Identity of a nation

Protecting the digital evidence of who we are

Anne Lyons

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

Policy Brief
Report No. 12/2018

About the author

Anne Lyons is a visiting fellow with ASPI's International Cyber Policy Centre. She has worked in both the public and private sectors for more than 20 years, including 15 years as a senior executive. She has enjoyed a broad range of roles, including policy, service delivery, strategic media and issues management, and communications and marketing. She is currently an assistant director-general at the National Archives of Australia. Prior to taking up the visiting fellowship at ASPI, she was the Archives' chief information officer.

Acknowledgments

The author would like to thank all those who kindly gave of their time and expertise when researching this paper, and for all the reviewers who provided comments, particularly Davina O'Dell. Thanks also to ASPI colleagues Melissa Liberatore, Eliza Chapman and Bart Hogeveen for their assistance and Danielle Cave, Fergus Hanson, Tom Uren, Paul Barnes and Michael Shoebridge who provided invaluable insights, guidance and feedback which greatly improved the final product.

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

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 December 2018

Cover image: '*Faces of Australia*' from the National Archives of Australia. Design by Lora Maricic.

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE
INTERNATIONAL CYBER POLICY CENTRE

NAA NATIONAL ARCHIVES OF AUSTRALIA

Identity of a nation

Protecting the digital evidence of who we are

Anne Lyons

Policy Brief
Report No. 12/2018

Contents

Foreword

By far the greatest part of Australia's discourse on cybersecurity is focused on the protection of systems: the software, the hardware and the communications networks that provide the access, storage and carriage of sensitive information. Without doubt, this is vitally important. After all, it is within the systems of information management that cyber vulnerabilities exist, and it is through understanding the capabilities of adversaries and vulnerabilities of systems that security can be strengthened.

But the thorough analysis of security threats requires more than just 'capability'. We also need to assess 'intent'. And more often than not, the intent that motivates a cyberattack is access to *data*. It's the data that needs to be protected from exfiltration, manipulation or destruction, because it's the data that holds information critical to Australia's agency and success as a sovereign nation. To date, however, there has been very little serious analysis of Australia's critical data assets or the national policy settings required for the proper recognition and management of this important national resource.

This ASPI report fills that gap, and comes at a crucial time as all Australian Government agencies continue on the path of digital transformation. Anne Lyons has reminded us all that our national identity assets form the heart of who we are as a nation, and her recommendations provide a sharply focused action plan for a whole-of-government policy framework that looks beyond the temporary, technology-driven threats and vulnerabilities affecting the current generation of government ICT and addresses instead the very foundation of Australia's digital future—the precious data that defines us.

David Fricker
Director-General National Archives of Australia,
President International Council on Archives

Impact

Throughout history, warfare has damaged and destroyed assets vital to nations' cultural heritage and national identity. While physical damage is often clear and immediate, cyberattacks targeting a nation's identity—its way of life, history, culture and memory— wouldn't have the same physical visibility, but have the potential to cause more enduring and potentially irreparable harm.

In our increasingly digital world, it isn't difficult to imagine the types of cyberattacks we'll be likely to face and the degree of impact on irreplaceable national identity assets.

Consider the following:

- The discovery that digital reference legal documents had been altered could bring the court system to a halt while the integrity of the entire system is reviewed.
- The deletion, encryption or corruption of information relating to landholdings or births, deaths and marriages would cause widespread societal disruption, stopping everything from property sales to weddings.
- A synchronised attack on half a dozen key historical archives—such as our entire newspaper archives, historical photo databases, war records and Indigenous archives—would cause an irreplaceable loss that would be likely to cause public outrage and a great collective sense of loss.
- Because we haven't anticipated sophisticated attacks against the organisations holding these assets and because they're generally undervalued, the protections in place are inadequate. And it isn't just nation-states, but cybercriminals and hacktivists who may cause serious damage.

This isn't just an Australian problem. Institutions and governments internationally face the same issue as truth becomes a victim of information warfare, fabricated news, and increasing and evolving cyberattacks.

Our national identity assets are the evidence of who we are as a nation—our resources, our people, our culture, our way of life, our land, our freedom, our democracy. What if we had no evidence of who we are, what we own, who governs us, where we have come from?

What's the problem?

Like other countries, Australia is focused on protecting its critical infrastructure from cyber threats; however, there's a serious gap in how we approach the protection of our valuable digital national identity assets.

A cyberattack targeting national identity assets has the potential to cause major disruption and collective psychological damage. Such an attack would almost certainly lead to the further erosion of public trust in Australia's democratic institutions and our reputation internationally.

Our vitally important national identity assets aren't adequately protected, and a long-term plan to protect them is lacking. The damage that their loss would cause makes them a tempting target for the next wave of cyber-enabled political and foreign interference.[1]

What's the solution?

Gaps in our protection of national infrastructure and information security need to be addressed. Australian governments—state and federal—need to begin a systematic effort to identify and value national identity data. A closer alignment between the professional fields of digital preservation and information security is required, and a stronger focus on information governance.

Australian governments need to ensure that our critical government-held national identity assets are protected and that memory institutions charged with their care are adequately funded to do so.

Until these issues are addressed, this increasingly 'invisible' vulnerability means that the potential loss of the digital evidence of who we are as a nation remains a sleeping, but urgent, national security priority.

