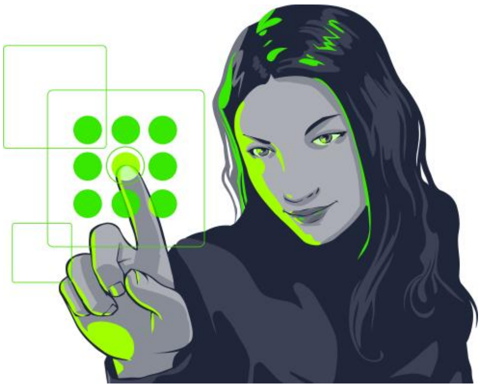
Adaptation and the Digital Disruption of Identity



Introduction

Did we not see the digital era coming – and the role that identity would play?

Headlines such as these…

"The economic impact of identity crime in Australia has been estimated to exceed $1.6 billion every year" … and

*"…data integrity problems undermine the operation of the Australian Business Register as the single source of truth for whole-of-government business registrations"…*send serious warning signals.

Australia used to be well known as an innovator, at the forefront of online / digital service delivery by government, but in recent years has fallen well behind the progress made by many other economies. At great economic cost.

And the clues as to this appalling situation can be found hiding in plain sight – in the Australian government's own reports.

There were three significant reports released by the Government in the second half of 2014, all of which made significant findings in relation to identity. These reports were: the Report of the National Identity Crime and Misuse Measurement Framework (the Identity Crime Report); the Report of the Murray Inquiry into the Financial System (FSI Report); and the report by the Australian National Audit Office (ANAO) into the Administration of the Australian Business Register (ABR), report number 48.

There are several concerning aspects of these reports when read together. The first is that the findings in these reports could ever be seen as surprising or novel, as if the issues had not been identified or considered previously by government. The second concerning thing is that it does not appear that other commentators have linked the common threads across these reports. More profoundly, these reports taken together paint a picture of systemic weakness driven by fractured processes, and fragmented siloed approaches across the "individual" and "business" domains in the digital identity ecosystem in Australia.

Digital identity is about far more than the identity of the individual. Whilst the topic of digital identity of the individual in Australia has been contentious, the ANAO ABR report highlights systemic problems with the integrity of the business identity (ABR) data. Across the board, there are major deficiencies throughout the identity ecosystem regarding validation, notification and assurance processes. Furthermore, there is no policy framework around reciprocity and digital credentials – and the looming challenge of digital identity and the Internet of Things has not yet entered the policy context and narrative of service delivery, at least in Australia.

The submission from the Centre for Digital Business (*"No Welfare Reform without Digital Payments Transformation and Digital Identity Strategy")* to the Murray Financial System Inquiry gained traction with a call to action for a digital identity strategy for Australia. The issues identified are resonating in digitally progressive economies such as Singapore and the Netherlands, where I recently delivered a keynote address at the European Digital Identity Conference - IDNext Conference – and was a judge in the 2015 European Digital Identity Awards.

This paper, *"Adaptation and The Digital Disruption of Identity"* not only draws the link between the reports and the issues, but does so against the historical context of digital identity in Australia – and in full view of the increasingly profound and pervasive role of identity in the digital era. This paper further highlights some inconvenient truths, drawn from the government's own reports, regarding digital identity imperatives across the individual and business domains.

Clearly, "truisms" at the time of the Access Card no longer apply. The "single identity, single card, single issuing authority" model of just nine years ago is not necessarily the best model for today, and certainly not for the future. Many commentators still confuse the various concepts related to identity, as if a card would resolve all issues.

Futhermore, commentators who viewed the Access Card program as not having delivered a "card", have no understanding of the extent to which the architecture and knowledge survived the cessation of the program.

If the debate does not include reciprocity, interoperability and customer choice, then we are stuck, and will remain stuck, in last century. Therefore the development of a framework for digital identity must without compromise include a view of the future and adaptation.

As with digital disruptions in other domains, the digital disruption of identity is being defined by the rise of the platforms which challenge and change the economics of the fragmented siloed and legacy bespoke solutions and processes.

There are inconvenient truths in these reports which can be summarized as follows:

That clearly, the 19th and 20th century identity structures and processes in Australia are ill-equipped to sustain the digital demands of the 21st century.

19th and 20th century identity structures and processes in Australia are ill-equipped to sustain the digital demands of the 21st century

In essence, what is offered is a perspective on the underlying fractures described in these government reports. The Centre for Digital Business has been undertaking research and development into a possible solution to Australia's digital identity dilemma. What is proposed is a set of principles to guide the development of a digital identity strategy for Australia: *the Adaptive Digital Identity Framework©.*

This is not from an academic or theoretical perspective, but from a practitioner who has carried the responsibility of design and implementation of digital identity capabilities in the business and individual domains across sectors of government in Australia.

The Inconvenient Question

On 21 October 2014, the Australian Government released its report of the National Identity Crime and Misuse Measurement Framework (referred to here as the Identity Crime Report) as part of the National Identity Security Strategy. This Identity Crime Report is compelling reading for a number of reasons. It claims to be the first attempt by any government worldwide to "systematically measure the incidents and impacts of identity crime" and it is well worth having a look at the methodology.

The report estimates that the economic impact of identity crime to Australia is likely to exceed $1.6 billion every year.

According to the Identity Crime Report, every year the personal information of an estimated 1.7 million Australians is stolen or misused (Australia has a population of 23 million people.)

This makes identity crime one of the most prevalent personal crime types in the country.

In bringing together available data from over fifty different Australian Commonwealth Government, Australian State and Territory Governments, as well as the private sector, the Identity Crime Report provides an insight into the fragmented status of the national identity infrastructure in Australia. Read in an historical context of initiatives over the past two decades, the Identity Crime Report illustrates the economic impact suffered as a result of Australia's fragmented approach to digital identity.

