PUBLIC

Lockstep Consulting
50 Margaret Street, Suite 1301B
Sydney NSW 2000
ABN 17 582 844 015

April 15, 2023

Expert Advisory Board,
2023-2030 Australian Cyber Security Strategy
Department of Home Affairs
Australian Government

By webform

Submission to the Cyber Security Strategy discussion paper

Introduction: Framing today's cyber challenges

Cyber security is understandably dominated by data breaches, criminality, liability and defence-in-depth. Lockstep Consulting, in reviewing the Cyber Security Strategy Paper, takes the opportunity to look at the positives and how to protect the potential of a world-leading data-driven economy.

Lockstep has worked in digital identity and data privacy since 2003, as researchers and advisers, in Australia and internationally. The fields of identity and privacy are converging to provide new approaches to holistic data protection. Over and above defensive security—under the traditional headings of *confidentiality*, *integrity* and *availability*—data protection can address the many aspects that make data valuable and maximise them. In different contexts, different aspects of data matter, be they originality, provenance, jurisdiction of source, algorithmic transparency, age (of the data), permissions to use, or liability provisions.

Given our strategic focus on data protection rather than defensive cyber security, Lockstep does not have much to say about cyber security standards, incident reporting, ransom policies, automated threat-blocking, legislation and so on. We therefore restrict ourselves to Discussion Paper Questions 1, 6 and 16 only.

We are delighted overall by the position paper's call for ideas. Australia needs new thinking to make systemic improvements to cyber resilience. We welcome the new government's appetite for new ideas.

In the main, we would like to address the data protection dimension of what the "most cyber secure nation in the world" would look like in 2030. Lockstep applauds the government's ambitious goal. We suggest that the idea of national data protection *infostructure* might have greater reach and socio-economic potential than any other cybersecurity uplift currently on the agenda and yet it is amongst the more achievable objectives within the 2030 timeframe.

We flesh out what we mean by *infostructure* below and provide concrete suggestions on how to start building national infostructure.

The importance of data

The central role of data in future economies is obvious. We won't pile onto the consensus, except to stress the point with reference to a few current initiatives.

- The Consumer Data Right (CDR) and the DATA Scheme created by the Data Accountability and Transparency Act are world-leading expressions of open banking and open data public policy reform. They each have a long way to go but we applaud that the CDR introduced enforceable cyber security standards for the first time in Australia, and the DATA Scheme brings a new *infostructural* focus with the Dataplace platform and something of a two-sided network structure joining accredited Data Users and Data Custodians.
- State government data sharing and analytics programs have been given additional structure and direction by the Australian Computer Society's recent *Frameworks and Controls for Data Sharing*.
- David Tudehope (CEO, Macquarie Telecom) writing for the Australian Strategic Policy Institute (ASPI) in July 2021 stated that "data is effectively the economy's critical infrastructure".

Data is itself now a utility as important as energy, food supply chains or transportation. And yet it remains precarious. Data is manipulated by bad actors at a scale unimaginable only 10 years ago, resulting in harms ranging across infrastructure disruption, theft, fraud, and distortion of national elections.

Identity fraud (and perhaps all cybercrime) is actually about bad data. The systemic reason that data breaches are so harmful to citizens and so fruitful for criminals is that no one can easily tell the difference between genuine original data and copied or synthetic data. Digital impersonation through stolen personal details is ridiculously easy and has been industrialised by organised crime.

A new idea: infostructure

Data is so critical now, it merits *infostructural* security so that the economic users of data can be confident knowing where it has come from and what it is intended to be used for. By *infostructure* we mean organised systems of standards, rules, technologies and governance processes that together protect data as a utility.[1]

To protect data holistically, we must start at the source(s). Government is trusted for so much of our core data, through critical resources such as birth and name change registers, citizenship and immigration records, driver licensing and electoral rolls. If the mission of government is to both protect and serve the citizenry, then when it comes to data, the most basic role for government could be to **make official data available to those who need it in the most reliable possible way**.

[1] The Oxford English Dictionary defines infostructure as "an organisational structure for the collection and distribution of information … hardware, networks, applications, etc. used by a society, business, or other group".

For resilience against breaches and cybercrime, citizens don't need changes to their official data (much less should they be changing their registered data after every major breach). And businesses do not need new identity data. Rather, all parties need the data to be better. Important data should be made verifiable, mobile, tangible, safeguarded against illicit replay, and useless to criminals.

