UNISYS | Securing Your Tomorrow®

Why it’s time to trust digital ID

By David Chadwick

Fear of being controlled is usually tempered with the desire to be safe and secure.

The idea of being monitored or watched has never sat well with humans. A quick look at the action flicks on your favourite streaming service will serve up a host of bleak dystopian thrillers where citizens have lost control of their personal information, privacy, and freedom.

However, our fear of being controlled is usually tempered with the desire to be safe and secure.

Citizens around the globe are currently being asked to contemplate this compromise with the introduction of government-led COVID-19 tracking and tracing apps.

In Australia, the COVIDSafe app records contact between registered users. According to Government Services Minister, Stuart Robert, health authorities only utilise the data gathered when a registered user tests positive to COVID-19, to help identify who they have been in contact with.

Use of the app in Australia is on a voluntary basis only, with the government stating that fines and gaol sentences will apply to any person or business that attempts to strongarm individuals into using the app.

While the payoff for registering to use the app is clear – more control over the spread of this deadly virus – for many the concept of government-led monitoring is too high a price to even consider.

In fact, most attempts to introduce identity-based digital security solutions at a national level in Australia have been met with outrage and cries of distrust. Whether it is the use of technology, such as biometrics or facial recognition apps, or a digital platform to facilitate the online identification of citizens, such suggestions are often pilloried by civil rights groups, politicians, and the media.

The information collected by government organisations that forms a person’s digital identity is highly sensitive and should be treated with the utmost respect and security. Citizens should never hesitate to question who can see it, how it will be used and where it is stored.

But what if citizens thought differently about their identity? What if citizens saw their identity as a powerful asset, not a tool for control or setting limits?

Every human has the right to be recognised as an individual and has a right to an identity.

Our personal information, from our name, date of birth, gender and nationality – everything that’s recorded on our birth certificate and passport identify us as a citizen of society who is able to enjoy essential social services such as health care, education and judicial protection.

Without an identity we are invisible. In fact, without proper ID documents, we have no power before the law.

Common Myths About Identity

Here are four myths we need to bust to start seeing our digital identities as a national asset.

Myth 1: The Government Collects Data to Spy on Us

When the Australian Government introduced the My Health Record to make it easier for patient information to be shared between health providers, a sense of unease settled over the nation.

Talk of ‘big brother’ style monitoring and concern about who would have access to our private medical information ran rife. The debate around the My Health Record platform highlighted a clear lack of understanding about the way data and information is handled by different departments.

While just one in every ten Medicare members made the decision to opt out of the My Health Record platform, the ongoing dialogue on privacy demonstrates a clear need to educate and empower citizens about their rights when it comes to their personal information and data.

Unisys’ own research has also shown that Australians do not have a clear understanding of how information is used by government departments, with the vast majority (90 per cent) believing government agencies already share citizen demographic data with each other, when they generally don’t.

In Australia, each government department acts as a silo and is bound to keep citizen data and information separate by strict legislation. Government workers are not spending their time cross-examining data and information to ‘catch citizens out’ or ‘spy’ on them – nor do they have any interest in doing so.

What government agencies do, on a daily basis, is confirm a person’s identity when they need a service or require support.

90 per cent of citizens believe government agencies share their demographic data with each other, when they generally don’t.

Confirming a person’s identity is required when they present in person at an office or service centre, over the phone and increasingly it is required to determine a person’s identity when requesting online support.

Proving our identity online is the current challenge for government departments and law makers alike; especially when you consider the very rapid move into the online world as a result of COVID-19.

Myth 2: People Can Steal Your Identity

Pick up a newspaper or take a quick scroll through your Facebook homepage and you will sight an article, friend or relative discussing ‘identity theft’.

However, it isn’t their identity that’s been stolen, it is the identity *information*, or the credential. Identity fraud can be committed, but identities cannot be stolen. If we implement proper security practices and systems, the use of a well-anchored identity can prevent fraud.

For example, compare the difference between a typical driver licence and the gold standard of credentials: an Australian passport.

If your driver licence was lost or stolen it would be quickly replaced, however, the sting is that your old licence will remain valid until it expires. This is because the licence number never changes and there are no credentials in place to check that the cardholder is who they say they are. The credential is compromised – not the person. The credential has a weakness that criminals have learned to utilise and that is because it is a licence to drive, not an identity credential.

Passports on the other hand, have a number unique to the document and the document holder. If a passport is reported missing, the passport number will be immediately and irrevocably cancelled.

If someone uses that passport to try and leave the country, they will fail as the identity credential will have been revoked. The passport could still be used in other use cases, but anything that involved the document verification service (DVS) would immediately pickup that the credential is no longer valid.

Biometric technology, such as the highly effective SmartGate systems used at Australian borders, further reinforce the value of biometric identification by ensuring that only the passport holder themselves can use the document to travel. It’s a strong credential being used in a strong system with very few weaknesses to exploit.