Introduction

Imagine this. You wake up in 2022 to discover that the Australian financial system's in crisis. Digital land titles have been altered, and it's impossible for people and companies to prove ownership of their assets. The stock market moves into freefall as confidence in the financial sector evaporates when the essential underpinning of Australia's multitrillion-dollar housing market—ownership—is thrown into question. There's a rush to try to prove ownership, but nowhere to turn. Banks cease all property lending and business lending that has property as collateral. The real estate market, insurance market and ancillary industries come to a halt. The economy begins to lurch.

At the same time, a judge's clerk notices an error in an online reference version of an Act. It quickly emerges that a foreign actor has cleverly tampered with the text, but it's unclear what other parts of the Act have changed or whether other laws have been altered. The whole court system is shut down as the entire legal code is checked against hardcopy and other records and digital forensics continue.

Meanwhile, a ransomware attack has locked up the digital archives of Australia's major media organisations and parallel archival institutions. Over 200 years of stories about the nation are suddenly inaccessible and potentially lost.

As the Australian public and media are demanding answers, the government is struggling to deal with the crisis. Hard paper copies of many key documents simply don't exist.

National identity assets are the evidence of who we are as a nation—from our electronic land titles and biometric immigration data, to the outcomes of our courts and electoral processes and the digital images, stories and national conversations we're having right now.

Increasingly, our national footprint and interactions are digital only, including both digitally born and digitalised material, all of which is increasingly being relied on as a primary source of truth—the legal and historical evidence we rely on now and into the future.

As companies, governments and individuals scramble to protect important data and critical systems such as telecommunications and power supplies from cyber threats, we overlook datasets that are perhaps even more valuable.

They're a prime and obvious target for adversaries looking to destabilise and corrode public trust in Australia.

With 47,000 cyber incidents occurring in Australia each year[2] and a permissive global environment for cyber adversaries, information manipulation and grey-zone cyber conflict aimed at disrupting nations and in particular Western democracies, the threat to our national identity assets is real. Both state and non-state adversaries have the capabilities to disrupt, distort and expropriate national identity data. What's been lacking to date is the intent to use them this way, and intent can change fast.

Keeping national identity assets safe and accessible is vital not only for chronicling Australia's past, but for supporting government transparency, accountability, the rights and entitlements of all Australians and our engagement with the rest of the world.

This report explores the value of Australia's digital national identity assets and the consequences of not protecting them. The need to protect them from theft, manipulation, destruction or unlawful action may seem a given, but this review has found that our vitally important sovereign national identity data and information isn't being adequately protected and lacks a long-term protection or preservation strategy.

Report methodology

Many national data assets are held in government digital holdings, and those assets are the main focus of this report.

More than 20 organisations across government, academia and the corporate sector were consulted and surveyed as a part of this research. In addition, 70 experts on critical infrastructure, information security, cybersecurity, digital preservation, risk management, information governance, archives and data management were interviewed. Roundtable discussions were held to explore national identity data as critical infrastructure and the international experience, as well as two workshops exploring possible scenarios and consequences.

National identity

Defining national identity

Australia's national identity is difficult to define. It's a complex, ever-changing, dynamic collective of Australians and our environment, history, geography, culture and outlook.

For some, it's the feeling shared with a group of people about a nation, expressed through patriotism, national pride and a positive emotion of love for one's country.[3] It's a construct of common points—national symbols, language, images, history, culture, music, cuisine, radio, television, landforms—and it's expanding. It's the collective experience of who we are as a nation, and, while it crosses public, private and personal information, this report primarily focuses on national identity assets in government digital holdings as a key ingredient in identity and in the functioning of our nation.

Digital national identity assets are the evidence of our national identity

National identity assets are the evidence of who we are, how we see ourselves and how we relate to the rest of the world. They include high-value personal, social, legal, democratic and historical data, such as records of births, deaths and marriages; immigration records; land titles; the decisions of our courts and parliaments; and the many stories told on our screens and airwaves through social and electronic media.

Digital assets include data, digital information, multimedia, imagery and sound. They're both digitally born (created digitally) and digitalised (analogue material digitised and available electronically). It's our digital heritage, being created now, that defines our unique Australian identity and is essential for the functioning of our democracy, our society, our culture and our legal system.[4]

This report doesn't set out to define or describe all of Australia's national identity data and digital information, but it does recommend developing a way of identifying and valuing those assets to enable appropriate protection.

Some examples of digital national identity assets include:

- Digitally born identity assets
  - Hansard (Department of Parliamentary Services, Parliamentary Library)
  - Indigenous War Service Project (Australian National University, Australian Institute of Aboriginal and Torres Strait Islander Studies)
  - evidence and findings from royal commissions (National Archives of Australia)
  - Australian Web Archive (National Library of Australia)
  - ABC Digital Library
  - Lindt Café siege social media collection (State Library of NSW)
  - passport biometrics and passenger arrivals (Department of Foreign Affairs and Trade, Department of Home Affairs, Border Force).
- Digitalised assets
  - convict records (NSW and Tasmanian archives)
  - Australian Institute of Aboriginal and Torres Strait Islander Studies photographic collection
  - newspaper collections (National Library of Australia and state libraries)
  - World War I records (National Archives, Australian War Memorial, NSW State Library)
- Hybrid analogue/digital assets
  - Fairfax photographic collection (Fairfax Media)
  - High Court decisions (High Court of Australia)
  - births, deaths and marriages records (state and territory government agencies and archives)
  - parliamentary papers and decisions (federal, state and territory parliamentary departments
  - immigration records (Department of Home Affairs, National Archives of Australia)
  - property ownership records (state and territory government agencies and archives)

Failure to protect national identity assets

Yesterday, the Australian Electoral Commission, the Department of Home Affairs and the NSW Lands Department discovered discrepancies in their election results databases, the public electoral roll, electronic land title registrations and citizenship data. Investigations haven't identified when the problems occurred. The discrepancies make it difficult to rely on the validity of their data holdings.

