Black Economy Report Biometric Digital Identity

Biometric Digital Identity

The Black Economy Report recommends that there be a once off sign up process for a citizen to give their biometric data (face, fingerprints) that would then be used across all government, licensing, social media platforms. They recommend this is **mandatory** for government interactions. The processes they describe sound terrifyingly risky, see Chapter 4. Later in the Black Economy Report, they openly discuss digital identity theft, identities being sold on the dark web but do not relate it back to this proposed biometric identity system. They don't reference any biometric identity hacks, although there have been hacks of government data bases and top security clearance databases. They seem quite willing to require Australians to give over their biometric data, stating that it will save money and efficiency. They make many unsubstantiated claims in this chapter.
Once biometric data is stolen, it cannot be 'changed' like a password. The person's digital identity is compromised forever. How does this combat identity fraud?!

Black Economy Report Identity
I have listed direct quotes from the report, with some of my comments.

"… It is our perspective that any solution that relies on a physical card or document for enduring identity verification is already outdated, **inherently less secure** and is less convenient. There are a number of advantages that a digital credential has over a card based identity.

- Unlike a physical card a **digital credential cannot be lost or easily stolen** — making it more secure. (Not true. There are multiple cases of digital identity theft, some from government agencies. The Black Economy Report talks about digital identities being stolen and sold on the dark web in another section)
- An enduring biometric marker that is verified upon each use ensures identity cannot be falsified or used by someone else the way point in time data stored on a card can be. (Not true. Biometrics can and have been falsified, with serious consequences)
- A physical solution, such as a card, does not translate into an online environment. (Nonsense. We use cards online all the time! And below they advocate for a 'physical solution'- smartphones!)

Current identity verification processes are not sustainable, secure or efficient. **Individual identity is arguably less secure than it has ever been** (Where is the evidence for this? I would say that 'less security' is because of the ability for digital data to be hacked and stolen)

Identity verification has remained largely paper based. (Has it? I upload digital images of my passport for KYC/AML)

Individuals have multiple identity profiles across institutions requiring the maintenance of multiple accounts, usernames and passwords. Establishing these accounts often requires the provision of the same (or similar) sets of information often either provided in person or

as a certified original. (Nope, I haven't had to provide in person documents for years, I send photos of my passport etc)

Once established, **it is often only a username and password** that are required to access services (sometimes coupled with a SMS or email confirmation). This does little to ensure the individual using the service is who they say they are. **It also means individuals have to remember multiple logins and passwords.** Removing these inefficient processes and replacing them with **a single reusable digital identity** will significantly reduce compliance costs and reduce red-tape for individuals and businesses. (One single reusable biometric digital identity would be a honeypot for hackers. Once biometric data has been stolen it can never be recovered- you can't 'change a password', you need new fingerprints or a new face!)

Community attitudes towards the use of biometrics have changed as technology has advanced; indeed we use biometrics in many daily interactions such as unlocking our phones by fingerprint, using voiceprints with the ATO and facial recognition as a part of crossing international borders. **These advancements should be harnessed to strengthen identity processes.** (Facial recognition technology databases at US borders were recently hacked and the info stolen)

The reliance on outdated physical methods of identity verification and the requirement to maintain multiple separate profiles **could be justified if it had eliminated the ability of individuals to game the system** and either disguise their identity or impersonate the identity of others. This has not been thecase. The ability of individuals to circumvent current processes and exploit the system has created mistrust, has resulted in poor service delivery and allows those with false identities to proliferate in the black economy. (Biometric data has been stolen, recently in US Customs agency, tope clearance security firms and US Federal Agencies)

The existence of markets for stolen and fraudulent identity documentation shows that this risk is real. It is estimated that every 20 seconds an Australian is a victim of identity crime.12 This shows that our existing KYC and related processes have been undermined. (There is a market for stolen digital identities. Why create more centralised data bases, of **biometric, unchangeable** information if 'the risk is real'?)

