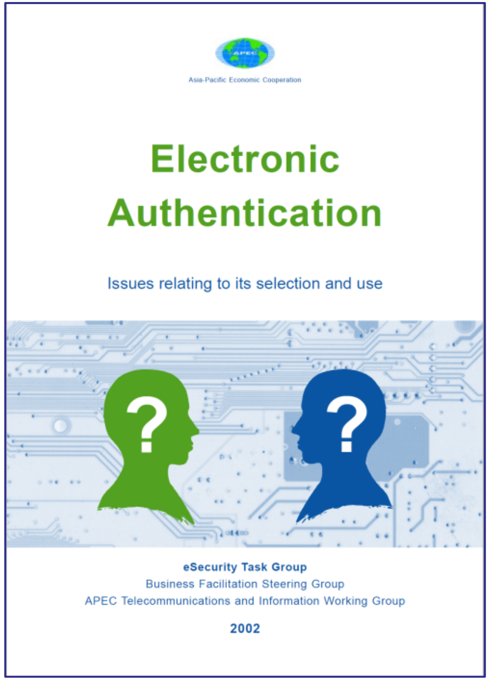
Data Protection Infrastructure for the Digital Economy

Citizens should be able to move trusted copies of their personal data around the digital economy as easily and as safely as they move their money.

Stephen Wilson
Lockstep

Based on a presentation to *Technology in Government,* Canberra, August 6, 2019.

Authenticity



Asia-Pacific Economic Cooperation

Electronic Authentication

Issues relating to its selection and use

eSecurity Task Group
Business Facilitation Steering Group
APEC Telecommunications and Information Working Group

2002

While digital identity has been simmering for many years, a more urgent problem has emerged: *authenticity*. How do we know what's real in the digital space? How do we combat digital counterfeits and fake accounts? How we do we shut down the black market in stolen data? We can frame authenticity very simply as *data protection* and then leverage digital identity know-how and solutions. The foundational work on authentication done by the APEC eSecuity Task Group is useful:

> ***The means by which a receiver of an electronic transaction or message makes a decision to accept or reject that transaction or message.***

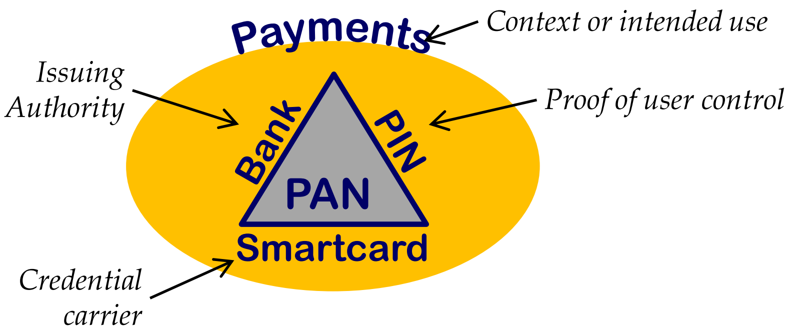
This way of framing authenticity is strong on both privacy and security, reflecting the principles of *Collection Limitation*, *Disclosure Limitation* and *The Need To Know*.

So in plain language, there are three questions for all online transactions:

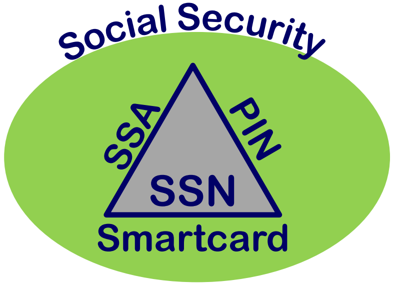
1. *What does a Service Provider (or Relying Party) need to know about its Customers or Users?*
2. *Where will the Service Provider get that information?*
3. *How will it know the information is true (or true enough) for its purposes?*

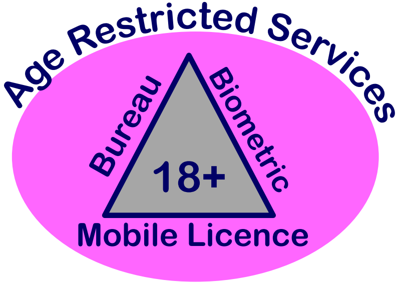
Today the digital identity industry provides a mature set of software tools, personal devices, web services and standards for conveying verified claims about users.

What do you need to know? How will you know it's true?