At the same time, the Department of Parliamentary Services received an anonymous report that over the past 12 months changes have been made to Hansard report proofs online. They have five days to remedy the issue before the source goes public, while public complaints, mainly through social media, have already started about digital images and material previously on the website that's no longer available, particularly Hansard reports of new parliamentarians' maiden speeches in the Senate and House of Representatives.

A few days ago, the daughter of a World War II veteran was interviewed on ABC Radio's morning program in the Northern Territory. She had written to the Attorney-General complaining that her father's war service record is no longer available. An investigation by the National Archives of Australia found that all the digitised service records for World War II on its website have been removed from the database holding and displaying them, and been replaced with images of Donald Trump, Xi Jinping, Angela Merkel and other world leaders.

Today, a major story was leaked to The Australian newspaper that implicated Australian companies involved in the 2006 royal commission into the Iraq oil-for-food program. The leaked documents were released to the public by Wikileaks. Those records are held by the National Archives. Wikileaks also announces that it will shortly be following up the leak with a release of the 2016 Census, which is supposed to be held by the National Archives and not released until 2115.

This is a fictional scenario created by the author.

Issues

A sleeping giant

The increasing vulnerability, invisibility and online exposure of our digital identity is an underappreciated national security issue.

In a global environment of increasing cyberattacks, capable state and non-state actors, information espionage and grey-zone cyber conflict aimed at disrupting nations, the threat to our national identity assets is real.

States such as Russia have demonstrated their intention to disrupt and undermine Western democracies,[5] and obvious future targets for such attacks are national identity assets that are poorly protected and offer high-impact results if disrupted, corrupted or destroyed. With more than 30 countries known to possess offensive cyber capabilities,[6] and cyber capabilities being in reach of non-state actors from individuals to cybercrime organisations, the number of potential adversaries able to target our national identity assets is significant and increasing.

> We've bought into the fiction that all of the information we could possibly want to access is there, all of the time—and for all time. But the truth is that the access of future generations to our recent history is more precarious than ever.
>
> —Kylie Walker, Chair, Australian National Commission for UNESCO

Because we're a liberal democracy, Australian society relies at its deepest level on the trust of the citizen in the state.[7]

National and state government archives play the role of 'impartial witnesses', identifying and holding this information and holding the government to account under the rule of law and in the 'court' of history. Many other institutions have additional holdings that collectively form our national identity assets. We need to trust that these impartial witnesses can identify, keep and preserve this evidence. This is a matter of national security and is at the heart of our society.

Previously, victors rewrote history. Now, in the digital age, our adversaries could rewrite our present. If we aren't vigilant, we run the risk that adversaries could destroy or manipulate our national identity assets, compromising the digital pillars of our society and culture.

If our land titles or our citizenship records were altered, what would be the result? If we lost our immigration and births, deaths and marriages data, how could you prove your citizenship? And what if that information were compromised and unreliable? What would be the authoritative source of information about Australians and their citizenship?

Public trust and perceptions

> If you can't trust the truth holders, then who can you trust?
>
> —Rachel Botsman[8]

The biggest impact from an attack on national identity assets would be the resulting corrosion of trust in public institutions. As Russian interference in other countries' elections has demonstrated, the erosion of trust is more corrosive to democracy than the win or loss of any particular candidate.

Attacks on truth and trust affect individuals and nations and, while just one breach can erode trust, a concerted campaign can do much more. As US academic and commentator Zeynep Tufekci so accurately describes, 'we are in an era where misinformation thrives and even true information can confuse and paralyse rather than inform and illuminate.'[9]

When more than 600 fake Facebook accounts were uncovered, linked to Russian and Iranian influence campaigns, a false and disingenuous dialogue and history were created.[10] We've already seen the manipulation of video become a reality,[11] and, as Peter Singer describes in his latest book, Like war, propaganda has been weaponised en masse and is now threatening democracies.[12]

Fraud and fakery aren't new—they're just happening in a new hi-tech domain, with the potential to do much greater damage at scale. It's inevitable that they'll expand into historical data and information. For example, in 2008 a British historian added 29 fake documents over five years to write a fake history of members of the British royal family collaborating with the Nazis during World War II.[13]

Closer to home, between 2007 and 2015 the Western Australian Registrar of Births, Deaths and Marriages removed vital information about Aboriginality and illegitimacy from birth certificates because the registrar deemed it too distressing for people.[14] While not fraud, or an external attack, it was an intentional changing of evidence that could have major repercussions personally, socially and historically.

Cybercriminals have already taken individuals' and organisations' data 'hostage' by encrypting it and demanding ransom to decrypt it. The good news is that this has yet to happen to national identity holdings.

As the physical world meets the digital world, protecting and securing authentic data has become an ongoing challenge. So, who will hold the source of truth, and how will people know whether they can trust the source?