In addition to the vulnerability issues highlighted in the Identity Crime Report, the strategic challenges related to identity are also described in the Report of the Financial Systems Inquiry (FSI Report). So central is the role of identity – and digital identity – to the economy and the performance of the financial system, that the FSI Report called out that Australia "…has not yet developed a detailed approach for the future of digital identities" and "…does not have a single over-arching technology strategy in place."

And the challenges extend into the business identity domain. The ANAO Report into the Administration of the Australian Business Register (ABR) report highlights systemic problems with the integrity of the business identity (ABR) data, and the completeness and accuracy of entity data. In a profoundly serious finding, the ANAO describes these deficiencies as undermining whole-of-government objectives.

Across the board, there are major deficiencies throughout the identity ecosystem regarding strategy, governance, standards, data integrity and assurance processes.

With this commentator's long involvement in digital identity from both a business and individual perspective, the Centre for Digital Business submission gained traction with the Final FSI Report referencing the Centre for Digital Business submission. The Centre for Digital Business submission *"No Welfare Reform without Digital Payments Transformation and Digital Identity Strategy"* drew the link between digital identity and the transformation of service delivery and emphasised the importance of enabling continuing innovation in identity solutions.

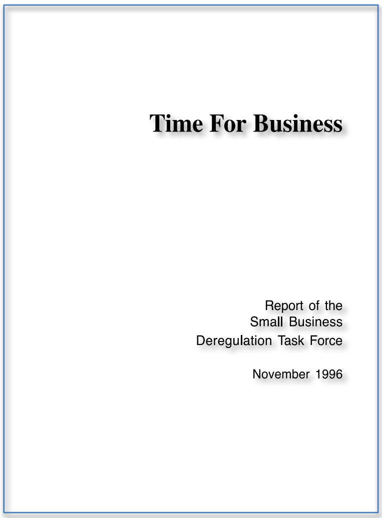
Together, these three government reports describe the situation, but what is the cause? What are the disruptive forces at play – the shifts – that are challenging government administration and service delivery so profoundly in the digital era?

How can it be, that across governments in Australia, governance in relation to identity is weak; processes are not followed; data integrity not maintained; duplicated initiatives fester; and the underpinning systems and processes suffocated by complexity, fragmentation and a lack of a strategic architecture.

This is like having an air traffic control system designed and managed differently at each airport. It is interoperability, trust and confidence in the whole system that is ultimately affected.

This inconvenient question causes some inconvenient truths over the past few decades to be examined across the business and individual domains – and the rapidly evolving domain of the Internet of Things.

The Inconvenient Truth - Business Identity



Time For Business

Report of the
Small Business
Deregulation Task Force

November 1996

The role of digital identity for business has a significant economic impact, as outlined in the Australian Information Industry Association (AIIA) submission to the National Commission of Audit (NCOA) in November 2013. The AIIA submission states:

"In 1996, the Howard Government commissioned a review into the compliance burden faced by business across the three levels of government – the Bell Report ("Time for Business") estimated the compliance burden to be some $17b per annum (17 years on and with the increased scope and complexity of government administration and regulation, it can be assumed that the compliance burden would be multiples of that figure.) Accepting all the recommendations of the Report, the Howard Government subsequently introduced strategies such as the single business identifier for business (the Australian Business Number), and electronic single point of entry for business (the Business Entry Point), and electronic authentication for business. In the digital age, further strategies are required to streamline the interaction between business and government – particularly small business to reduce the compliance burden and drive economic productivity."

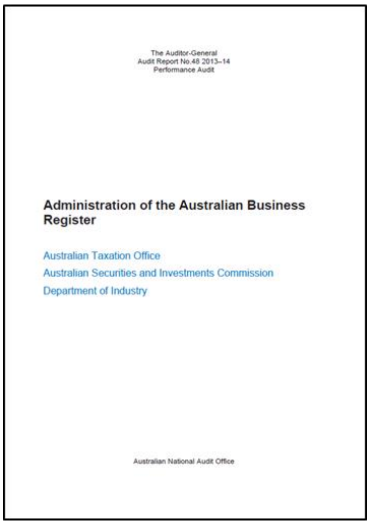
The introduction of the New Tax System in 2000 was a national economic driver for addressing aspects of business identity with all business required to register for an Australian Business Number (ABN) – this was the unique identifier for business. I led the Business Entry Point in collaboration with the Australian Tax Office to deliver the ABN online registration process. The delivery of the ABN was lauded and awarded as a significant achievement in government transformation at the time.

The ABN has always been about business identity to facilitate the interaction between businesses and all levels of government in Australia. The purpose from the outset was beyond taxation.

For the first time, all businesses in Australia had a unique business identifier – a national platform of business identification. On the basis of this platform, other business identity initiatives were both trialed and implemented. The Business Authentication Framework (the BAF), and authentication brokerage services with the implementation of Vanguard, a very significant whole-of-government capability. Other business identity and authentication innovations were also trialed, such as the digital professional credential. The digital professional credential has the potential to radically transform the way in which credentialed professionals such as builders and engineers engage with government and other providers seamlessly and completely online. All this is dependent upon strong data integrity of the ABNs.

The findings of the ANAO ABR report regarding the continuing problems with the integrity of the ABR data and particularly "the number of entities on the register and incomplete and inaccurate entity information on the ABR" illustrate the profound risk to the achievability of whole-of-government transformation strategies.

The ANAO is a conservative and measured institution, not prone to making dramatic statements. Yet it bluntly calls out that "…there has been limited progress in achieving whole-of-government objectives for the ABR" and that "…shortcomings undermine the operation of the ABR as providing the 'single source of truth for whole-of-government business registrations'."



The Auditor-General
Audit Report No.48 2013–14
Performance Audit

Administration of the Australian Business Register

Australian Taxation Office
Australian Securities and Investments Commission
Department of Industry

Australian National Audit Office

And it is the ANAO that calls out the inconvenient truth, a truth that many businesses engaging with government in Australia already know. That the ABN, intended to be the unique identifier for businesses in Australia (in fact it started out being called the UBI, Unique Business Identifier), is now no longer unique. And worse.