Future





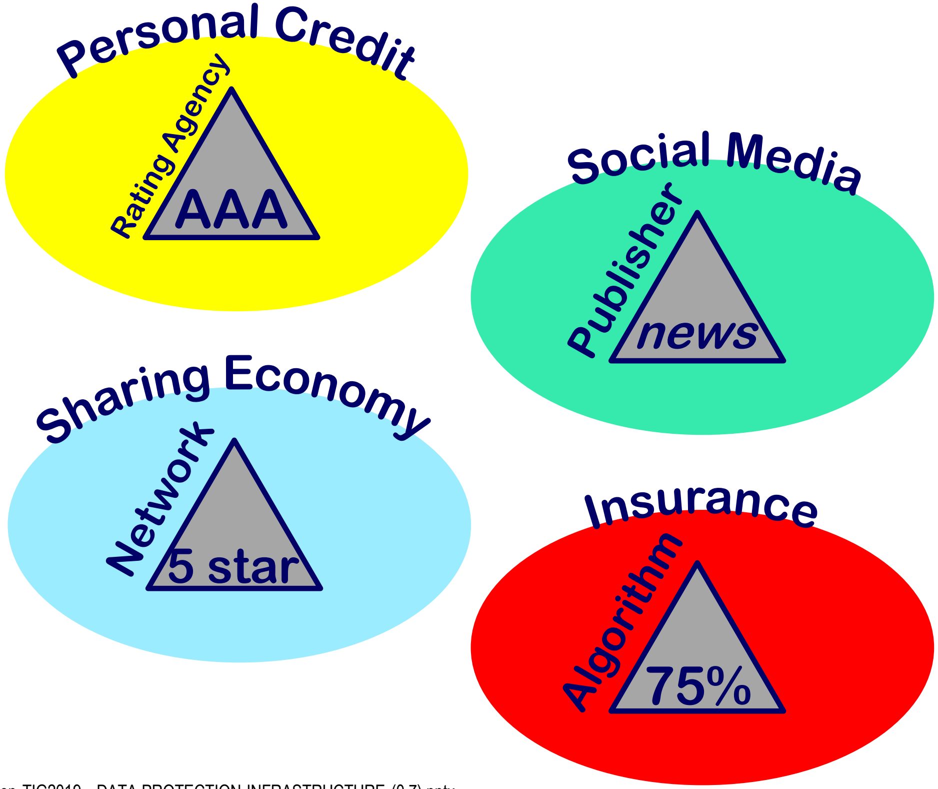
The things we need to know depend on the context of an activity or transaction. For example, a merchant really only needs to know a customer's credit card number (PAN) and expiry date. Tragically, data breaches have made card data unreliable, so merchants gather extraneous information like CVV — which in turn gets stolen and traded on the black market, creating a vicious cycle. If card data sent over the Internet was inherently trustworthy (as it is in a card-present transaction) then the extra details would be unnecessary, merchants would be safer and consumers more private.

Most personal attributes of interest have a natural authority or *source of truth*; for credit card numbers, it's the issuing bank; for age, it's classically a driver licence bureau.

The credential carrier used to present an attribute can add an extra layer of security. A smart credit card for example offers *proof of possession* or user control. Unlocking a smartcard by PIN demonstrates that the card is probably being operated by its legitimate owner.

Similarly, a mobile driver licence could be used to convey the holder's age with proof of possession by a biometric. A smart Social Security card protected by PIN could convey the Social Security Number.

Provenance generally



The digital identity industry has developed a range of protocols, tools and solution patterns for conveying the provenance of authentication data. These same techniques are ready to be applied to the bigger problem of provenance of all data.

Data provenance and other qualities are critical as the Digital Economy takes shape. We need to know that a properly registered doctor signed a prescription, a reputable agency issued a credit rating, an accredited media bureau originated a news report, a legitimate party published a social media advertisement, an endorsed algorithm generated an insurance risk rating, and a genuine customer posted a rating for a share-ride.

Eventually, every participant in the emerging data supply chains should be adding their own verifiable quality signals (evaluations, attestations, ‘digital assays’ and other metadata) to information as they process it and move it on down the line.

“Data is the new crude oil”

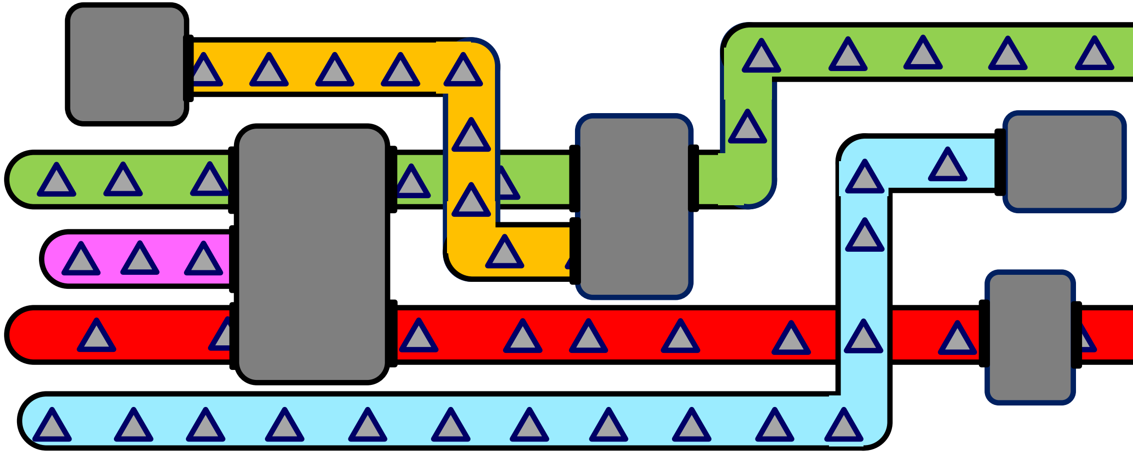
Data may be compared to crude oil for economic importance amongst other things. We shouldn’t stretch the metaphor but it does run deep. Data is making certain business people great fortunes; it is the lifeblood of new companies and whole new sectors; and uncontrolled data mining is laying waste to corners of the Internet.

