Anne Lyons

Our new cyber frontier

Protecting Australia’s national identity and the evidence of who we are
Overview

- Background
- Where to begin?
- Environment & Objectives
- Activity to date
- Key issues
- Policy areas identified
- Research, consultation
- Report & Recommendations
National Archives Director-General David Fricker asked “why is digital national identity information not considered national infrastructure.”

Start of the conversation and partnership with ASPI with the fellowship to explore that very question
Background
Background

- **ASPI** – 45 staff, 12 visiting and non-resident fellows
- Think Tank 40% funded by Defence
- Defence, Cyber, Risk & Resilience, Law Enforcement
- **ICPC** – eight staff. self-funded by industry, government
- cyber policy research, training and capability development
Background

Twitter – ASPI Cyber Policy @ASPI_ICPC

aspi.org.au/program/international-cyber-policy-centre
Where to begin?

- Methodology & Discovery
- Where do I start?
- What is the problem?
  - Define National identity
  - Examples
  - Born digital v digitised
  - Size of the problem? Is there a problem?
  - Parameters
  - Is anyone else looking at it?
The problem

- Increasing cyber tempo
- Evidence of state attack on western democracies & systems
- Evidence who we are as a nation
- Major impact if damaged or manipulated
- Objective – start conversation & get issue on broader national security agenda.
The problem

- Desk Research
- Just take action
- Discovery discussions
- Issues Paper
- ideas, objectives, parameters, and draft recommendations developed during the Discovery phase
- What's in What's out

NATIONAL IDENTITY
Restoring from back-up...
The Problem

Why is it important?
• Transparency
• Chronicling the past
• Proving who we are

Prime target
• Destabilise & disrupt
• Corrode public trust
• Unclassified and vulnerable
• Concerted campaign could be devastating
• Trust in truth holders
Approach

• 60+ discussions and one-on-one meetings
• Issues Paper
• Three Roundtables
• Three workshops – scenarios, policy areas & Recommendations testing
• Survey
• Articles for The Strategist
• Final report
• Recommendations
Issues

- State attack v criminal v hacktivism
- Born digital or digitised
- National identity data as critical infrastructure
- Value and valuation of digital assets
- What is national identity?
- Cultural heritage destruction during conflict
- Relationship of national identity & personal identity
- Authenticity, integrity & reliability
Issues

- Identifying national identity digital assets
- Protection > digital security & preservation
- How to test vulnerability & impact?
- Cultural assets used for re-building community
- Digital dark age & unknown data loss
- Cost of storage
- Access v lock down
1. National Identity as Critical Infrastructure

- Protecting critical infrastructure
  - From all forms of attack, including cyber
  - Critical Infrastructure Centre (CIC) part of Department of Home Affairs
  - Australian Signals Directorate
- Attack on Government
  - Not just critical infrastructure services
  - Democratic functioning
  - Government continuity
- Defining National identity
  - Difficult
  - Varying opinions on how it should be done
  - Focus on the organisations
  - Include in CI Framework and Trusted information Sharing Network
2. Protection = security & preservation

- Information Security
  - Large infosec industry
  - Perimeter protection
  - Surveillance
- Omissions
  - Digital preservation
  - Information governance
  - Whole of organisation view

Closer alignment between infosec and preservation is required to make data more resilient, not just the hardware and software it lives on.
3. We protect what we value

- **Disconnect**
  - More focus and value on classified and national security data
  - Systems and budgets prioritised
- **Models to value data**
  - Economic & market
  - Intangible historic and cultural value
  - Replacement cost
  - Volume
- **Reporting**
  - Not required in financial reporting
  - Some agencies value digital assets
What next?

Sleeping national security priority

Address critical infrastructure and information security

Better protection & care

Stronger focus on information governance

Identify & value national identity digital assets
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.
What next…..

• In the next week:
  – Ask questions
    • Do we hold national identity data?
    • How do we govern our information and data assets?
    • Do we have an Information Governance Framework?
    • Are we genuinely connecting digital preservation and cyber security? What more could we do?
    • Are there any opportunities to further investigate or research? *(YES!)*

• In the next three months:
  – Challenge and explore how and if your team and organisation
    • **values** data and information, and what opportunities there are to progress this internally, professionally, externally
    • Can connect your national identity holdings and national security
  – Explore what you can do to elevate the issue externally and with other organisations
Want to know more?

Identity of a Nation Report

- https://www.youtube.com/watch?v=fCkK1uZQd3s#action=share

Launch featuring Head of ASPI Peter Jennings, National Archives Director-General David Fricker
Head of the International Cyber Policy Centre
Fergus Hanson & author Anne Lyons

The Strategist
aspistrategist.com


Australian Strategic Policy Institute
aspi.org.au