital identity

Fergus Hanson

Policy Brief
Report No. 9/2018

Embargoed until 11.59pm, 17 October 2018 AEST. Media may report 18 October 2018.

Contents

What's the problem?

Another major government digitisation scheme—digital identity—is set to cause controversy and risk further disempowering Australians in the absence of clearer policy and legislative controls. That's problematic because digital identity has the potential to power the 21st-century economy, society and government by providing easy, high-confidence verification of identity that will allow millions of offline transactions to move online and enable a string of enhanced services, such as easy delegation of authority (for example, to pick up prescriptions) and verifications (such as proof of age online). However, the national digital identity program, known as GovPass, faces obstacles on multiple fronts:

- Public communication about the scheme and its implications has been wanting, leaving the public largely unaware of the change afoot.
- A key biometric enabling service for digital identity, the Face Verification Service (FVS), risks being conflated with the far-reaching law enforcement biometric enabler—the Face Identification Service (FIS)—that's part of the same national facial biometric matching capability agreed to by Australian Government and state and territory government leaders in October 2017. The FIS lacks adequate safeguards and in its current form is likely to attract public opposition far exceeding that directed towards the My Health Record scheme.
- The government is now building two digital identity schemes that will compete against each other. The first, which is already operational, was built by Australia Post at a cost of $30–50 million and is known as Digital iD. The second scheme, GovPass, secured $92.4 million in the 2018–19 Budget to create the infrastructure that will underpin it and fund its initial rollout.
- Neither GovPass nor Digital iD is governed by dedicated legislation, beyond existing laws such as the inadequate *Privacy Act 1988*, leaving Australians vulnerable to having their data misused.
- The lack of clarity about how the private sector will and will not be able to use the schemes will turbocharge the ability to gather detailed profiles of individual Australians. Controls are needed to prevent a Western version of China's 'social credit' scheme emerging.

What's the solution?

National multi-use identity schemes have a poor track record in Australia. To gain public approval for this major reform, the government needs a fresh approach that places the citizen at the centre of the system. To help restore public confidence in digital initiatives after a string of failures, the introduction of this reform needs to be accompanied by an overhaul of citizens' and consumers' rights so that they're fit for purpose in the 21st century.

The government should work with civil society to stimulate and lead a national debate on the benefits of digital identity, including medium- to long-term plans for the scheme. It should emphasise the strengthened protections that the public will gain against the encroachment on citizens' rights that this and other digital reforms are producing.

Proposed legislation enabling the FVS and FIS should be far more tightly drafted, paring back the applications that the FVS and the FIS can be used for and precisely defining their uses. Dedicated legislation should be introduced to govern both government digital identity schemes.

Opportunities should be explored to avoid duplication between the two schemes. Protections for individuals in the schemes should be strengthened to prevent private-sector actors using the service to build profiles of individual citizens and on-selling those profiles in a for-profit version of China’s social credit scheme. While detailed customer profiles can already be built through methods such as loyalty programs, digital identity will enable a vastly expanded range of activities to be linked to verified identities and so exponentially expand the scope for profile building and ranking if left unchecked.

Introduction

The 2014 Financial System Inquiry recommended that the government ‘develop a national strategy for a federated-style model of trusted digital identities’ that would be accessible for both public and private identity verification.[1] The recommendation was subsequently agreed to by government.[2] Creating this digital identity is a major micro-economic reform. How it’s deployed, structured, understood and protected will fundamentally shape the sort of Australia we end up with.

On 5 October 2017, the then Prime Minister and state and territory leaders laid the foundation for digital identity when they agreed to establish a ‘national facial biometric matching capability’. This connects national, state and territory photographic databases via an exchange. It has two key components. The FVS will use the exchange to allow digital identity verification. This is a one-to-one image-based verification that matches a person’s photo against an image on one of their government records (such as a passport photo) to help verify their identity. The second component, the FIS, is a one-to-many image-based identification service that matches a photo of an unknown person against multiple government records to help establish their identity and is designed for law enforcement purposes.[3]

What’s digital identity?

Digital identity is essentially a credential scheme allowing you to quickly confirm your personal details, entitlements and authorisations, such as proving you are over 18 years old or an Australian citizen, online or in person via your phone. It requires a one-off verification—for example, by photographing your driver’s licence with your phone (the details of which are then checked against the relevant government database) or, for higher level verification, taking a selfie (which is then checked against a biometric template of your face that the government has collated).[4] The selfie is tested against only one image—the document consented to and nominated by the individual.[5] Through the FVS, the selfie would be checked separately against a template of the photos that it’s compared against, which would be your driver’s licence photo, a passport photo or a visa/citizenship photo. Stored on a mobile app, you can use this digital identity to transact with government and companies (for example, by entering your phone number on their websites and then providing permission to undertake the identity check via your digital identity mobile app) or in person, without needing to carry a wallet and identity documents.