Look at Huntington Beach, California circa 1920 at the peak of the oil rush, and as it is today. Oil hasn’t gone away but we’ve made the petroleum industry *orderly*, and imposed regulated and standardised supply chains.

COMMERCIAL IN CONFIDENCE

Data supply chains

The metaphor of data as crude oil has other implications, such as the need for orderly data supply chains. If we draw on the lessons of digital identity, we can recognise an emerging ecosystem of attribute (or claims) providers and verifiers, meeting the needs of "relying parties" or, simply, data processors and data intermediaries. Many of these players exist today as information brokers; many are in a state of flux as they improve their business models and practices.

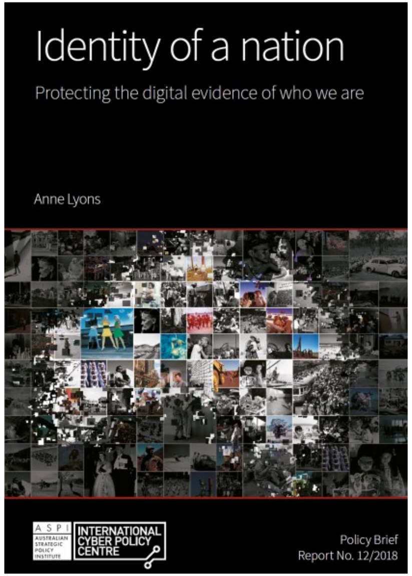


To better protect the emerging data supply chains, we can leverage existing digital identity technologies. We can also draw on the experience of the payment card industry, which has moved away from ad hoc handling of raw card numbers: precious account data is now handled automatically in chip cards, digitally signed, encrypted and/or "tokenised" to protect it against breaches or theft. The same techniques can be used to protect *all* data flows against tampering and counterfeiting.

An orderly industry

Petroleum supply chains depend on physical critical infrastructure as well as *soft* infrastructure, including rules and social norms. For instance, petrol is only sold at licensed service stations. Likewise, over time, we should expect data flows to be more tightly controlled through smart technologies, replacing clumsy human handling, and curtailing bad habits formed in the early ‘Wild West’ days of the Information Age.

An orderly Digital Economy



Identity of a nation

Protecting the digital evidence of who we are

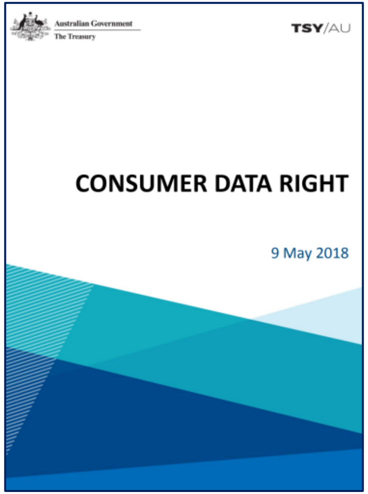
Anne Lyons

ASPI AUSTRALIAN STRATEGIC POLICY INSTITUTE

INTERNATIONAL CYBER POLICY CENTRE

Policy Brief
Report No. 12/2018

As with all industries, the right level of regulation for information technologies is settling out over time, which will enable critical *infostructure* to be built on a public-private basis. An early example is the *Consumer Data Right* for Open Banking and fair data sharing. Anne Lyons of the Australian Strategic Policy Institute has called for national identity assets to be treated as critical infrastructure.



Australian Government
The Treasury

TSY/AU

CONSUMER DATA RIGHT

9 May 2018

The digital identity industry has created solutions and governance frameworks that are ready to protect the provenance and fidelity of all critical data, while it is moved, refined, value-added, and injected into new economic processes. Leveraging identity technologies and existing networks, citizens could therefore be given the means to move verified personal data around as easily and as safely as they move their money today.