It would be a simple matter for governments to issue official data to a choice of mobile wallets without any change to the data or its meaning and for consumers to have the option to present their data digitally with an easy, familiar "Click to Prove" user experience. Mobile wallets make data better.

The digital option for data presentation could be phased in, being offered to start with in select government and business web forms. Verifiable digital presentation would not be mandatory; organisations could continue to accept plain text personal data entry as they do now, although pressures to adopt the better option will emerge if and when it proves to be easier, faster and safer.

Take-up of new identification methods is in fact determined more by businesses than consumers. Businesses today know what to do with official government-issued data and are generally resistant to new data because it brings new rules and risks. What businesses really need is better assurance that the core data they routinely rely upon is known to have come from the official source, has been presented with consent by its legitimate subjects, and hasn't been tampered with or synthesised.

Data resilience is a solved problem in payments. The "identity problem" presumed to arise with data breaches can be reframed and solved in the same way as card payments, familiar to many consumers already. Citizens should have the means to present verifiable facts about themselves as easily, privately and securely as they present their payment details when shopping online. That transformation alone would do more to undercut organised identity crime than any other proposal we've seen. And it's already underway.

End-to-end support

Mobile wallets are a reality in payments and are being extended to hold all manner of digital credentials. The industry standard technology is known as "verifiable credentials"; multiple Australian public service agencies are well advanced in procuring verifiable credentials solutions. State and federal Ministers have recently highlighted the potential for a range of government credentials to be digitised and held in a choice of wallets. This is great progress and sets the stage for national infostructure.

And yet a subtle point about interoperability goes unnoticed in the enthusiasm for mobile wallets. **Digital credentials and wallets only work when the intended receivers know what to do with them and have arrangements in place for their software to recognise and accept approved credentials**.

This reality is readily appreciated by considering credit card arrangements. When a merchant decides to accept credit card payments, they sign on with a chosen card scheme and install terminals and/or gateway software to process customer details. Customers'

cards are useless without these arrangements on the merchant's side. It doesn't matter what sort of wallet you use: it is the *merchant's set-up* that determines which cards you can use to go shopping.

Therefore, Australian governments need to consider more than legislation when rolling out digital credentials, especially when certain credentials are going to be mandatory. Consider proof of age for online liquor purchase. It seems likely that multiple options will soon be available from Australian state governments. National online retailers (actually, their software providers) have a major challenge ahead working out which proofs of age are officially endorsed (or perhaps mandated).[2]

Verifiable credentials are a powerful tool, but they do not verify themselves. They must go hand-in-hand with infostructure for (a) approving issuers before loading credentials to a wallet, and (b) processing credentials when presented to parties depending upon them.

Data protection for a cyber secure nation

A cyber secure nation will treat data as an asset, as important as clean drinking water or stable electricity supply.

We suggest that a cyber secure nation would feature widespread uniform digitally secure data handling. At present, most organisations handle data on an ad hoc basis, making decisions in isolation as to which sources of data they trust, what standards to follow, and what liability goes with using data. Consider how difficult it is for these decisions to be made in the field of trade qualifications. State governments wish for digitised qualifications and licences to be interoperable nationwide, but employers and training organisations (and software vendors too) will need to make separate bilateral arrangements for digital credentials to be ingestible online. We risk losing the economic dividends of digital transformation in a rat's nest of bilateral administrative decisions.

A cyber secure nation will no longer tolerate ad hoc point-to-point data connections and unverified data flows—just as it is illegal to make unlicensed electricity and gas connections. Instead, a cyber secure nation will build public platforms for brokering data issuers and data users. It is good that some such governance is anticipated in the Commonwealth's DATA Scheme.

We need more security built in. For instance, all crucial data flows should be cryptographically signed and verifiable, in the same way that embedded chip technology

[2] On a technical point of detail, the relying party software processing verifiable credentials presented by customers must be configured ahead of time with metadata that characterises the recognised credential issuers, the approved credential formats, the version numbers of governing standards, the certification status of the credential issuers, and the "master keys" (public root keys) with which to decode digital signatures on credentials. Without these technical details, the receiving software will, by design, reject the presented credentials, in the same way as a merchant terminal configured to only accept Vias and Mastercard will reject an American Express card.

is used to seamlessly protect the integrity and provenance of data flows from Apple and Google wallets, tap-and-go transit tickets and e-passports.[3]

Our responses to selected Strategy Discussion Paper Questions

Question 1. What ideas would you like to see included in the Strategy to make Australia the most cyber secure nation in the world by 2030?