Australians make more than 800 million transactions with government annually; 26 million of those transactions involve face-to-face verifications, and more than 300 million require phone or other authentications. Some 750,000 applications for tax file numbers are made each year, requiring in-person verification or the sending of certified copies—a process that can take up to 40 days.[6] More broadly, the government operates more than 30 different logins for online services.[7] A single government digital identity can simplify this landscape, allowing a single login for each individual across governments—federal, state and territory—and also simplify the 800 million transactions. This can significantly reduce irritation on the part of citizens accessing government services, and if done properly should in fact enhance privacy by tailoring the amount of personal information disclosed to the bare minimum required for the specific transaction. It has many other far-reaching applications, such as improving child safety online, reducing cyberbullying and de-anonymising the online experience.

Decoding the jargon

MyGov: the existing common credential for authenticating to many government departments, but without strong identity verification (generally, you have to prove who you are to each department).

MyGovID: the brand name for the Australian Taxation Office's (ATO's) new 'Commonwealth digital identity provider' (formerly, AUSid). This is the portal through which people can validate their identity under the GovPass scheme.

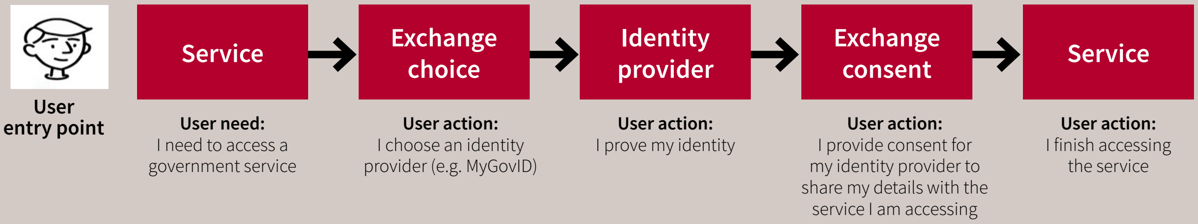
GovPass: the overall system name for the federated identity scheme of the Digital Transformation Agency (DTA). MyGovID will be one of the components of GovPass and will allow people to validate their identity. GovPass is a DTA-led multiagency program in which the DTA plays an oversight, integration and delivery role, working in collaboration with the ATO, the Department of Human Services (DHS) and the Department of Home Affairs.

Trusted Digital Identity Framework (TDIF): the standards that describe the GovPass identity federation, which include provision for multiple identity providers, subject to their accreditation (currently Australia Post's Digital iD and the ATO's MyGovID).[8] This creates consumer choice, but also means that all identity providers need to maintain high security standards if citizens' data is to be protected. The TDIF defines the requirements to be met by government agencies and organisations in order to achieve TDIF accreditation for their identity services (for example, as an identity provider).

Face Verification Service (FVS): a one-to-one image-based verification service that can match a person's photo against an image on one of their government records, such as a passport photo, to help verify their identity. Often, these transactions occur with the individual's consent.[9]

Face Identification Service (FIS): a one-to-many image-based identification service that can match a photo of an unknown person against multiple government records to help establish their identity. Access to the FIS will be restricted to agencies with law enforcement or national security related functions.[10]

GovPass in action



User entry point

Service
User need: I need to access a government service

Exchange choice
User action: I choose an identity provider (e.g. MyGovID)

Identity provider
User action: I prove my identity

Exchange consent
User action: I provide consent for my identity provider to share my details with the service I am accessing

Service
User action: I finish accessing the service

Boston Consulting Group has estimated that digital identity could save $11 billion annually 'through reduced cost to serve, cost of fraud and improved customer experience'.[11] Deloitte Access Economics has estimated 'productivity and efficiency savings of $17.9 billion over 10 years (if we reduce the number of transactions completed via non-digital channels from 40 percent to 20 percent)'.[12] Identity crime is estimated to cost over $2.2 billion annually and affects one in five Australians during their lives.[13] While the government estimates that it costs $17–20 each time someone tries to prove their identity to access a service, the cost of doing so digitally is somewhere between $0.40 and $2.00.[14] Various different schemes are already operational in places such as New Zealand (RealMe), the UK (GOV.UK Verify), India (Aadhaar), Estonia (ID-card), Sweden and Norway (the last two have separate systems, both called BankID).

Digital identity, properly applied, should significantly improve users' experiences when they deal with the public and private sectors. In 2015, 61% of Australians said they had used the internet for their most recent dealings with local, state or federal government, but only 29% were satisfied with their experience, and 58% encountered some problem with the online service. 'The most common issue was that the process was long or difficult (21%). 15% had technical difficulties and for 13%, the service they needed was not available online. 11% couldn't remember their user name or password.'[15] Digital identity should help significantly to alleviate these problems.