A widely accepted single source identity verification framework that operates across the economy (encompassing **private, business and government** interactions) and is secured through biometric means will **reduce the proliferation of false identities**, correct issues of **poor-quality data**

A **digital identity verification service** that allows individuals to easily prove their identity and provide **validated credentials to government and private institutions... improve the data integrity of registries and data bases across both the private and public sector.**

While the implementation of the service should span multiple platforms, **the proliferation of smartphone ownership** and the increasingly central role they play in the delivery of services **make these devices ideal for facilitating a new identity paradigm.**

Institutional trust will play a significant role in the successful delivery of any identity

verificationsystem. In selecting a preferred provider, the Government will **need to assure individuals that the organisation providing the service and holding the data will not expose or otherwise share their information** (intentionally or otherwise) beyond what the user has agreed to or authorised. Beyond this, **a provider who is not inherently tied to either the private or public sector** could better facilitate broad take-up of the identity credential as a verification process. (Who is this? Someone will be set up ready to take this role on and make $$ from it)

Similarly, **it is likely perceptions and concerns of privacy risks will be raised.** However, a properly designed and implemented proposal in line with what is presented here will **reduce risks to individual privacy by better securing and enhancing control individuals have over their information.** The solution proposed here will also be able to operate without requiring that individuals provide any additional information to Government or private sector firms beyond what they currently do. It is the existing system that has failed to protect individual privacy; this proposal will correct those faults. (Evidence of this at all being true?? They don't list any research beyond their opinion)

To put beyond doubt issues of privacy, the Government could consider implementing a **set of data-protection principles similar to the General Data Protection Regulation** that has been adopted in Europe which provides individuals with certain rights and **imposes certain obligations on entities in relation to personal data.** Any use of this data requires explicit consent from the owner. (Interesting they mention this because there was recently a huge leak of citizen information and the European Commission insisted the General Data Protection Act **did not apply to them) https://www.express.co.uk/news/world/967585/gdpr-eu-personal-data-hack-leak-personal-data-brussels**

This should be considered in light of the **existing provisions within the *Privacy Act*** which class **biometric information as 'sensitive information',** meaning it attracts greater protections than other personal information. Most notably, this includes a default rule in Australian Privacy Principle 3.3 that **entities can only use sensitive information with consent,** and in the case of agencies, for a purpose that is reasonably necessary for the agency's functions and activities. (But the Black Economy Report said that the **secrecy provisions we currently have are outdated** and should be replaced with a new Data Sharing Act)

One option would be for the Government to keep the framework standard closed and only allow a single provider to deliver the identity service. This has clear benefits including control over accessand the potential to mitigate perceptions of security issues. However, it creates a single point of failure, potentially limits innovation and creates privacy issues. Alternatively, **allowing the underlying identity framework to be open to allow other trusted entities to develop identity services** will encourage the convergence of private and public sector approaches to identity, support consumer choice and **facilitate ongoing innovation in the sector.** (Who are these trusted entities!? Why are they allowed to contribute? Terrifying.)

P82 We recommend the introduction of a single individual identity to allow individuals to instantly and securely prove their identity using a digital identity credential, secured

biometrically, when dealing with Government. This does not involve an identity card. It does not involve a government database of biometric information. (Then how does it work? With a private database of biometric information? They don't make this clear)

P84 There are also a range of **private sector institutions** that have begun to utilise biometrics and other technological advancements to improve identity verification processes. (Apple etc)

P87 The development of a common identity framework across the whole of the Commonwealth is required to allow individuals to quickly and securely prove who they are and then, through the us eof a biometrically secured digital credential, use their proven identity. The use of this credential should only **require individuals to prove who they are once** and be reusable across (This sounds **much less safe** that KYC with documents such passports!!)

P87 A set of credentials uniquely and securely linked to an individual: The identity should be uniquely and securely linked to an individual using multiple factors such as **face and finger biometrics**, pin numbers, message tokens and other emerging techniques **(including social media).**
Mandatory across government: Use of a digital identity, through a biometrically secured digital credential, should be mandatory in all dealings with Commonwealth agencies where identity verification is required, including online, in-person and over the phone. (THIS IS NOT OPT OUT)

This is the process they describe, **it does not sound secure at all!!!**
Establishing the credential:

1. An individual downloads the identity app onto their connected device.
2. The individual enters into the app, one time only, key identification details (for example: name, date of birth, passport number, etc.) and captures a 'selfie'.
3. The identifying details are checked against data held by issuing Government agencies through the Document Verification Service.9 The 'selfie' is verified against the Face Verification Service.
4. The identity is created and secured to the individual within the device using pin, fingerprint and face biometrics.