Vulnerability and invisibility

Recent studies by the University of NSW and University of Canberra identified examples of Russian targeting of Australian voters in 2017.[15] Our universities, businesses and governments are under a constant attack in which 400 Australian companies were targeted in 2017.[16] Countries such as Israel,[17] Iran,[18] North Korea, China[19] and the US[20] are also known to have publicly used malicious cyber actions against other nations, including Australia.[21]

A future frontier for these attacks is likely to be national identity assets, but despite this there's a lack of engagement and awareness in government and the community about the safety and security of those assets and the government institutions that hold them, and a lack of care about data and information security more generally.[22]

Our critical infrastructure, defence, border security, privacy, personal information and economic assets attract the headlines, the attention and ultimately the dollars.

There's no strong narrative about the need to protect holdings of digital national identity assets nationally or internationally. Many memory institutions find it difficult to be heard and secure funding, except when the need involves Australia's military history, or when a tragedy occurs, such as this year's devastating fire at Brazil's National Museum.[23]

The ravages of time

Digital assets aren't as resilient as most analogue or paper forms and decay over time, including through degradation, obsolescence or the breakdown of computerised information. All digital material is prone to some sort of decay (sometimes known as 'data rot').[24] This doesn't take long, particularly with the current speed of technological change and growth in the quantity of data.

All organisations need to be aware of potential decay that can make their information and data unusable.

Resourcing and capability of institutions

Australia's ultimate information and data custodians— the memory institutions, such as national and state archives, records organisations, libraries and other cultural institutions—struggle to keep even their basic services afloat, let alone to protect and preserve digital heritage and national identity data.

The current parliamentary review of national institutions in Canberra is evidence of that.[25] The committee has received numerous submissions and testimonials from the heads of cultural institutions decrying the consequences of continued funding cuts.[26] Although a handful of agencies have recently received one-off funding for digital initiatives, the National Archives of Australia, which holds some of the government's most valuable and sensitive information, unsuccessfully sought funding to build a secure digital archive five times over the past 10 years. Recently, it received an adverse finding in the Australian National Audit Office's latest cyber resilience audit for not meeting all essential information security requirements.[27]

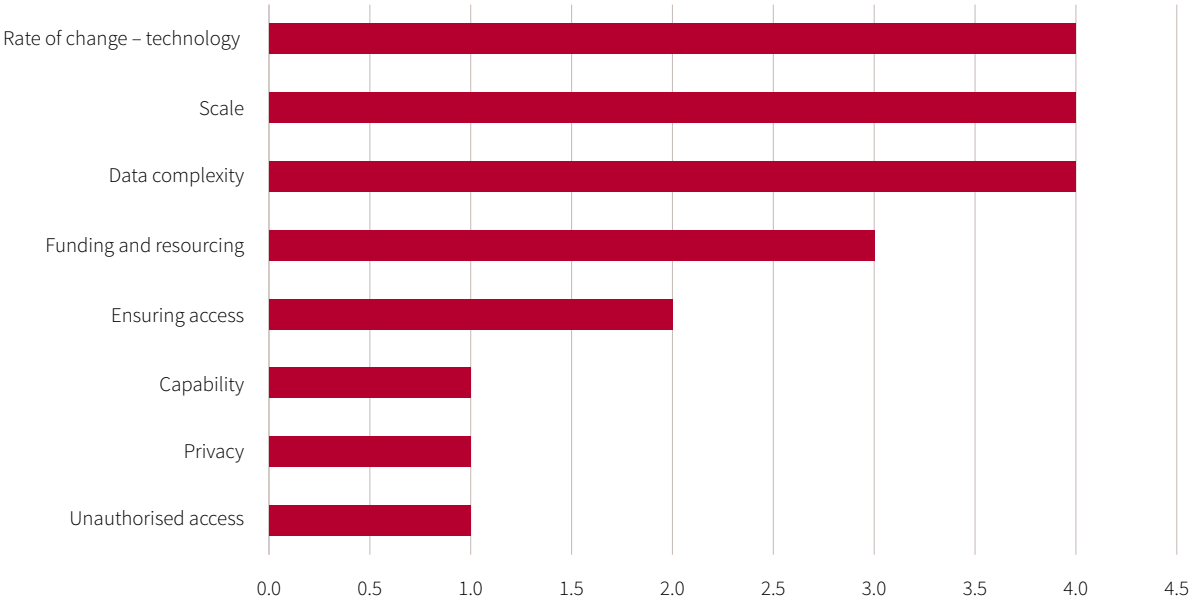
Fair funding

A great deal of effort, funding and focus is placed on protecting critical infrastructure such as roads, communications and ports, as well as classified and sensitive information, but the same can't be said of our national identity data, or of the national and state institutions that protect and provide access to those digital assets.

Digitalisation of information is only going to increase; most Australian governments are committed to being fully digital within the next few years. As custodians of the bulk of national identity data, government agencies have a responsibility to protect it from birth over its life. And, with the creation and retention of fewer paper traces, accessing and preserving this information is becoming more complicated.

Of the 20 government agencies and universities surveyed as part of this project, the rate of change, scale, complexity and resourcing were identified as the biggest problems facing them in their quest to protect our digital information and assets (Figure 1).

Figure 1: Some survey results



A crowded ungoverned space

The plethora of information, data, cyber and security protocols, strategies, policies, frameworks, legislation and agencies involved at the federal and state levels in Australia is confusing and inconsistent. At least 20 organisations are involved in information and data policy, protection and management in the Australian Government space alone.