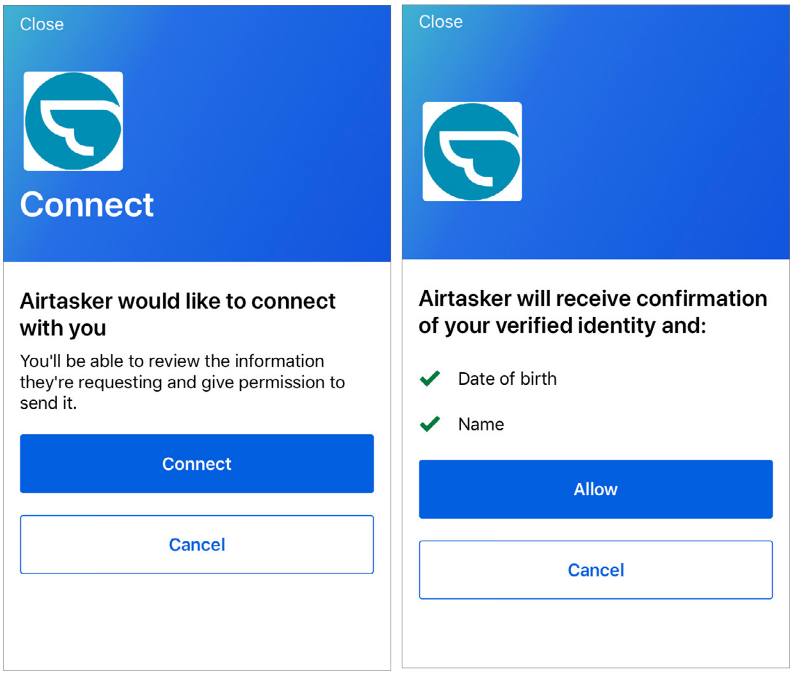
Meet Digital iD and GovPass

The Australian Government is building two competing digital identity schemes. The first one, known as Digital iD, is already operational. It has been developed by Australia Post, an Australian government-owned corporation, at an estimated cost of $30–50 million.[16] The second is GovPass, a scheme being developed by the DTA.

Australia Post's Digital iD now has a product team actively selling access to the private sector. This identity service is already accepted in licensed venues in the Australian Capital Territory, the Northern Territory, Queensland, Tasmania and Victoria, and by companies such as Travelex and Airtasker.[17] For individual users, the scheme is free of charge.

To function, Digital iD uses Australia Post's access to government identity databases as well as private-sector databases, such as credit header records, and postal records. Creating a digital identity is quick and is done over the Digital iD app.[18] It essentially involves verifying your mobile number by entering a code sent to your phone and taking a photo of an identity document (driver's licence, passport or Medicare card), which is checked against the government databases. To validate your ID on, say, Airtasker, you click 'connect' and input your mobile number, and that sends an alert to your phone (Figure 1). Once you open the app, you're notified that Airtasker would like to connect and are offered the option of 'connect' or 'cancel'. If you hit 'connect', you're notified that Airtasker is requesting confirmation of your identity plus your date of birth and name, giving you the option to 'allow' or 'cancel'.

Figure 1: Using Digital iD to engage with AirTasker



Close

Connect

Airtasker would like to connect with you

You'll be able to review the information they're requesting and give permission to send it.

Connect

Cancel

Close

Airtasker will receive confirmation of your verified identity and:

✓ Date of birth

✓ Name

Allow

Cancel

Parallel to the Australia Post scheme, the Digital Transformation Office (now the DTA) was given the task of developing a second scheme, known as GovPass.[19] Underway since 2016 (Australia Post's foundational research on digital identity was also released in 2016[20]), the scheme was initially intended to start public beta testing in mid-2018, but has been delayed.[21] It finally secured $92.4 million in funding in the 2018–19 Budget[22] to create the infrastructure that will underpin GovPass and roll out the scheme, initially for grants management, the My Health Record, Youth Allowance, business registration, NewStart, the Unique Student Identifier and tax file numbers. The government aims to roll out pilot services to half a million users by the end of June 2019.[23]

DHS will operate the exchange or gateway between the services and identity providers, the ATO will be the initial identity service provider,[24] and the DTA will oversee the program. DHS will be the scheme administrator and the operator of the interoperability hub that will provide access to verification services run by or on behalf of other government agencies. Australia Post will be seeking accreditation as an identity provider (alongside the ATO), in addition to maintaining its existing Digital iD system. The range of actors involved in GovPass and the complexity of the model will make it difficult to deliver the project on time and without incident.

Digital iD is distinguished from GovPass mainly by the fact that it isn't a federated model (Australia Post is the only entity through which you can verify your identity for Digital iD). It's envisaged that multiple entities could provide this service under the GovPass scheme, giving consumers choice about which entity they use to prove their identity.

Some companies, such as Mastercard (and likely others) through its My Digital Life program, are positioning themselves to facilitate access to the rich data pools that the digital identity service will enable by serving as a platform through which third-party attribute vendors can sell data on individual Australians. If poorly regulated, these sorts of schemes could create serious privacy issues involving

third-party data access. An indicator of this can be seen in the controversy over Facebook providing personal data to third-party organisations, including Cambridge Analytica. (Australia Post isn't selling access to personal information; rather, companies that use Digital iD to verify their customers' identities are being enabled to easily gather related data, such as purchase history, location and so on, and link it to a confirmed individual identity.)