Using the credential:

Individuals use the secured credential to prove who they are in all dealings with Government seamlessly providing information **through their device either through automated background processes**, on command, through a scannable code, or potentially via near-field communication technology.
- Automated background processes- is this constant monitoring in the background?
- Near-field communication technology: a method of wireless data transfer called NFC (Near field communication) that detects and then enables technology in close proximity to communicate **without the need for an internet connection.**

The UK's VERIFY service launched in May 2016 with similar aims to what is proposed here. To date, t**he service has failed to achieve wide uptake.** This has been **attributed to the opt-in nature of the service** (both for the Government and individual) which has failed to incentivise both sides to make full use of the services... There is a general view that there needs to be a complete re-think of how the UK government delivers these services. (I am assuming this re-think involves making the service mandatory, like they have suggested for us)

Singapore Personal Access (or SingPass), which launched in 2003, is a gateway to hundreds of digital services offered by more than 60 government agencies, enabling users to only have to remember one password when connecting and transacting with the Government. Recently the Singapore Government announced it would enhance this service through the incorporation of biometric identification and an **open identity interface** which will allow **the private sector to integrate theSingPass digital identity into their services.** (So the services starts out as government only , and then when they have captured everyone's biometrics and data, they open it up to the private sector.

P182 Agencies need to be able to share information and data in order to effectively coordinate action; such information and data sharing is **currently too constrained by secrecy and privacy provisions that are not fit for purpose,** as well as **organisational cultures and technology platforms that impede information sharing.**

Black Economy Reports comments about the Dark Web/Identity Theft

P288-289
"… Criminals are able to carry out fraud in **online banking and identity crime.** As well, they are able to facilitate criminal trade in a low-risk manner (for example, by using the dark web... It also draws attention to the increasing opportunities for money laundering (including through cryptocurrencies... and alternative banking systems).
The internet has provided organised criminals with new opportunities. **Hackers can access personal information and steal identities, … can be traded via the dark web,** and **ransomware can be used to lock people's data unless they pay for it to be returned**.

Criminals also seek to identify and engage with **corrupt public officials who can help them circumvent or compromise regulatory processes and systems.** This is a particular risk where **a single official has broad discretion to make decisions which create value** and also where they are responsible for oversight of, for example, security matters…

Organised criminals are also heavy users of the dark web... **sell information from hacked government databases (including, for example, Medicare cards**).

The dark web provides access to internet content generally via specific software or authorisations.Content on the dark web is not indexed by search engines and its hosting

and access is **entirely anonymous due to the use of layered encryption which makes it impossible to track users…**."

Some breaches

Biometric Security Systems
The biggest known biometric data breach to date was reported recentlywhen researchers managed to access a 23-gigabyte database of more than 27.8m records including fingerprint and facial recognition data.
This breach highlights a major problem with biometric security systems that effectively use people's biological measurements as passwords. Unlike usernames and passwords, biometric data can't be changed if it is stolen.
https://theconversation.com/stolen-fingerprints-could-spell-the-end-of-biometric-security-heres-how-to-save-it-122001

Biometric Federal Agencies
On Wednesday, the Office of Personnel Management said hackers stole 5.6 million fingerprints it had on file. That's significantly higher than the agency's original estimate of 1.1 million fingerprints.

This is extremely sensitive information that poses an immediate danger to American spies and undercover law enforcement agents. As an OPM spokesman told CNNMoney in July: "It's across federal agencies. It's everybody." Hackers now have a gigantic database of American government employee fingerprints which can be used to positively identify the true identities of those employees. https://money.cnn.com/2015/09/23/technology/opm-fingerprint-hack/index.html

US Customs facial recognition data
CBP statement said none of the image data had been identified "on the Dark Web or Internet." But reporters at The Register, a British technology news site, reported late last month that a large haul of breached data from the firm Perceptics was being offered as a free download on the dark web.
"This is a bombshell," said Evan Greer, deputy director of the advocacy group Fight for the Future, in response to the reporting. "Even if you 100% trust the U.S. government with your biometric information (which you shouldn't) this is a reminder **that once your face is scanned and stored in a database, it's easily shared across government agencies, stolen by hackers, other governments, etc.**"
https://www.salon.com/2019/06/11/facial-recognition-data-collected-by-u-s-customs-agency-stolen-by-hackers/