The ANAO ABR report goes on to describe the complexity and subsequent fragmentation of the ABR IT environment, which is impacting the operations of other agencies as well as Australian businesses.

One of the inconvenient truths is that this situation is not about the IT system of the ABR. The ABR always was an economic *platform* not an IT system subject to the internal discretions of an agency, ie the ATO. It is irreconcilable that – in the face of the increasing compliance burden of duplicated processes overwhelming businesses – that the ANAO describes improvements to the ABR being constrained by the ATO internal budget cuts and priorities.

As an economic platform, there is different governance required and an enforceable strategic capability architecture, not an IT systems architecture.

The ANAO provides a damning summation:

“Rather than being the unique identifier for business to meet regulatory obligations, and to reduce business registration requirements and entry points to government as intended when introduced in 1999, a number of initiatives with similar purposes have subsequently been established. As potential efficiencies provided by these schemes have not been achieved, businesses are required to provide the same information to different agencies, or different parts of the same agency.”

These metastasized manual repetitive processes across government not only drive inefficiencies across public administration, but seriously impact economic productivity. Deloitte released a report in 2014 “Get Out of Your Own Way: Unleashing Productivity” that estimated the economic burden of rules, regulations and processes imposed by government to be $95 billion per annum. This number overshadows the 1996 compliance burden estimate of $17 billion per annum.

The very harsh reality is that the siloed approach in the digital age, has compounded the impact of the compliance burden. “Digital” – without transformation – is not only superficial, but regressive.

This is the same inconvenient truth for individuals (see following section): that business and individuals are required to provide the same information to different agencies, or different parts of the same agency. That government outcomes are compromised by a fragmented and siloed approach – but as in other domains such as banking and retail, the rise of the platforms generates different economic models enabling far greater performance and innovation.

The rise of the platforms in government challenges the silos of agencies and silos within agencies and demands a rethink of models, governance, and accountability of public administration in the digital era.

The Inconvenient Truth – Identity of the Individual

The challenge of introducing a digital identity framework of the individual has been even more contentious.

Over the past decade, the challenge of navigating government has become more complex – not easier – notwithstanding the various "online government" agendas.

The past decade also saw the initiative to introduce a national smartcard into Australia – the Access Card – and it's deeply concerning to contrast the underlying risks at that time back in 2006 with the risks described in the Identity Crime Report last year. I was the Chief Technology Architect of this national digital identity platform program designed to deliver a smartcard capability, reciprocity framework and architecture to strengthen Australia's identity infrastructure. This smartcard project called the Access Card, was terminated on political grounds in 2007 following a change of government.

This paper does not advocate for a re-run of the Access Card program or the introduction of any particular token, but rather the need for a bold whole-of-government strategy of interoperability driven by standards across the digital ecosystem to break through the intractable issues driven by the current agency-by-agency paradigm.

In the years since the cessation of the Access Card program, the world economy has been transformed by technology and new economic models in digital payments and digital identity. However, the lack of a digital identity framework and overly complex and rigid payment arrangements remain as the common root cause of both inefficiencies and a significant constraint on innovation in government service delivery.

Passport
NATIONAL IDENTITY SECURITY STRATEGY
Identity crime and misuse in Australia
Key findings from the National Identity Crime and Misuse Measurement Framework Pilot
IDENTITY SECURITY

The Identity Crime Report characterises Australia's national identity infrastructure as a "…complex federated network…in which around 20 government agencies manage over 50 million core identity credentials". These credentials include driver's licences (issued by six Australian states and two territories), passports, Medicare cards, birth certificates and visas. In addition to this 50 million government identity credentials, there is a further comparable number issued by private sector and non-government organisations.

The Identity Crime Report notes that "…while the primary purpose of these credentials was not to serve as evidence of a person's identity, they have become increasingly used in this way throughout the community." Furthermore, Australia's identity ecosystem is highly dynamic: each year hundreds of thousands of identity credentials are updated or re-issued as people change their address or get married or learn to drive.

The Identity Crime Report goes on to describe "the system that Australians rely upon to help establish and verify their identities…is an interdependent network of systems that has evolved over time by practice and convention, not necessarily by design." This is an ecosystem of interdependencies, whereby "…each agency that issues identity credentials within Australia relies upon those issued by other organisations to help verify their clients' identities."

In this system of interdependencies "…a breach of identity security in one organisation can have potentially serious 'downstream' consequences for the identity of an individual or another organisation, and affects the strength of the network as a whole."

Whilst the Identity Crime Report describes Australia's identity infrastructure as "federated", a more apt description would be that it is a fragmented infrastructure suffering from a lack of design, a lack of an enforceable architecture, a lack of strategic investment and reform by a range of credential issuing authorities, and a lack of widespread utilisation of the underpinning verification services.

Notwithstanding the national identity strategy policies that have been in place and updated during the past decade, delivery appears problematic.

Weak and Vulnerable Credentials

The Identity Crime Report documented significant problems with weak and vulnerable credentials in use across the identity ecosystem.

There is a range of identity assets, capabilities, services and processes that could be considered to constitute the identity ecosystem architecture: policies and strategies; government registers; government issued credentials; proof of identity (POI) processes; private sector issued credentials (such as bank cards); and verification and notification services.

Many of the government issued credentials used to establish and prove identity, have little or no security features and according to the Identity Crime Report, the price of fraudulent identity credentials "…suggests they they are relatively cheap and easy to obtain." According to the Australian Federal Police, "…the price of fraudulent identity credentials

ranges from around $80 (Medicare cards) to around $350 (driver licences)…" and these prices were not for the most recent versions that contain state-of-the-art security features.

Furthermore, according to the Identity Crime Report "…the fact that Medicare cards are the cheapest fraudulent credential on the black market suggests that they are relatively easy to produce, particularly in light of the fact that they contain very few security features, such as facial image or hologram."

This was a known vulnerability that was to be addressed by the Access Card program back in 2006.