A key enabler for both schemes will be the FVS, which will be vital for higher level identity checks that are required for transactions requiring greater confidence that someone is who they say they are, such as creating tax file numbers (Australia Post's existing scheme currently performs lower level checks using biographic data). This was made possible by the Intergovernmental Agreement on Identity matching Services.[25] The agreement essentially enabled the federal, state and territory governments to share access to their databases of government-issued photographic identity documents (such as driver's licence and passport databases) for a broad range of applications spanning road safety, law enforcement and identity checking. For identity checking, this will simplify the process of confirming identity, and the photos will enable higher levels of identity assurance. The FVS's creation is enabled by the Identity-matching Services Bill 2018, which at the time of writing is still before the House of Representatives.[26]

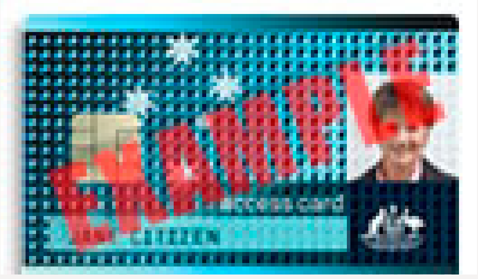
As with the Australia Post scheme, it's envisaged that the private sector will be able to rely on GovPass for identity checking in future. An example of how this would work is Australia Post's Digital iD, which is already used by Australia's largest credit union, CUA, for new members applying for some CUA accounts online or via their mobile devices. This allows accounts to be created in minutes without visiting a branch.[27]

Challenges

The take-up by individuals of digital identity schemes will require the government to overcome challenges in the areas of communication, rights protection, limit setting, coordination, commercialisation and security.

Communication

In all discussions about GovPass, the Australia Card experience looms large, and GovPass has been designed to deliberately distinguish it from previous efforts. The Australia Card was proposed by Prime Minister Bob Hawke in 1985 and eventually led to a double dissolution election before the proposal was dropped. Other failures also overshadow the rollout of GovPass. In 2006, Prime Minister John Howard made another attempt with the Access Card,[28] before it too was shut down by the new Rudd government in 2007.



The government's own polling suggests that it's right to be fearful of scaring the Australian public. Sixty-nine per cent of Australians are more concerned about their online privacy than they were five years ago. A majority (58%) of Australians are 'somewhat concerned' or 'very concerned' about biometric data being used to gain access to a licensed pub, club or hotel (although that percentage is down from 71% in 2013), and 56% are concerned about using biometric information for day-to-day banking and 43% for boarding flights.[29] Only a third of Australians are comfortable with the government sharing their personal information with other government agencies, and only 10% are comfortable with businesses sharing their information with other organisations.[30] The controversy over police access to the My Health Record and the need to add further privacy protections in that scheme also point to heightened public awareness and concern about digitisation processes, including about losing control of personal information that might be used to cause harm.[31]

The DTA has issued regular updates on the progress of the GovPass scheme, but, with few exceptions, the updates haven't been brought to the public's attention by leaders,[32] and there's been very little discussion of the scheme in the media. When the Council of Australian Governments (COAG) announced the key underlying agreement to share identity information and create a national biometric exchange system, the focus was placed on the counterterrorism potential of the biometric database, not the broad digital identity possibilities for the Australian population. As the then Prime Minister said at the time, 'Imagine the power of being able to identify, to be looking out for and identify a person suspected of being involved in terrorist activities walking into an airport, walking into a sporting stadium … This is a fundamentally vital piece of technology.'[33]

Ending the erosion of rights

The shift to a digital world is eroding citizens' rights. With each new digitisation initiative, people are forced to trade off more of their rights for the convenience offered. Repeatedly, they're assured that everything's fine, only to discover that they've been hoodwinked. 'Opt in' becomes 'opt out'. 'Safe and secure', it's later discovered, means warrantless police access. Over time, people are being disempowered, but these initiatives could have the opposite effect if properly implemented and communicated.

Instead of thinking about how digital identity can solve a departmental problem and focusing narrowly on users' experience in that context, a citizen-centric perspective is needed. In a citizen-centred society, the role of government should be as the custodian of citizen data—guaranteeing its security and integrity and the citizen's inviolable rights to and control of their data.[34]

For government, this requires an overhaul in approach. What's needed is a root-and-branch review of how citizen protections can be made fit for purpose in the 21st century and of opportunities to take advantage of digitisation to simplify the web of rules that we created for our paper-based society. Those rules are often needlessly complicated due to misaligned incentives between competing bureaucracies and rent-seekers who have fed off complexity. The Australian Treasury's 'consumer data right'[35] is a step in the right direction to empower citizens, but a far more holistic approach is needed.

Clearer limits are needed

The creation of the FVS and FIS is enabled by the Identity-matching Services Bill 2018, but loose drafting leaves so much scope for unexpectedly broad use of the FIS (for law enforcement purposes) that it risks public backlash against the FVS (which is critical for identity matching). As the backlash against My Health Record demonstrated, sharing without consent is almost certain without well-crafted policy and legislation that's accompanied by an effective public communications campaign.