In 2015, when it released its Digital Continuity 2020 policy,[28] the National Archives of Australia had already recognised the urgent need for information governance, and this was reiterated in the Open Data Initiative as part of Australia's first Open Government Partnership National Action Plan in 2016.[29]

The Digital Continuity 2020 policy required agencies to have information governance frameworks and information governance committees in place by June 2016. By September 2017, only 64% of Australian Government agencies had achieved the latter.[30]

This policy needs to be extended to include governance and coordination at the whole-of-government level to ensure the robust and reliable management of national identity data.

The way forward

Include national identity assets within the critical infrastructure framework

> Government archive material, must be considered as equivalent to any critical national infrastructure, given its value to national identity, values, history.
>
> —David Irvine, Chair, Foreign Investment Review Board

Critical infrastructure is firmly in the sights of those conducting cyberwarfare and industrial sabotage.[31] Cyberweapons can turn off power grids, derail trains, cause offshore oil rigs to list, turn petrochemical plants into bombs and shut down factories.[32]

Attacks are increasingly common and becoming more sophisticated. Ukraine's energy sector was the target of a Russian cyberattack in 2015 that caused power outages that affected more than 200,000 citizens,[33] and in 2017 there was an alleged Russian state hack of US electricity companies.[34] Both Iran and Russia have been linked to an attack on a petrochemical plant in Saudi Arabia in 2017 that was described as a new kind of cyber assault designed to trigger an explosion.[35]

Like other countries, Australia is focused on protecting its critical infrastructure. However, there's a serious gap in our approach, which currently doesn't include the protection of national identity assets.

Digital national identity assets underpin our democracy

Australia's Critical Infrastructure Centre describes critical infrastructure as underpinning the functioning of Australia's society and economy and integral to the prosperity of the nation.[36] National identity assets do all that and more—they also underpin our democracy—and should be considered as part of the nation's critical infrastructure.

Attacks on governments show that we must recognise the threat posed by cyberattacks not only to critical infrastructure services, but also to democratic functioning and government continuity.[37]

Data and information don't fit within the traditional conception of critical infrastructure. In Australia, 'critical infrastructure' is taken to mean the supply chains, information technologies and communication networks, the destruction, degradation or lengthy unavailability of which would significantly damage the social or economic wellbeing of the nation or affect our ability to conduct national defence and ensure national security.[38]

Australia has eight critical infrastructure sectors: banking and finance; the Australian Government; communications; energy; food and groceries; health; transport; and water.

There's an argument that, if national identity assets were included, the existence of digital and analogue information would require differing control measures and consequential tighter controls, making it harder to access, or measures to replicate data holdings so that disruption and manipulation can be dealt with by turning to authoritative alternative holdings. Also, if whole systems—hardware, software, personnel, data and information—are considered critical, that could lessen the meaning and idea of 'critical'.[39]

While defining the strict parameters of national identity assets might be problematic, that can be broadly overcome by focusing instead on the organisations that create, keep and preserve them. The intrinsic value of Australian Government national identity assets, such as those held by the National Archives and National Library, should be recognised as part of the Australian Government critical infrastructure sector. Consideration should also be given to how similar assets of state governments should be protected.

Estonia, a country recognised for e-government, has acknowledged the vulnerability of its data and information and is replicating its critical government data in Luxembourg in what's been called a 'virtual embassy' to protect it and ensure that government and services will be uninterrupted in the case of an attack on Estonia.[40]

The closest Australia has come to officially considering data and digital information as critical infrastructure was the 2017 public consultation on the Security of Critical Infrastructure Bill, which asked whether data centre assets should be included.[41] They weren't.

Increased focus on data security

Despite this, during 2018 there's been an increased focus on data security and engagement by the Australian Critical Infrastructure Centre, which is working with the Australian Cyber Security Centre and the Digital Transformation Agency on whole-of-government infrastructure.[42] But this isn't just about systems, security and services. We need to go one step further and consider the data held within them.

The Australian Productivity Commission's 2017 Data availability and use report noted that data is an asset, and that there are plenty of datasets and collections the degradation or unavailability of which 'would significantly impact the social or economic wellbeing' of Australia.[43]

Australia's electoral roll and Census data are two such cases. The latter not only guides the allocation of much government funding, but also helps to determine electoral boundaries—a key component of our democratic process. As noted by the Productivity Commission, if it were to be compromised that would jeopardise public trust.

There's valid evidence of a pressing need to review what critical national identity assets are and to include national identity and high-value data within Australia's critical infrastructure framework.[44] We also need to investigate a legislative response to how they should be managed and evaluated nationally, supported by the Australian Trusted Information Sharing Network and focusing on those assets in the critical infrastructure sectors and the states and territories.

We protect what we value

If Australia were a person, and her digital house was on fire, what would she grab and load in her car to save? What would be ready and in a convenient location, so that she could pick it up and run?

Sometimes it takes a disaster before a new or upgraded system is funded.

There's a disconnect between how we value and how we protect our data and digital information. Currently, more focus and value are placed on the security of classified, national security and personally identifiable information. As a result, the systems that hold and manage that information are prioritised.

The volume of digital information and data is increasing at a rapid rate, and the percentage that needs to be kept for business, legal, evidentiary and archival purposes is also growing.[45]

Valuing digital identity assets

There's also no standard, guidance or formula for valuing digital information and data, or any requirement to report data assets in financial reports. In the case of digital national identity assets, there's no long-term view on their value or their protection, although many memory institutions do include them in financial reporting.