Credentials that are in ubiquitous use and with weak security features (such as Medicare cards and driver licences) are more likely than other credentials to be used to facilitate identity crime, according to the Identity Crime Report. The combined risk profile of "ubiquitous use and weak security features" underscores the importance of verifying the information presented on these credentials with the issuing agency.

While not initially intended to be used as an identity document, in practice driver licences have become the key identity credentials used by Australians. Given the reliance on these weak feeder documents, the findings of the Identity Crime Report are of considerable concern. Of the eight road transport and licensing agencies, only two advised to the Identity Crime Report that they had data and information about incidents of fraud.

The vulnerabilities of one of the driver licensing systems (ie the underpinning driver licence register) were famously highlighted in the 2007 Report of the Victorian Ombudsman "Investigation into VicRoads Driver Licensing Arrangements". The Ombudsman's report found that the Victorian driver licensing system was vulnerable to corruption. Victoria Police advised that "…the pattern of [organised crime] using false driver licenses stems from the ease of obtaining them and the inability of VicRoads to detect them once fraudulently issued."

Following the 2007 Ombudsman's Report, VicRoads used facial recognition software over a four year period (2007-2010) to audit around 700,000 licenses, which identified 600 suspected frauds.

Illustrating the systemic vulnerabilities stemming from weak government credentials and processes, the Identity Crime Report referenced the 2011 inter-agency investigation and busting of a sophisticated fake credit card syndicate. In raids in Sydney, police "…found 12,000 blank credit cards and hundreds of blank New South Wales driver licences in addition to equipment and computer files used to manufacture fraudulent documents. It is estimated that the fake credit cards could have been used to complete $30m in fraudulent transactions."

At the time of the publication of the Identity Crime Report, only two of the driver licensing authorities – the Western Australian Department of Transport and VicRoads were reported to have "…undertaken projects to use facial recognition technology to help identify fraudulent driver licences."

Notification and Verification Processes

In addition to the vulnerabilities stemming from weak government credentials, there are systemic vulnerabilities as a result of weak processes and practices to do with notification and verification of credentials in use. According to the Identity Crime Report:

"The price of fraudulent birth certificates indicates that these documents are more widely available than these figures would otherwise indicate. This is likely because most government agencies and private sector organisations do not have arrangements in place to notify the relevant Register of Births Deaths and Marriages (RBDM) when they detect a certificate that is suspected to be fraudulent. It is likely therefore, that RBDMs are not notified of the majority of incidents involving fraudulent versions of their certificates."

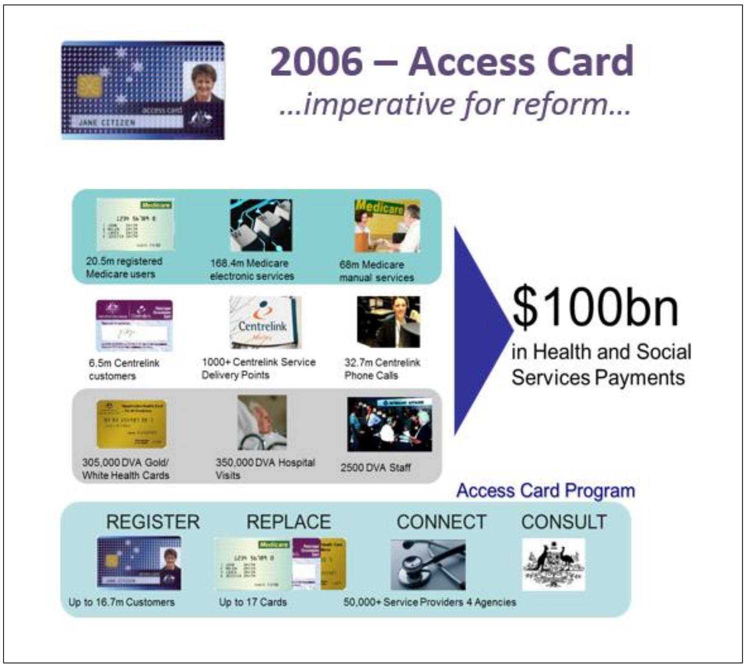
The Document Verification Service (DVS) is a national online system that allows organisations to compare a customer's identifying information with a government record. It enables user organisations to match the biographical data presented on identity credentials with the issuing authority. The DVS was to be a key pillar of the Access Card program, as it has been long recognised that this verification service strengthens the evidence of identity processes for government and the private sector. There is an increasing number of identity credentials that can be verified through the DVS including those at most risk or misuse (Medicare cards, driver licences, birth certificates and passports).

Originally, the DVS was only available to government agencies. However, and in contrast to the limited usage of the DVS by government agencies, there is strong demand for use of the DVS amongst private sector organisations. In 2012-2013 Australian governments decided that the use of the service should be extended to private sector organisations particularly those with legislative obligations to verify the identities of their customers.

Notwithstanding that the DVS is a critical component of the identity infrastructure in Australia, there is currently limited usage of the DVS by government agencies with only one of the eight Road Traffic Authorities and RBDMs currently using DVS.

Systemic Vulnerability from Manual Processes and Outdated Technology

The identity processes and card security vulnerabilities highlighted in the Identity Crime Report have been known for many years and were among the key drivers for the Access Card program almost 10 years ago. The vulnerabilities in these government-issued POI credentials and POI processes had and still have significant ramifications for the government's service delivery arrangements.



2006 – Access Card

...imperative for reform...

20.5m registered Medicare users

168.4m Medicare electronic services

68m Medicare manual services

6.5m Centrelink customers

1000+ Centrelink Service Delivery Points

32.7m Centrelink Phone Calls

305,000 DVA Gold/ White Health Cards

350,000 DVA Hospital Visits

2500 DVA Staff

$100bn in Health and Social Services Payments

Access Card Program

REGISTER REPLACE CONNECT CONSULT

Up to 16.7m Customers

Up to 17 Cards

50,000+ Service Providers 4 Agencies

In April 2006 the Australian Government announced the introduction of a health benefits, veterans' and social services Access Card to replace up to 17 existing Australian Government benefits plastic and paper cards and vouchers. It was designed to utilise smartcard technology underpinned by biometrics to streamline and modernise the delivery of Australian Government health and social services. It was to enable people to obtain Australian Government benefits in a straightforward, convenient and reliable way without having to re-register and repeat the same information each time they visit an Australian Government office.