An important provision of the COAG agreement that establishes the national biometric exchange system is that it can only be used for 'general law enforcement' purposes when suspected offences carry 'a maximum penalty of not less than three years imprisonment'.[36] This key provision is missing from the Identity-matching Services Bill.

In practice, this will mean that for requests between jurisdictions (for example, a NSW agency checking a Victorian's identity), the three-year-penalty rule agreed by COAG would need to be spelled out in interagency agreements. If NSW police wanted to check a photo of a suspect they would need to log the crime the person was suspected of (carrying at least a three-year prison sentence) and then run the check. It's also possible that they could still run the check if the crime carried at least a three-year penalty in NSW, but less than a three-year sentence in Victoria.[37]

For intrastate biometric identity searches (such as NSW police searching NSW databases), it's up to individual states to set any limits on what state police could use the federally run system for (that is, it could potentially be applied to any petty offence). Without clearer restrictions, the FIS in particular is open to serious misuse, especially given the Bill's stated purpose of allowing it to be used for 'preventing' crime.

The parliamentary reviews of the legislation raised multiple concerns about the Bill that are beyond the scope of this paper but point to the need for far tighter controls.[38]

Competing government schemes and lack of oversight

It's unfortunate that Australia has ended up with two taxpayer-funded digital identity systems. How this competition will play out is still to be seen. However, given the differences between the schemes and the groups behind them, it's possible to foresee how it might evolve.

GovPass may dominate for government-linked identity checks, and Digital iD for private-sector identity checks. Australia Post is far more entrepreneurial than most government agencies, and if its scheme continues to operate without dedicated legislation it will also be more attractive to private-sector clients (the private sector's ability to verify identity using GovPass is likely to be more restricted). Another potential advantage Australia Post might enjoy is working to achieve some degree of global harmonisation by working with other international postal services' digital identity systems[39] (although the DTA is considering similar international harmonisation for GovPass[40]).

While the Identity-matching Services Bill governs the use of the biometric FVS, it isn't specifically focused on regulating the GovPass scheme. It's yet to be decided whether dedicated legislation to cover GovPass will be developed. Given the sweeping applications of the scheme and open questions on issues such as liability, potential for misuse and privacy concerns, legislation is needed for both GovPass and Digital iD.

Commercial applications

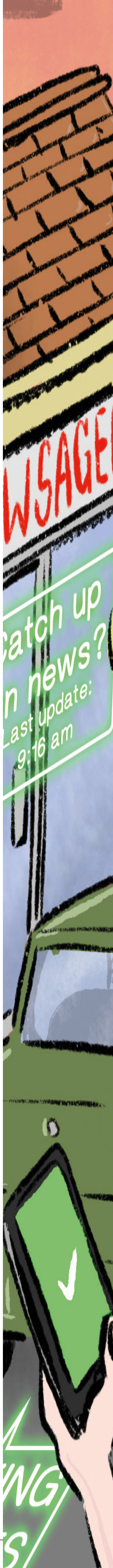
Both digital identity schemes offer significant potential benefits for the private sector. If used, they should reduce identity fraud and theft. Some 69% of Australians are concerned about becoming victims of those crimes,[41] which cost the Australian economy billions of dollars. The schemes will also make it much easier for consumers to transact with businesses and have the potential to better control and manage personal data.

Digital identity will also allow more limited sharing of personal information. At present, most identity checks involve an over-sharing of personal information. The person selling you a beer doesn't need to know your name, home address, driver's licence number, or even your date of birth. They just need a yes/no answer that you are 18 years old or older.

However, without safeguards, digital identity opens up the possibility of serious misuse. With digital identity, the shop assistant selling you alcohol might see less of your personal information but, because they are able to confirm who you are, your purchase information could be on-sold to interested parties, such as your health insurer (affecting your premium) or DHS (affecting your cashless debit card payments). The DTA has advised that it's currently considering establishing an oversight authority, oversight rules, or both, that would seek to prevent the on-selling of data the gathering of which is facilitated through digital identity verification.[42] This sort of oversight is critical for both GovPass and Digital iD.

As we move to a world where identity can be confirmed easily and cheaply, it opens up the possibility of building up profiles of individuals. If digital identity becomes the de facto way to buy alcohol, log on to social media, buy tickets, travel and shop, all of the data that those transactions collect (such as where you are, how much you spend, what you buy and what you look at) can be linked to an individual identity and sold (via your agreement in fine-print terms and conditions) to a third-party profile builder.