While there's an accounting standard for valuing cultural and scientific collections, that's primarily for physical collections. Valuing digital assets is proving more difficult. The valuation industry has developed varied approaches and methodologies and, depending on the volume and complexity, such valuations can come at a significant cost.

What's being done

The NSW Government is currently valuing its digital collections, and the Australian Bureau of Statistics is valuing its Census data. In 2014, the New Zealand Bureau of Statistics valued its 2013 census data at $1 billion,[46] and in 2016 the Australian Bureau of Communications Research estimated that Australia's open data was worth $25 billion per year, or 1.5% of Australia's GDP.[47]

We need to do more about standardising the way we value our national identity assets.

The inability to access, understand and adequately discriminate between what's valuable and what isn't is a key challenge, as is maintaining appropriately skilled people to ensure quality, accuracy and analytics, including privacy and ethics considerations.

In 2016, American historian Abby Rumsey argued that we're now so far ahead of ourselves in the accumulation of data that we may never catch up or truly understand its significance.[48] And data is only valuable if it can be explored and we can get insights and information from it.[49] We may have a future in which a generation of history is lost because it doesn't exist or is inaccessible.

A simple way to identify, assess and value national identity data and information needs to be developed, along with a consequence framework to assess the impact should it or its provenance be lost or damaged.

Security, preservation and governance

> We have to value our government data holdings as a national asset and within government we have to adjust our behaviours and our policies accordingly.[50]
>
> —David Fricker, Director-General, National Archives of Australia, President International Council on Archives

Protection of national identity assets is far more than information and cybersecurity.

Internationally, there's a large 'infosec' industry, which continues to grow. Governments and a swag of organisations and agencies are dealing in cybersecurity, information security, big data, privacy and information policy.

The glaring omissions are digital preservation and governance—not just for digital national identity assets, but for all business-critical information and data. This includes assets relied upon by the public and business for planning, redundancy and technology that can read the data in 10 or 100 years from now.

This crowded landscape calls for a strategic and coordinated approach and stronger focus to address a major vulnerability that all organisations face—the integrity, reliability, authenticity and accessibility of digital assets now and into future, whether it's three years, thirty-three or forever, as with national identity assets.

Earlier adoption of digital asset preservation

Digital preservation isn't widely understood or practised except by organisations with dedicated preservation functions. Even then, digital preservation usually involves work streams and professions separate from information security functions.

Digital preservation is essential for digital authenticity, reliability and access over time, and is far more than just creating a backup. It ensures the accurate rendering of authentic content over time, including protection from medium failures and software and hardware obsolescence.[51]

The 2017 edition of Australian Government's Information security manual includes no digital preservation requirements, other than backup for business continuity and disaster recovery.[52] The 2018 manual will expand backup requirements to ensure that information can't be manipulated or changed, and the author understands that, based on the recommendations of this report, digital preservation is being considered for inclusion from 2018 onwards to guide those Australian Government agencies with national identity and high-value assets.

Increasingly, blockchain technology is being used by industry and government to assure transactions and services, the most recent such use being the pilot rollout of NSW digital drivers' licences.[53] This should continue to be explored to ensure the integrity of national identity assets.

We need to start the conversation about digital preservation earlier, at the beginning and not at the end of digital asset creation. Along with information management, digital preservation must be considered by all organisations before they build or upgrade systems that create, use and keep

valuable information and data for any length of time. This is for governance, discovery and access, and to ensure that the evidence remains authentic, can be migrated to and managed by memory institutions into the future, and be accessed and read whenever it's needed.[54]

Information security reporting and audits

Currently the 'confidentiality, integrity and availability' security model is heavily weighted towards confidentiality. This imbalance is a vulnerability, and, despite improvements in cybersecurity,[55] many organisations aren't meeting this base-level security requirement. A recent audit by the Australian National Audit Office (ANAO) found that, out of three Australian government agencies, only one was cyber resilient.[56]

While the Australian Cyber Security Centre (ACSC) surveys the status of information security in the public and private sectors,[57] it's difficult to assess just how safe Australian organisations are and what they're doing to ensure that their systems and data are safe. Further work is needed in this space to audit data authenticity and to check for evidence of manipulation or change. This would require new methodology and practices—possibly drawing on digital preservation skills and approaches—that should eventually become business as usual.

There's no independent or public reporting of the state of cybersecurity within individual organisations, or a 'state of the nation' report on how agencies and businesses are managing and protecting data.

Public self-reporting is needed, and more transparency is one of several recommendations made by the ANAO in its 2018 cyber resilience audit.[58] A snapshot or dashboard showing how Australian organisations are performing in cybersecurity should also be developed as part of the ACSC's annual survey.

Lack of coordination and information governance

Immediate business needs tend to overshadow the way information is governed and managed.

Many government and private-sector organisations are easy prey to cyberattack, not just because of weak cybersecurity, but because of the absence of a comprehensive whole-of-organisation view on how all information and data assets are to be managed and protected.

There's an urgent need to implement better information governance across the public and private sectors in order to protect Australia's digital national identity assets.