The underpinning KPMG Access Card Business Case (Public Version) went on to describe the problems with the (then) current services system.

In 2006

- Consumers confronted with an array of different service standards, different service access points and different standards of POI in each agency.
- There are multiple registration points and some consumers having to repeat the same information to different agencies and often provide the same proof of identity (POI) information to the same agency if they want a different service.
- There are multiple cards for different concessions and entitlements, many are paper based – in all, there are 24 cards in use in the Department of Human Services (DHS) service delivery system
- DHS agencies are overly reliant on face-to-face interviews with 110 million face-to-face transactions each year.
- Customers spend 90 seconds to 4 mins proving who they are, every visit.
- Cannot authenticate consistently face to face.
- More than 20% of the applications provide the wrong information and documents, requiring multiple return visits.

Compare the situation in 2014. Notwithstanding the billions of dollars that has been spent on technology over the past decade – and acknowledging the considerable progress has been made in some areas - the Australian Government service delivery and associated processes remain largely manual and highly repetitive. This is not a criticism but a statement of fact.

In 2014

- Many of the 170 million face-to-face transactions were to prove identity, up from 110 million in 2006.
- All the multiple cards including paper based cards are still in use.
- Almost 35 per cent of government transactions are still carried out manually (face-to-face, over the phone, by correspondence, etc.)
- Of those are carried out 'digitally' it is unclear what percentage of these are actually completed end to end online.
- Government agencies still manage over 105 million voice calls per year.
- Some 250 million letters are still sent by the Commonwealth each year.
- Only 17 federal government agencies provide 'smart forms' to assist engagement with clients/customers.

Clearly over the past decade, the challenge of navigating and dealing with government has become more complex, exacerbated by the fragmented approach to identity.

Access Card – Architecture and Interoperability

The Access Card was not intended or planned to be an identity card, but this was widely misrepresented and misreported in the media and by commentators. This was mainly caused by the nature of the legislation and policy in that both would enshrine the mechanism of delivery ie via the "card". The legislation further proposed to enshrine the design of the chip and the data model. The legislation for the UK Identity Card (2006) similarly would enshrine the nature of delivery in the legislation. Enshrining a system and delivery design into legislation is always a flawed policy strategy in that it is not focused on the desired policy outcomes, and risks locking in design gaps and obsolescence.

The significant achievement of the Access Card program was the breakthrough thinking and work on architecture, interoperability and standards, not only in government but across the economy.

Again, commentators who viewed the program as not having delivered a "card", have no understanding of the extent to which the architecture and knowledge survived the cessation of the program.

The challenge however is for policy adaptation to enable reciprocity and interoperability which will stimulate an ecosystem of service delivery innovation.

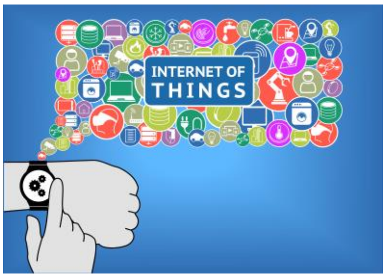
Consider the collaboration on the smartcard interoperability standard ISO 24727. The Access Card team collaborated with Queensland Transport (which at the time was developing its smartcard driver's licence); the Australian Government Information Management Office (AGIMO) and the US Government National Institute of Standards and Technology (NIST). The importance of ISO 24727 was that it would underpin service delivery infrastructure interoperability and enable an ecosystem of services interoperability. The ISO ratification was a very significant achievement.

ISO 24727 was developed in conjunction with a framework of reciprocity. This meant that any smartcard compliant with this interoperability standard (such as a smartcard driver's licence or smartcard bank card) and issued within the identity framework would be reciprocally accepted for the purposes of POI, and potentially payments. Furthermore, this interoperability framework also meant that compliant smartcard credentials could be used for the purposes of online authentication to both government and financial services.

A trusted identity framework would mean that other strong and trusted credentials – such as bank credentials which are issued under the Anti-Money Laundering (AML) legislation requirements – could be used by customers if they so choose for online authentication to government services. This is the extension of the paradigm of a customer of a bank using their bank credential to access their funds by authenticating at another bank's ATM.

Standards and a framework of trusted reciprocity in an adaptive digital identity framework could drive this transformational level of interoperability; eliminate manual and repetitive processes; and achieve strong assurance. This still remains an opportunity to be realised.

Identity and the Internet of Things



The three government reports taken together highlight weaknesses and vulnerabilities of processes and systems regarding both business identity and individual identity.

But the need for a digital identity strategy is even more pressing as we consider the rapidly expanding horizon of the Internet of Things (IoT). The IoT is already here but the evolving concept of identity and IoT is as yet untouched territory of policy or service delivery considerations, at least in Australia.

Gartner, Inc. forecasts that 4.9 billion connected things will be in use in 2015, up 30 percent from 2014, and will reach 25 billion by 2020. The Internet of Things has become a powerful force for business transformation, and its disruptive impact will be felt across all industries and all areas of society. (Gartner Symposium/ITxpo 2014, November 9-13 in Barcelona, Spain.)

What has the Internet of Things to do with identity? The answer is everything and the context is pervasive.

Sensors, devices and applications seamlessly and autonomously sending, receiving and analysing data will drive innovation and new economic activity: the Internet of Things is disruptive and will be a transformative driver in service delivery, policy formulation and analysis.

However, the Kantara Initiative, a digital identity think tank (https://kantarainitiative.org) presents some confronting questions regarding identity and the Internet of Things

- How will devices preclude impersonation of the other devices with which they exchange data?
- Will owners/users have the ability to prevent their devices from being discovered?
- If an auto manufacturer owns data collected by a vehicle, will it require consent from the vehicle owner and service provider?