Commercial operators are already exploring this possibility. Mastercard (and no doubt competitors), for example, is considering using Australia as the first country to test and deploy its My Digital Life program. This will be a platform through which third-party 'attribute vendors' can confirm different attributes of individual consumers, many of which will be enabled via digital identity. For example, when you engage with a company you have never dealt with before, the company might request half a dozen attributes about you via the My Digital Life app to improve its confidence that you will be a good customer to engage with or are worth offering a higher level of customer service. This might include confirming that you have a perfect credit score, that you always pay your bills on time, that you never



gamble, that you purchase fewer than 20 standard drinks of alcohol each week, that you give at least $1,000 a year to charity and that you volunteer. With your consent, My Digital Life will then request confirmation of those attributes from the third parties who have collected this information to on-sell via platforms such as My Digital Life and will send the results to the requesting company.

The private sector has been a leader in the development of 'know your customer' best practices and privacy protections, and some sharing of attributes (such as credit scores, police checks, speciality licences and working with children certificates) may facilitate commerce and community engagement. However, without tighter constraints, the potential applications of Westernised versions of China's social credit scheme could seriously encroach on basic rights.

Security

It's difficult to provide detailed cybersecurity risk assessments of GovPass (which is still being designed) and Digital iD (for which detailed architectural designs aren't available). However, one area where risks are likely is in spoofing the FVS. Researchers in the US have demonstrated that wearing specially designed eyeglass frames 'can effectively fool state-of-the-art face recognition systems'.[43] Technical means to overcome these immediate challenges are likely to emerge, but this demonstrates that biometrics won't be a panacea for identity fraud.

More broadly, this ASPI policy brief has identified several issues of concern, including the security risks presented by having multiple identity providers, each of which will need to maintain rigorous security standards, as well as the potential for the schemes to be used to facilitate vastly more ambitious profile building of Australians.

There also appears to be no legislative impediment to the ATO using its existing powers to use the GovPass exchange to request information that would allow for data matching—something likely to attract public concern. Data from the ATO-run MyGovID identity service portal could be used to match a particular user with other government services. The DTA exchange is designed at a technical level to resist an identity provider trying to do this sort of matching but won't stop an authority with legislative power to demand the data.

A range of other security-related issues remain open. If either or both of the schemes are widely adopted, it's unclear whether companies could mandate the use of them (for example, for online banking), making them de facto compulsory. It's also unclear whether companies that have traditionally not required validated identity checks could start to do so. For example, companies such as Facebook that have a real-name policy could adopt mandatory digital identity verification for Australian users to enforce that policy.[44]

Opportunity ahead

Despite the challenges, digital identity is critical for a 21st-century economy. Done properly, it will allow citizens to enhance their privacy by sharing less personal information and save time by doing more things online with less hassle. If it's accompanied by an overhaul of citizens' rights, it could put Australians back in charge of their online lives, allow them to monitor and easily contest inappropriate uses of their data, and remove unnecessary regulatory and legislative complexity as the shift from offline to online proceeds.

Features of GovPass

User-centred design

User-centred design is a key principle for GovPass, and the program is being developed in accordance with the Digital Service Standard, which aims to ensure that digital teams build government services that are simple, clear and fast.[45] In addition, the TDIF has a component dealing with usability and accessibility requirements that government agencies and organisations need to meet in order to be accredited under the TDIF.

Privacy

The GovPass platform's conceptual architecture is designed to be consistent with 'privacy by design' principles. Personal information that's essential to provide the requested service will be collected and used with informed consent.[46] Govpass has been designed as a federation of identity providers and an exchange using 'double-blind' architecture. Having the exchange means the service doesn't see your identity documents, the identity provider doesn't know what service you're accessing, and your identity attributes aren't stored centrally. The exchange merely passes those attributes on to the service. It doesn't retain the attributes, but only some logs to record what occurred. The DTA advises that its research suggests that there's community demand for multiple identity providers so citizens have choice for different transactions (for example, using a government provider for government transactions and a private-sector entity for commercial transactions).

Express consent

The GovPass program has been explicitly designed to be 'opt in' for users, although other schemes such as My Health Record have transitioned from 'opt in' to 'opt out'. The exchange will be the vehicle for a user to express consent. Once a user has established their identity through an identity provider, the exchange will ask them to consent for their attributes to be passed to the requesting service (relying party). Unless the user gives explicit consent, the attributes can't be passed on.

Recommendations

1. **Accompany the introduction of digital identity with an overhaul of online citizens' and consumers' rights.**

In democracies, governments exist to serve the citizenry, so it's only logical that the citizen be placed at the centre as far-reaching schemes such as digital identity are introduced. Helpfully, this will also provide the most important ingredient needed for the success of digital identity: trust.

The government should conduct a root-and-branch review of how citizen protections can be made fit for purpose in the 21st century and of opportunities to take advantage of digitisation to simplify rules created for our paper-based society. This should include ensuring that minimum security baselines and rules for data use are maintained, regardless of who has custody of the information (government or the private sector).

The review should look at reforms that provide citizens with easy and meaningful control over their data. It should consider providing citizens with an online log every time their personal information is accessed by any arm of government or the private sector, and with a one-click process for contesting any access they believe may be unauthorised. It should allow citizens to decide who can access different components of their data (such as individual records) and provide strong default settings to protect those who don't bother to adjust their settings.