Policy recommendations

1. Australia's national identity and high-value data and information, the destruction or corruption of which would have a serious impact on our sovereignty, should be recognised as part of our critical infrastructure framework.
2. The Trusted Information Sharing Network should examine existing coverage of vulnerabilities and establish a dedicated forum on that data and information.
3. The Australian Government should explore a legislative response to managing and evaluating that data on a coherent national basis.
4. National security agencies should engage with the National Archives of Australia to undertake a risk assessment of the archives' digital national identity assets and jointly develop proposals to defend them from future attack.
5. The National Archives of Australia should use its legislated powers to prescribe what government information and data constitutes national identity assets and set mandatory management and governance standards to ensure, protect and maintain their long-term integrity and reliability of those assets.
6. The Australian Productivity Commission should explore the value of digital national identity assets to Australia, defining the parameters to be considered in identifying and valuing them and the cost should they be destroyed or manipulated, or should trust in their authenticity and reliability be eroded.
7. The Australian Government, through the Department of Finance, should investigate and provide guidance and standards for agencies to assess the value of their information and data assets.
8. The Australian Government, through the Department of Finance, should develop a tool to assist organisations to assess the value of their data and digital information, to assist in developing strong business cases for protection.
9. A new funding model for memory institutions should be explored by Australian governments to help protect digital national identity material.
10. Digital preservation principles should be built into information security requirements, such as those in the Australian Government's *Information security manual*.
11. The Digital Transformation Agency, in conjunction with CSIRO's Data 61, should explore the use of blockchain technology to track, record and ensure the provenance of national identity and high-value data.
12. The ACSC should produce a 'state of the nation' report on cybersecurity health and readiness.
13. All public, private and community sector organisations holding national identity assets should be encouraged to publicly report their annual cyber resilience status.
14. The ANAO, in conjunction with the ACSC, should explore the creation of an authenticity audit, so that internal and external auditors can assess digital assets on a scheduled, regular basis, employing a standardised methodology.
15. All Australian governments (federal and state) should better coordinate their information, data and related cyber policy agencies and strengthen information governance as the overarching requirement, incorporating all elements of information management, security, privacy and data management.

Notes

1 Kelsey Munro, 'Foreign interference in elections "will be repeated": former US cyber tsar', SBS News, 22 February 2018, online; 'Five Country Ministerial 2018', Department of Home Affairs, 29 August 2018 online.

2 Dan Tehan, 'Silent dangers: launch of the Australian Cyber Security Centre's *2017 threat report*', National Press Club address, 10 October 2017, online.

3 JC Turner, 'Some current issues in research on social identity and self-categorization theories', in N Ellemers, R Spears, B Dossje (eds.), *Social identity: context, commitment, content* (6–34), Blackwell, Oxford, UK, 1999.

4 Eliza Chapman, 'Should data be considered critical infrastructure?', *The Strategist*, 18 April 2018, online.

5 Jeremy Herb, Lauren Fox, Manu Raju, 'Senate committee agrees with intelligence community assessment of election meddling, breaking with GOP House investigation', *CNN*, 16 May 2018, online; Culture, Media and Sport Select Committee, *Russian influence in political campaigns*, UK Parliament, 29 July 2018, online.

6 Steve Ranger, 'US intelligence: 30 countries building cyber attack capabilities', *ZDNet*, 5 January 2017, online; James R Clapper, Marcel Lettre, Michael S Rogers, 'Joint statement for the record to the Senate Armed Services Committee: foreign cyber threats to the United States', 5 January 2017, online.

7 Tim Gollins, 'The national archives, big data and security: why dusty documents really matter', in Jennifer Cole (ed.), *Big data for security and resilience: challenges and opportunities for the next generation of policy-makers*, proceedings of the Big Data for Security and Resilience Conference, March 2014, online.

8 Rachel Botsman, *Who can you trust? How technology brought us together and why it might drive us apart*, Penguin, 2017.

9 Zeynep Tufekci, 'How social media took us from Tahrir Square to Donald Trump', *MIT Technology Review*, 14 August 2018, online.

10 Sheera Frenkel, Nicholas Fandos, 'Facebook identifies new influence operations spanning globe', *New York Times*, 21 August 2018, online; Ben Nimmo, Graham Brookie, '#TrollTracker: Facebook uncovers active influence operation', *@DFRLab*, 31 July 2018, online.

11 Tim Leslie, Nathan Hoad, Ben Spraggon, 'Can you tell a fake video from a real one?', *ABC News*, 3 October 2018, online.

12 PW Singer, Emerson T Brooking, *Like war: the weaponization of social media*, Houghton Mifflin Harcourt, New York, 2018.

13 Paul Lewis, 'The 29 fakes behind a rewriting of history', *The Guardian*, 5 May 2008, online.

14 Rebecca Turner, '"Aboriginal" redacted from birth, death, marriage certificates after being deemed an offensive term', *ABC News*, 17 May 2018, online.

15 Tom Sear, Michael Jensen, 'Russian trolls targeted Australian voters on Twitter via #auspol and #MH17', *The Conversation*, 22 August 2018, online.

16 Stephanie Borys, 'Russian hacking: up to 400 Australian companies caught up in cyber attacks blamed on Moscow', *ABC News*, 17 April 2018, online.

17 Ellen Nakashima, Joby Warrick, 'Stuxnet was work of US and Israeli experts, officials say', *Washington Post*, 2 June 2012, online.

18 Patrick Howell O'Neill, 'Cobalt Dickens threat group looks to be similar to indicted hackers', *Cyberscoop*, 24 August 2018, online.

19 Jonathan Landay, 'US intel chief warns of devastating cyber threat to US infrastructure', *Reuters*, 14 July 2018, online.