Myth 3: Online Verification Systems Equal Mass Surveillance

Since the introduction of CCTV in 1942, we've become accustomed to the fact that our movements on our way to work, catching public transport or having a drink at the local pub are being captured. But this is not proactive video surveillance – these recordings can only be used for analysis after an incident has occurred.

Mention the use of biometrics and public monitoring and the response is instant panic. You are no longer just a face in the crowd, but an identifiable individual whose every move can be tracked.

Implementing a system to actively monitor a public place, with real time facial recognition, that matches individuals against a large number of identities, is extraordinarily difficult to do with any form of accuracy. The simple reality is that the effectiveness of mass video surveillance is over-stated by some technology companies and industry commentators.

Recent analysis of the use of video surveillance in the UK has highlighted that the error rates are too high to be used as anything other than a tool that suggests potential persons of interest to police. This is no different, in reality, to police carrying photos of wanted persons and talking to potential matches as part of their duties.

If police agencies plan to trial, or implement, a facial recognition-based surveillance system, they need to be upfront and transparent about how the system is being implemented and for what purpose. As a society, we gain nothing if the technology that is meant to protect us undermines our sense of freedom and erodes trust in the bodies responsible for public safety.

Citizens need to have a clear understanding of when and how these systems and solutions will be utilised, in order to be able to trust the agencies that are using them.

Citizens need a clear understanding of when and how these systems will be utilised.

Myth 4: An ID Database Would Be a Honeypot for Thieves and Hackers

Another myth doing the rounds is the idea that an identity system creates the ideal honeypot to attract hackers and ID thieves. If this were the case, then every national ID scheme in the world would have been hacked by now – including our own passport and drivers licence systems.

The reality is that these are not simple databases that can be hacked – they are well designed identity ecosystems that have been architected to ensure that no biometric data can be replaced to hijack an identity.

Being anchored with a biometric enables uniqueness of identity to be confirmed and actually helps a citizen recover from a major incident such as a bushfire or the total loss of identity information – by verifying their identity against the biometric record, their identity can be instantly confirmed – effectively like crossing the border and confirming your identity against your passport record.

The Future of Identity Credentials

Single Use Credentials

Australian organisations and government departments must adopt the use of credentials that can be cancelled and not reactivated. For example, our driver's licence number stays the same even when a new card is issued. With each new card there should be a new number.

One of the most critical aspects is determining uniqueness of identity – this is paramount for having confidence in the identity and being able to trust it. The focus moving forward will be on utilising data points that truly make us individuals.

Verification of Identity

Expect to see greater utilisation of Face Verification Services to verify you against an authoritative source.

It’s up to government and industry to **educate** the public in clear and simple terms.

David Chadwick, Director of Identity and Biometrics for Unisys in Asia Pacific.

David has 18 years’ law enforcement and 12 years of federal government experience, with the past 14 years being specifically focused on identity and biometrics.

He can be reached at David.Chadwick@unisys.com

More Verification Services for Everyday Activities

Anticipate the use of further identity credential-based systems for high risk transactions such as banking and superannuation. Significant identity verification will become a part of normal practices and processes.

The Way Forward

Organisations, industry and Government must start speaking the same plain language to allow members of the public to understand how their identity provides them with access and control, not the other way around.

The next step is to separate the terms ‘identification’ and ‘verification’. For example, there is a distinct difference between a Face Identification System (FIS) that enables law enforcement agencies to search or match faces and the Facial Verification Service (FVS) that allows an individual to confirm their identity using their own passport or drivers licence records.

It is critical that the public understands the difference between the two and that government, the media and industry all play their part in clear and open communication on the topic.

The Digital Transformation Agency, and other government departments, will look to use the FVS to enable citizens, on a voluntary basis, to confirm their identity to a high level of assurance to enable them to conduct higher levels of transactions online – creating a Digital Credential that can be used as needed. This is a revolutionary concept and one that makes use of the national asset that is currently held, but not utilised – identity records.

Finally, the security and public sector should consider a complete rebrand of the term ‘Digital Identity’ to ‘Digital Credential’ or ‘Digital ID’ to elevate the purpose of this technology.

Unisys research shows that when the public is informed and agree with the purpose of security measures, they are more likely to strongly support them. For example, the 2018 Unisys Security Index™ revealed that 65 per cent of respondents were comfortable with using biometrics to facilitate faster travel through airport border processing.

It is up to all of us in Government, industry and the biometrics sector to educate the public in clear and simple terms so that they can understand that the future fight against fraud lies in our ability to utilise effective verification systems, and that neither identity nor biometrics are the enemy.

About Unisys

Unisys is a global information technology company that builds high-performance, security-centric solutions for the most digitally demanding businesses and governments. Unisys offerings include security software and services; digital transformation and workplace services; industry applications and services; and innovative software operating environments for high-intensity enterprise computing.

To learn more about digital government services,
visit www.unisys.com/smartdigitalgovernment
or contact unisysapac@unisys.com.

For more information visit www.unisys.com