- Reliable pedigreed data is as important as clean drinking water and stable electricity.
- A cyber secure nation would have nation-wide *infostructure* to distribute digestible data and quality-related metadata, such as proof of origin, proof of possession, intended use, and terms & conditions for use.
- Governments should continue the transformation to digital wallets in citizen service delivery but must appreciate that wallets and verifiable credentials do not work at scale without underpinning infostructure that makes the meaning of all data machine-readable, clear, and dependable.
- Infostructure in general is core business to government, dating from well before the digital age. Examples include telephone and telecommunications networks, Medicare and PBS payments, e-passports, electronic conveyancing, and the NBN.
- Private-public partnerships can build and operate the new data protection infostructure, incrementally, modelling on existing two-sided network business models in retail payments.

Question 6. How can Commonwealth Government departments and agencies better demonstrate and deliver cyber security best practice and serve as a model for other entities?

- Commonwealth agencies can almost immediately offer "Click to Prove" user interfaces for presenting selected official data, beginning perhaps with Medicare numbers. Citizens would be given the option of having their Medicare number issued as a verifiable credential in a mobile wallet.
- Services Australia could develop an API and web service for any other organisation to ingest and verify Medicare numbers from mobile wallets. Healthcare providers could invite their patients to "Click to prove" their details digitally. Verifiable patient Medicare numbers is one way to curb common and costly forms of provider fraud.
- Such APIs and web services could then be expanded (while driver licences and the like are rolled out to verifiable credential wallets) and made available to any AML-governed entity for digital identification in account opening.

[3] Note that any new national digital ID as flagged by the Prime Minster would need to use state of the art verifiable credentials and mobile wallet technology. Yet these very same tools could be deployed today to safeguard the personal data elements used in routine identification, and close off the pinch points where stolen data is used by fraudsters. By phasing in verifiable credentials for driver licences, Medicare cards and birth certificates, government would render stolen data useless to criminals and thus defuse the black market for personal information.

Question 16. What opportunities are available for government to enhance Australia's cyber security technologies ecosystem and support the uptake of cyber security services and technologies in Australia?

- Given that government is the authoritative source of so much official data used in routine identification and digital risk management, a foundational opportunity is to make official data available in the most modern and reliable form factor.
- It would be a simple for state and federal governments to issue official data to a choice of approved mobile wallets (without any change to the data or its meaning) and for consumers to have the option to present their data via the "Click to Prove" user experience now familiar to so many. Official citizen data would then be mobile, more tangible and controllable, instantly verifiable by service providers, and useless to criminals.
- The "identity exchange" function of Services Australia (which in Lockstep's estimation will be fast superseded along with TDIF by modern verifiable credentials approaches) should be reframed around data distribution and rearchitected to play the role of a fourth party public utility for data verification.

About the authors

Stephen Wilson is a researcher, innovator and analyst in data protection. He has been a lead digital adviser to the governments of Australia, Hong Kong, Indonesia, Kazakhstan, Macau, New Zealand, and Singapore, and has been awarded 10 patents. He was a member of the NSW Digital Identity Ministerial Advisory Council (DIMAC). Steve's clients and projects have included the NSW Digital Driver Licence, Medicare Australia, the National eHealth Transition Authority, and the W.H.O. digital vaccine certificate working group. Lockstep is the only Australian company to be awarded a commercialisation contract by the U.S. Dept of Homeland Security (for a mobile digital credential wallet for First Responders).

George Peabody is a payments adviser, writer and entrepreneur, based in Boston. He consults across a range of business and technology areas with emphasis on mobility, merchant risk, online and offline data security, and digital identity. An accomplished communicator, George is the producer and host of Glenbrook Partner's 100+ episode podcast series, *Payments on Fire®*.

In 2013, George and Steve published *Fractional Identity: An Alternative to NSTIC and Federated Identity*, which made the case to shift focus from centralised identity providers to contestable attribute providers, foreshadowing today's verifiable credential movement. In 2023, George joined Lockstep Consulting as a Partner, to collaborate on the development of a data verification architecture.