Clearly the domains of business, the individual and "things" are not stand alone. A digital Identity framework must encompass a cohesive contextual and interdependent narrative across the business, individual and IoT domains.

It needs to encompass a framework for identity and the Internet of Things, and an engagement on standards, taxonomies and policies across the technology, academic and research sectors.

In the digital era and the rise of the Internet of Things, policy adaptation relating to identity will be a profound challenge.

Adaptation – the Different Philosophical Approach Needed

Identity underpins the functions of government and is key to enabling the transformation of service delivery. Identity underpins privacy; strengthens transparency and governance; promotes empowerment; and is an essential factor in economic activity.

In the eight years since the cessation of the Access Card program, the world economy has been transformed by technology and new economic platforms in digital payments and digital identity. Recognising some phenomenal advances that have been made in some areas, strategically in government the lack of a digital identity framework remains as the common root cause of both inefficiencies and lack of innovation in government service delivery.

The absence of a highly reliable and consistent digital credential and framework of reciprocity has constrained the efficiency of service delivery, and locked out the opportunities for policy and service delivery innovation.

This is a significant policy failure and market failure. It is a symptom of the inability to adapt.

Furthermore, the Identity Crime Report observed that "while not traditionally considered as critical infrastructure, Australia's identity management systems have many of these characteristics. In the event that these systems are compromised or become unavailable for any length of time, there could be significant impacts on the Australian economy."

The causes of the problems described in the Identity Crime Report, the FSI Report, and the ANAO ABR Audit are due to siloed structures, fractured and duplicated processes, lack of an enforceable architecture and weak governance and accountability across the identity ecosystem.

Notwithstanding the range of identity policies in place, decisions about various aspects of Australia's identity infrastructure continue to be taken on an agency by agency basis; jurisdiction by jurisdiction basis; and issue by issue basis.

These local decisions have system-wide and economic impact, as illustrated by the Identity Crime Report.

Effectively, there is no digital identity strategy – in any of the domains, individual, business, and "things".

What we see is the 19th and 20th century bureaucratic structures and processes of agencies ill equipped for the demands and power shifts of the digital era.

19th and 20th century paradigm - "the authority of the agencies"

The 19th and 20th century paradigm can be described as "the authority of the agencies". This paradigm is characterized by agency systems; the dominance of the silos; manual, repetitive and discretionary processes; discretionary investments in agency systems; duplicated investments; lack of an architecture; ballooning red tape; and no understanding of the customer experience notwithstanding 20 years of "citizen centric" intentions.

21st century paradigm - "the architecture of the platforms"

In the 21st century, by contrast, we see the rise of the platforms across the global economy which changes business models and the economics of industries. The 21st century paradigm can be characterized as "the architecture of the platforms". Payments is one example of a platform. The emphasis shifts from agencies and individual enterprises to platforms; there is the dominance of architecture and standards, which catalyses the evolution of identity concepts such as the Internet of Things and makes possible unprecedented levels of process automation and adaptation.

In the 21st century, investment and maintenance of the platforms cannot be subject to agency discretion as in previous centuries – and the effects of which have been laid bare in the ANAO ABR audit and the Identity Crime Report.

In the digital era, different investment models and governance is needed in digital identity platforms in order to sustain confidence and trust in the whole ecosystem.

Unlike the supposed "citizen centric" approach of the 19th and 20th century, the 21st century is characterized by the shift in power to "customer choice driven by the customer experience".

The unavoidable and inconvenient truth is that the silos are being rendered obsolete and ineffectual by the rise of the digital platforms and the power shift of the digital era.

The challenges and the approaches of the past twenty years cannot be repeated in the next twenty years.

A Framework for the Next Twenty Years

The preceding summary and analysis paints a grim picture of Australia's identity preparedness for the digital economy. Some of the critical requirements for a digital identity are almost self-evident but many are not, and all must be accommodated into an evolving ecosystem.

Furthermore, 'truisms' at the time of the Access Card no longer apply. The "single identity, single card, single issuing authority model" of just nine years ago is not necessarily the best model for today, and certainly not for the future. Therefore the development of a framework for digital identity must without compromise include a view of the future and adaptation.

Finally, some of the earlier digital identity work, such as the ABN, is currently failing to meet requirements according to the ANAO ABR report. This is not because the ABN was faulty, it was lauded and awarded at the time and was embraced by industry and government alike. Rather it is because there has been no appropriate governance of the ABN within the context of the entire digital ecosystem, allowing government agencies and others to create and issue business identities in competition with the ABN. This is not just maverick behaviour by other agencies; the ABN has not evolved to meet changing needs and therefore the new needs that have arisen have been met through alternative identities.

In short, even the existing digital identity components must be re-evaluated, not just with a view to repair them, but to test their value or otherwise to the overall resilience and robustness of the digital identity ecosystem.

The Centre for Digital Business has been undertaking research and development into a possible solution to Australia's digital identity dilemma. We see the need for an "Adaptive Digital Identity Framework©" that can meet current and future digital identity requirements through managed evolution. The following paragraphs highlight some of the characteristics of this framework that we have identified so far. Some might go on to be founding principles of the framework, others might not make the cut. Exciting times lie ahead as we contemplate the adaptation of digital identity!

Principles of the Adaptive Digital Identity Framework©

In the digital era and the rise of the Internet of Things, ecosystem-wide policy adaptation relating to identity will be a profound challenge.

As in biology, the process of adaptation describes any alteration in the structure or function of an organism or any of its parts that results from natural selection and by which the organism becomes better fitted to survive and multiply in its environment.

And here is one illustration of why a different philosophical approach of adaptation is needed.

A commentator recently stated that "identity was done" given the Government's announcement of the Digital Transformation Office, and the emphasis on myGov and the call for a digital identity framework. The history of the past twenty years shows that identity is never "done" – and given the absence of public policy dialogue on identity and the Internet of Things, further illustrates this very point.