The Privacy Act should be amended, including to create a principle that all digital identity checks gather only the minimum necessary personal information and where possible in de-identified ways (such as via yes/no answers for proof-of-age verification, rather than date of birth transmission).

2. **Communicate with the public about the schemes and the accompanying rights overhaul.**

After announcing a review to strengthen online citizen protections, the government should lead a national debate on the benefits of digital identity schemes, including by outlining medium- to long-term plans for the schemes and the strengthened protections that citizens will receive to guard against encroachments on their rights. This should include the production of an issues paper that clearly sets out the major implications and long-term plans for digital identity. The paper should be followed up with traditional consultation mechanisms, such as town hall meetings, industry roundtables and media engagement.

3. **Place both Digital iD and GovPass under legislative oversight and protect both schemes from overreach. Expressly prohibit 'social credit' schemes that are facilitated by government-enabled digital identity checking.**

Given that Digital iD and GovPass rely on government identity databases to operate and have far-reaching applications, both schemes should be brought under dedicated legislative oversight. The legislation should place strict limits on information about individual citizens that can be gathered through the use of digital identity verification and on-sold. The development of social-credit-style schemes should be expressly prohibited.

4. Explore options to join the schemes.

Opportunities should be explored to avoid duplication between the two schemes. This could include reviewing whether Australia Post's already operational scheme could be adopted as a national scheme (and GovPass scrapped, although keeping the existing FVS), or strengthened sufficiently so that it is suitable by drawing on the TDIF. At a minimum, Australia Post should replace the ATO as the government identity provider under the GovPass scheme. This would be consistent with one of the DTA's own core procurement principles of avoiding duplication by not building platforms that other agencies have already built.[47]

5. Apply stricter and clear limits on the use of biometrics at the federal, state and territory levels.

The governance of the FIS is largely beyond the scope of this paper, but is still relevant because current overreach threatens to undermine the digital identity schemes. Parliamentary inquiries into the Identity-matching Services Bill have exposed a litany of shortcomings, including inadequate privacy protections, insufficiently precise drafting, potential for overreach, and the key issue that Australians never consented to having their photographs for government identity documents repurposed for use in the biometric identity matching services now being contemplated.

Identity matching uses a relatively benign one-to-one match of a particular user's photo against a reference photo via the FVS (although, as this policy brief has outlined, it could still be seriously misused if sufficient controls aren't in place). The FIS is a one-to-many match of an unknown user against millions of possible matches, which has far-reaching privacy implications and the potential for serious misuse and expansion into many-to-many matching by adjusting the way the FIS works. Specific recommendations to strengthen the Identity-matching Services Bill have been provided in a separate submission to the Parliamentary Joint Committee on Intelligence and Security.[48]

6. Establish a national taskforce.

Discussions with government agencies working on different applications of face-matching services, which include the FVS and the FIS, suggest that second- and third-order consequences of different aspects of the schemes haven't been considered because they fall outside specific agency or department remits. Developments at the state and territory level and within the private sector also need to be considered as part of a national approach that puts citizens at the centre. A taskforce (federal, state and territory) that includes key private-sector and civil society actors should be established to ensure that whole-of-nation implications are considered and addressed.[49]

Notes

1 Financial System Inquiry, *Final report*, 7 December 2014, online.

2 Australian Government, *Improving Australia's financial system: government response to the Financial System Inquiry*, 20 October 2015, p. 15, online.

3 Department of Home Affairs, *Face matching services*, Australian Government, no date, online.

4 Financial System Inquiry, *Final report.*

5 Financial System Inquiry, *Final report.*

6 Michael Keenan, 'Delivering Australia's digital future', address to the Australian Information Industry Association, 13 June 2018, online; Angus Taylor, 'National standards to support government digital ID', media release, 5 October 2017, online; Sara Howard, *Unlocking up to $11 billion of opportunity*, Australia Post, 5 December 2016, online.

7 Angus Taylor, 'What a Govpass digital ID would look like for Australians', media release, 17 October 2017, online.

8 Financial System Inquiry, *Final report.*

9 Financial System Inquiry, *Final report.*

10 Financial System Inquiry, *Final report.*

11 Australia Post, *A frictionless future for identity management: a practical solution for Australia's digital identity challenge*, White Paper, December 2016, p. 7, online.

12 Australia Post, *Choice and convenience drive 'digital first' success*, Insight paper, November 2016, p. 5, online.

13 Parliament of Australia, Identity-matching Services Bill 2018, Explanatory memorandum, p. 3, online.

14 Digital Transformation Agency (DTA), 'Digital identity: enabling transformation', handout, Australian Government; Keenan, 'Delivering Australia's digital future'.

15 Australia Post, *Choice and convenience drive 'digital first' success*, p. 7.

16 DTA, 'Digital identity: enabling transformation' and interviews for this research.

17 Australia Post, *Digital iD*, online.

18 One-off versions can also be created on the Australia Post website.

19 Rachel Dixon, 'Digital identity: early days in the discovery process', DTA, 8 March 2016, online.

20 Australia Post, *Digital identity white paper: a single digital identity could unlock billions in economic opportunity*, no date, online.