20 Nakashima & Warrick, 'Stuxnet was work of US and Israeli experts, officials say'.

21 Nick McKenzie, Angus Grigg, Chris Uhlmann, 'China uses the cloud to step up spying on Australian business', *Sydney Morning Herald*, 20 November 2018, online.

22 David Donaldson, 'Password123: public servants risk cyber attacks with weak security', *The Mandarin*, 22 August 2018, online.

23 John McCormack, 'Think the museum fire in Brazil can't happen here? Think again', *Los Angeles Times*, 9 September 2018, online.

24 Angela Stringfellow, 'Digital decay: understanding digital decay, its impacts on modern business, and best practices for preserving digital assets and data', *MerlinOne*, 5 March 2018, online.

25 Joint Standing Committee on the National Capital and External Territories, 'Inquiry into Canberra's national institutions', Australian Parliament, no date, online.

26 Sally Whyte, 'More cuts will put national institutions' "core purposes" at risk', *Canberra Times*, 13 May 2018, online.

27 Australian National Audit Office (ANAO), *Cyber resilience*, report no. 53 of 2018–18, ANAO, Canberra, online.

28 National Archives of Australia (NAA), *Digital Continuity 2020 policy*, NAA, Canberra, 5 April 2018, online.

29 Department of the Prime Minister and Cabinet, *Open Government Partnership Australia*, '3.3—Improve the discoverability and accessibility of government data and information', online.

30 NAA, '2017 digital continuity statement: whole-of-government snapshot', NAA, Canberra, 2017, online.

31 Stephen Cobb, 'Trends 2018: critical infrastructure attacks on the rise', *WeLiveSecurity*, 30 May 2018, online.

32 Tim Johnson, '"Preparing the battlefield": Hackers implant digital grenades in industrial networks', *McClatchy*, 27 June 2018, online.

33 Donghui Park, Julia Summers, Michael Walstrom, 'Cyberattack on critical infrastructure: Russia and the Ukrainian power grid attacks', Henry M Jackson School of International Studies, 11 October 2017, online.

34 Kanishka Singh, 'Russian hackers penetrated networks of US electric utilities: WSJ', *Reuters*, 24 July 2018, online; US Computer Emergency Readiness Team, 'Alert (TA18-074A): Russian Government cyber activity targeting energy and other critical infrastructure sectors', 15 March 2018, online.

35 Nicole Perlroth, Clifford Krauss, 'Cyberattack in Saudi Arabia had a deadly goal. Experts fear another try', *New York Times*, 15 March 2018, online; David E Sanger, 'Hack of Saudi petrochemical plant was coordinated from Russian institute', *New York Times*, 23 October 2018, online.

36 'What is the Critical Infrastructure Centre', Department of Home Affairs, no date, online.

37 Dante Disparte, 'Cities held for ransom: lessons from Atlanta's cyber extortion', *Forbes*, 2 April 2018, online.

38 Trusted Information Sharing Network, 'Critical infrastructure', no date, online.

39 Chapman, 'Should data be considered critical infrastructure?'.

40 Daniel Cooper, 'Estonia will back up its government in a "digital embassy"', *engadget*, 22 June 2017, online.

41 Security of Critical Infrastructure Bill 2017, Australian Parliament, online.

42 Asha McLean, 'Canberra to deliver platform and hosting strategies by November', *ZDNet*, 7 May 2018, online.

43 Productivity Commission, *Data availability and use*, 'Overview and recommendations', report no. 82, 31 March 2017, online.

44 Chapman, 'Should data be considered critical infrastructure?'.

45 IDC, *The digital universe of opportunities: rich data and the increasing value of the internet of things*, 'Executive summary: Data growth, business opportunities, and the IT imperatives', April 2014, online.

46 Statistics New Zealand, *Valuing the Census*, New Zealand Government, April 2013, online.

47 Bureau of Communications and Research, 'Open government and why it matters', Department of Communications and the Arts, Australian Government, 8 February 2016, online.

48 Abby Smith Rumsey, *When we are no more: how digital memory is shaping our future*, Bloomsbury Press, 2015.

49 Susan Bennett, *What is information governance and how does it differ from data governance?*, Sibenco Legal and Advisory, 2017, online.

50 David Fricker, 'Government–citizen engagement in the digital age', Senate Occasional Lecture, NAA, 28 April 2017, online.

51 Digital Preservation Coalition, *Digital preservation handbook*, 'Glossary', no date, online.

52 Department of Defence, *Australian Government information security manual: controls*, Australian Government, 2017, online.

53 Rohan Pearce, 'NSW digital licence rollout driven by blockchain', *Computerworld*, 10 September 2018, online.

54 NAA, *Digital Continuity 2020 Policy.*

55 Australian Cyber Security Centre (ACSC), *2017 threat report*, Australian Government, 2017, online.

56 ANAO, *Cyber resilience.*

57 ACSC, 'Publications', online.

58 Stephen Easton, 'Auditor-General still waiting on cyber resilience in the Commonwealth', *The Mandarin*, 25 July 2018, online; ANAO, *Cyber resilience*.

Acronyms and abbreviations

ACSC	Australian Cyber Security Centre
ANAO	Australian National Audit Office
CSIRO	Commonwealth Scientific and Industrial Research Organisation
GDP	gross domestic product

ASPI
AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

NAA
NATIONAL ARCHIVES OF AUSTRALIA