Such rigid thinking presents a clear and present danger to innovation and the efficiency of public administration and economic productivity.

Such rigid and siloed thinking is one reason why – in the digital era – the annual compliance burden in Australia has gone from $17 billion in 1996 to $95 billion in 2014. If we don't take a significantly different philosophical approach, far from being the vanguard of innovation and transformation, "digital" will magnify the inefficiencies and rigidities of the siloes and destroy customer value. "Digital" is already a significant magnifier of inefficiencies.

In the context of the principles and the different philosophical approach proposed, a brief reflection on adaptation, contestability and customer choice is important.

The Australian Government National Commission of Audit Report (NCOA) of 2014 went into some detail to propose the myGov service as the centrepiece for an aggressive digital by default strategy. The Centre for Digital Business strongly supports NCOA's objective for an aggressive digital by default strategy, however cautions against anointing any particular service as the centrepiece of the digital strategy.

There is in fact no concept of a centrepiece in the digital ecosystem. It is standards and adaptation that drive innovation, not government monopoly.

Adaptive means that various reports of government, industry and research sector are "read" together; and signals and issues considered and responded to systematically and systemically.

Similarly, the digital identity framework will need to be adaptive to better support the economic ecosystem and avoid the systemic fractures described so clearly in these reports.

Big data and analytics will influence the adaptation.

Taking the different philosophical approach of adaptation for the next twenty years, means that ***new services not yet created*** would evolve to provide customers with far greater choice and an increasingly contextual customer experience. In a framework of interoperability and reciprocity, government could seek to leverage these new services and platforms, not compete with them.

The lessons from the past twenty years outlined in this paper show that standards matter and far from constraining innovation, provide a platform for experimentation and innovation. The significant contribution from the Access Card to public administration – notwithstanding the program's termination – was the architecture and standards survived the cessation of the program, and were taken up not only in government but across the economy.

Similarly, the lack of adherence to standards and architecture, and the proliferation of bespoke business identifiers across government has impacted the whole-of-government operations of the Australian Business Register.

"Contestability" in the digital age – even for government – will be driven by standards and customer choice.

This framework of adaptation is necessary to support innovation, and the emergence of services, concepts and models not yet created.

To summarise the lessons and challenges presented in this paper, the Centre for Digital Business has developed the following "Principles of the Adaptive Digital Identity Framework"©.

"Principles of the Adaptive Digital Identity Framework"©

1. An *ecosystem* approach must be taken and a healthy ecosystem adapts to maintain confidence and trust.
2. The whole digital identity ecosystem and its *components* must be considered – registers (government, non-government and social); processes; data standards; credentials; tokens; services; things; and concepts that are not things – such as sound.
3. All *domains* must be considered – the individual, business and "things" – and the adaptive philosophy means that other evolving domains and concepts become part of the Framework over time.
4. All *sectors* across the economy must be encompassed.
5. Interoperability and the customer experience across *jurisdictions* must be encompassed given the borderless nature of business models.
6. The principles of *reciprocity, interoperability and contestability* will be enabled by standards.
7. *Standards must evolve* and adapt to drive innovation.
8. The role and emergence of *platforms* must be encompassed in terms of governance, risk and leverage.
9. Adaptive Digital Identity Framework© will be *privacy enhancing*.
10. Reciprocity and contestability will enable *customer choice*.
11. Customer choice will be driven by the *customer experience*.
12. Identity is highly *contextual* in the digital era.
13. The role of biometrics, genome data and other data such as personal fitness and behavioural data must be carefully considered given the evolving *"Internet of the Person"*.
14. The *architecture* of the Adaptive Digital Identity Framework© must be enforced across government.

Stop Admiring the Problem – and Adapt

This paper and the proposal of "Principles of the Adaptive Digital Identity Framework"© is offered as a contribution to public policy dialogue, not from an academic perspective, but from a practitioner who has carried the responsibility of design and implementation of digital identity capabilities in the business and individual domains across sectors of government.

This has included designing and delivering many of the digital identity capabilities of government – referred to in this paper and which are in fact, digital identity assets of the economy. Capabilities such as the Australian Business Number; the Business Entry Point; the Business Authentication Framework (the BAF); professional digital credential trials; the early design work of authentication brokerage services that led to the implementation of Vanguard; Access Card; the BasicsCard; and the Immigration Online Account.

Many of these capabilities are now at the centre of the digital strategy for government.

Far from perfect – a fact which underscores the need for a framework of adaptation – and we need to be forward looking.

What was innovative and entrepreneurial in the development of these capabilities, was the focus on architecture, standards and the customer experience.

The Australian Federal Government Budget of 2015 announced a number of significant measures to start addressing the problems described throughout this paper. The establishment of the Digital Transformation Office and the focus on the development of a trusted digital identity framework is a very important and positive move by government. As stated earlier, the final report of the Financial Systems Inquiry referenced the submission from the Centre for Digital Business which called for innovation in payments, the development of a digital identity framework, and the establishment of a "*Digital Transformation Commission*".

Also in the Australian Federal Government Budget of 2015 is a significant measure to streamline business registration to develop a single online portal for business and company registration; publish new computer code to enable developers to build new registration software; and reduce the number of business identifiers.

Both of these measures are necessary and urgent and clearly in response to issues raised in many government reports some of which are referenced in this paper.

However, given the very significant investments in digital capabilities over the past twenty years mentioned above, the measures in the Australian Federal Government Budget of 2015 could be described as repair measures. Although repair is necessary, the focus must be forward looking, innovative and different.

How did this situation arise – and with past performance not being an indicator of future success – what should we do differently?

Actually, this situation is not new, has not arisen suddenly and has been brewing for some time. The evidence of the digital disruption of identity has been hiding in plain sight for many years – and in many of the government's own reports.

For too long, we have been captivated by admiring the problem and fixated with measuring the wrong things, lulled into believing that such activity is progress.

What has changed over the past twenty years has been mass penetration of telecommunications infrastructure; the pervasive adoption of Internet standards; the rise of different and borderless business models; and changing demographics and societal expectations of service and connectivity.