21 Taylor, 'National standards to support government digital ID'.

22 Australian Government, *Budget 2018–19: Budget strategy and outlook*, Budget paper no. 1, 2018–19, pp. 1–22, online.

23 Keenan, 'Delivering Australia's digital future'. Level 2 identity verifications don't require biometric verification. Four of the eight services being developed require a Level 2 identity verification and therefore aren't dependent on the FVS.

24 Keenan, 'Delivering Australia's digital future'.

25 Council of Australian Governments (COAG), *Intergovernmental Agreement on Identity Matching Services*, 5 October 2017, online.

26 Parliament of Australia, Identity-matching Services Bill 2018, online.

27 Credit Union Australia Limited, 'CUA leading the way in bringing Digital iD to banking', media release, 8 August 2017, online.

28 Office of Access Card, 'What is the Access Card?', Australian Government, no date, online.

29 Office of the Australian Information Commissioner (OAIC), *Australian community attitudes to privacy survey, 2017*, Australian Government, 2017, pp. i, 21, online.

30 OAIC, *Australian community attitudes to privacy survey, 2017*, p. ii.

31 Dana McCauley, 'Health Minister backs down on My Health Record', *Sydney Morning Herald*, 31 July 2018, online.

32 Keenan, 'Delivering Australia's digital future'.

33 Karen Barlow, 'Turnbull dismisses privacy concerns in asking for a national facial recognition database', *Huffington Post*, 4 October 2017, online.

34 See David McCabe, 'Scoop: 20 ways Democrats could crack down on Big Tech', *Axios*, 30 July 2018, online.

35 The Treasury, *Consumer data right*, Australian Government, 9 May 2018, online.

36 COAG, *Intergovernmental Agreement on Identity Matching Services*, p. 12.

37 There's provision in the COAG agreement to review this after the first 12 months of operation; COAG, *Intergovernmental Agreement on Identity Matching Services*, section 4.25.

38 Parliament of Australia, Identity-matching Services Bill 2018.

39 Sara Howard, *A world without borders*, Australia Post, 19 December 2016, online.

[40] Asha McLean, ‘DTA considering international “brokerage” of digital identities’, *ZDNet*, 9 February 2018, online.

[41] OAIC, *Australian community attitudes to privacy survey, 2017*, p. 33.

[42] The potential oversight authority would have legal authority to enforce operating rules and the TDIF on participants of the identity federation. The operating rules would set out the legal framework for the operation of the identity federation, including the key rights, obligations and liabilities of participants (including relying party services).

[43] Mahmood Sharif, Sruti Bhagavatula, Lujo Bauer, Michael Reiter, ‘Accessorize to a crime: real and stealthy attacks on state-of-the-art face recognition’, *CCS 16*, 24–28 October 2016, Vienna, p. 12, online.

[44] ‘What names are allowed on Facebook?’, *Facebook*, 2018, online.

[45] Financial System Inquiry, *Final report.*

[46] Financial System Inquiry, *Final report.*

[47] DTA, *Digital sourcing framework for ICT procurement*, Australian Government, no date, online.

[48] Parliamentary Joint Committee on Intelligence and Security, Review of the Identity-matching Services Bill 2018 and the Australian Passports Amendment (Identity-matching Services) Bill 2018, ‘Submissions received by the committee’, submission no. 18, online.

[49] GovPass has a steering committee that reports to the Digital Leadership Group and is exploring how to broaden the group.

Acronyms and abbreviations

ATO	Australian Taxation Office
COAG	Council of Australian Governments
DHS	Department of Human Services
DTA	Digital Transformation Agency
FIS	Face Identification Service
FVS	Face Verification Service
TDIF	Trusted Digital Identity Framework

Some previous ICPC publications

When the winner takes it all

Big data in China and the battle for privacy

Lotus Ruan

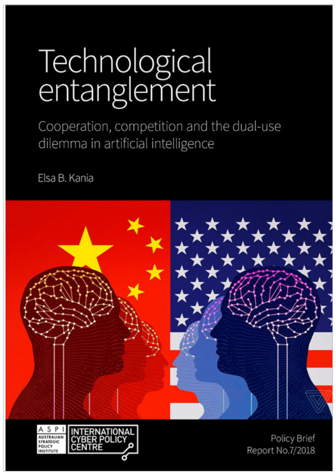
Issues Paper
Report No.5/2018

Social credit

Technology-enhanced authoritarian control with global consequences

Samantha Hoffman

Policy Brief
Report No.6/2018



Technological entanglement

Cooperation, competition and the dual-use dilemma in artificial intelligence

Elsa B. Kania

Policy Brief
Report No.7/2018

A S P I
AUSTRALIAN
STRATEGIC
POLICY
INSTITUTE

INTERNATIONAL
CYBER POLICY
CENTRE