Government has not adapted to these changes. Clearly over the past two decades, the challenge of navigating government has become more complex – not easier – notwithstanding the various "online government" agendas.

What we have not done, is to adopt a fundamentally different philosophical approach. In relation to digital identity, that different philosophical approach is a framework of adaptation, as proposed through the Adaptive Digital Identity Framework©.

The very harsh reality is that the siloed approach in the digital age and over the past 20 years, has compounded the impact of the compliance burden and made government more complex and costly.

The temptation will be to admire the problem - to be captivated by its apparent complexity – and then reach for a quick-win digital solution. Quick wins will not address the underlying fractures so clearly identified and described in these three Commonwealth Government reports.

The challenge – is to remain future focused on re-invention with a twenty year forward horizon, not captivated in a cycle of repair of the past twenty years. The only way to navigate this challenge of the digital disruption of identity is to change the momentum across the ecosystem through a different philosophical approach of adaptation.

~~~~~~
~~~~~~

About the Author

Marie Johnson is the Managing Director and Chief Digital Officer of the Centre for Digital Business. An experienced public entrepreneur, CIO and CTA, Marie has delivered significant technology, innovation and digital services transformation programs across taxation, business, social services, payments and immigration operations in the Australian Government. Jointly with the ATO, Marie led a team on the implementation of the Australian Business Number (ABN) registration, and subsequently initiatives on business authentication. Marie was the Chief Technology Architect of the Australian Government Health and Human Services Access Card program. At Microsoft, Marie was the Worldwide Executive Director of Public Services and eGovernment based in Redmond USA. In this role, Marie was the joint author with Dr Jerry Fishenden of the Microsoft Strategy "The New World of Government Work", and led Microsoft's strategy for identity in government.

Marie is sought after internationally as a speaker, commentator and thought leader on topics such as digital disruption, digital identity, egovernment, transformation and innovation. Marie collaborated with Dr Jerry Fishenden from the UK on a major paper "A tale of two countries: the digital disruption of government". This paper was a twenty year historical comparison of the online / egovernment strategies of Australia and the UK and was delivered at the biennial conference of the Commonwealth Association of Public Administration and Management (CAPAM) in Malaysia in October 2014, and subsequently published in the CAPAM Innovation Review. In November 2014, Marie was invited to address a special session of the United Nations ESCAP in Bangkok on "ICT, e-Government and Women's Empowerment". In April 2015, Marie was a keynote speaker on digital identity at the European Digital Identity Conference IDNext in The Netherlands.

In 2006-2007, Marie was named "Innovative CIO of the Year – Australia". In 2013, Marie was named one of Australia's "100 Women of Influence".

Marie is a Board Director of the Australian Information Industry Association (AIIA), a member of the NSW Government ICT Advisory Panel, which advice on transformation and ICT strategic directions for the NSW Government, and a member of the NSW Digital Government Taskforce. In 2015, Marie was appointed as the Head of the Technology Authority for the National Disability Insurance Scheme; and Co-Chair of the Digital Careers National Committee. Marie has an MBA (Melbourne Business School); Bachelor of Arts; Harvard University John F Kennedy School of Government Senior Executive Fellows Program; and a Graduate of Australian Institute of Company Directors. Marie is a contributor to CIO Online (Australia) www.cio.com.au and to The Mandarin www.themandarin.com.au.

Notes

- Marie is currently writing a book on the *Access Card* program in Australia.
- This paper "Adaptation and the Digital Disruption of Identity" is available at www.centre-for-digital-business.com
- Related articles including the recently published "A Tale of Two Countries: the Digital Disruption of Government" are also available at www.centre-for-digital-business.com.

References

- Centre for Digital Business Submission to the Financial System Inquiry and the McClure Welfare Reform Consultation "No Welfare Reform without Digital Payments Transformation and Digital Identity Strategy". 4 August 2014. http://fsi.gov.au/consultation/second-round-submissions/
- http://www.ag.gov.au/RightsAndProtections/IdentitySecurity/Documents/IdentityCrimeAndMisuseInAustralia.pdf
- The Financial System Inquiry 2014 (David Murray AO - Chair) - Interim Report - released 15 July 2014
- The Financial System Inquiry 2014 (David Murray AO - Chair) - Final Report - released 7 December 2014
- Administration of the Australian Business Register conducted by the Australian National Audit Office (ANAO), report number 48. 23 June 2014. http://www.anao.gov.au/Publications/Audit-Reports/2013-2014/Administration-of-the-Australian-Business-Register
- Australian Information Industry Association (AIIA) Submission to the National Commission of Audit (NCOA), November 2013. http://www.aiia.com.au/resource/collection/F22C309D-816A-467D-9A09-473D98C7F3A2/13126DRAFTCOAFinal.pdf
- Deloitte report "Get Out of Your Own Way: Unleashing Productivity" 2014. http://www2.deloitte.com/au/en/pages/building-lucky-country/articles/get-out-of-your-own-way.html
- Report of the Victorian Ombudsman 2007. "Investigation into VicRoads Driver Licensing Arrangements". https://www.ombudsman.vic.gov.au
- KPMG Access Card Business Case (Public Version). http://pandora.nla.gov.au/pan/65938/20070207-0000/www.accesscard.gov.au/various/kpmg_access_card_business_case.pdf
- Australian Government Attorney General's Department – Identity Security: www.ag.gov.au/identitysecuritywww.ag.gov.au/identitysecurity
- Document Verification Service: www.dvs.gov.au
- Gartner Symposium/ITxpo 2014, November 9-13 in Barcelona, Spain.
- European Digital Identity event 2015 "IDnext Conference". http://www.identitynext.eu/en/events/the-european-digital-identity-event-2015/
- Kantara Initiative, a digital identity think tank. https://kantarainitiative.org
- Australian Government Federal Budget 2015. http://www.budget.gov.au/index.htm

~~~~~~
~~~~~~