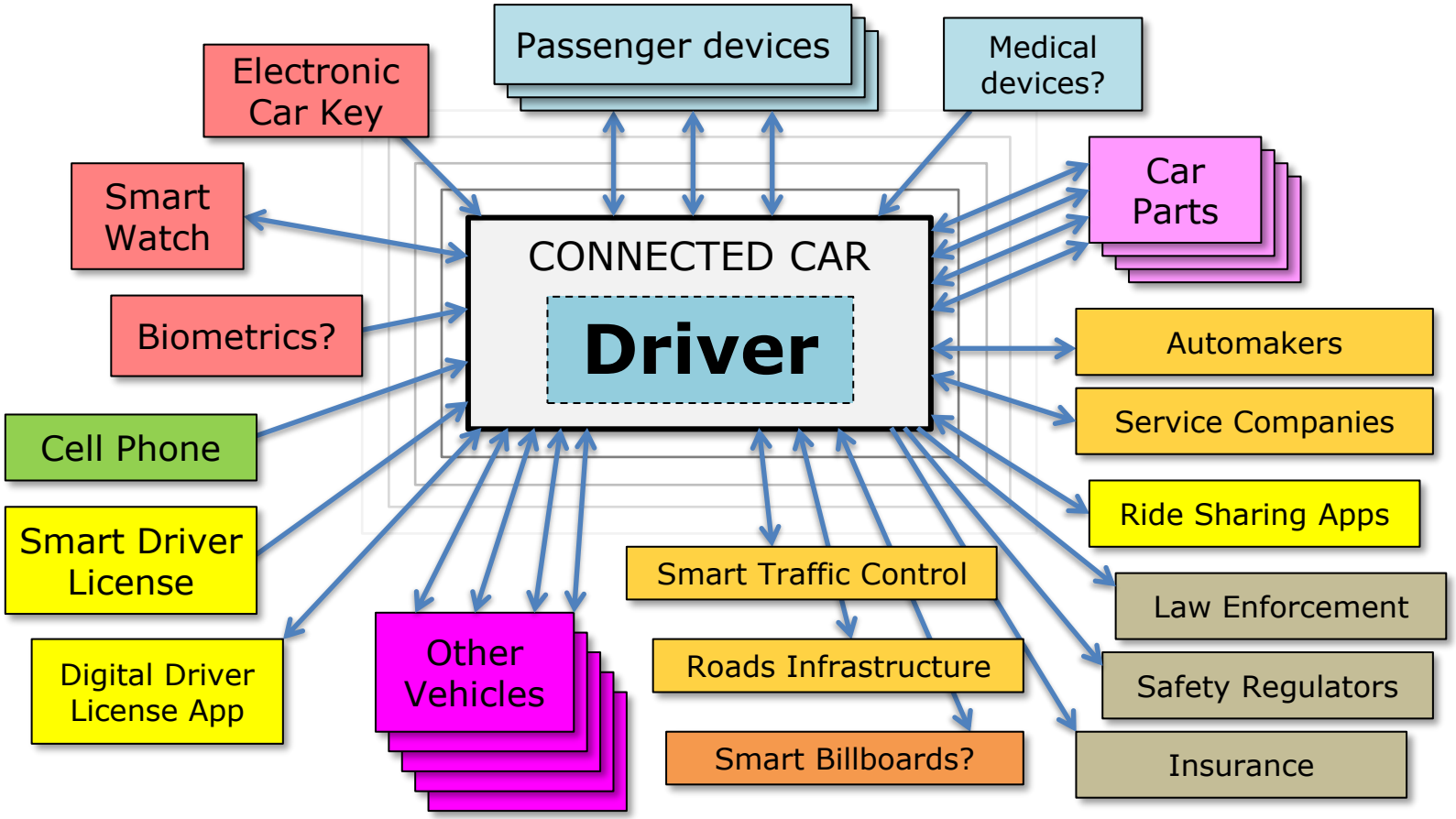
A Digital Identity Stack to Improve Privacy in the IoT

Stephen Wilson, Nour Moustafa & Elena Sitnikova
University of NSW, Canberra

IEEE 4th World Forum on Internet of Things
Singapore
5 February 2018

The Internet of Things

If we don't attend to personal information flows in the Internet of Things, cyberspace will turn into privacy "grey goo". Just look at how personal data leaks around connected vehicles (where Ray Kurzweil estimates one gigabyte of data is generated per car per second).



The Internet's "Identity Crisis"?

For many years commentators have said the Internet was created without an "identity layer". Microsoft's Laws of Identity, The OpenID Foundation and the Identity Commons community all explicitly have an "identity layer" in their missions. But there's been no precision in this idea.

"The Internet's Missing Identity Layer"

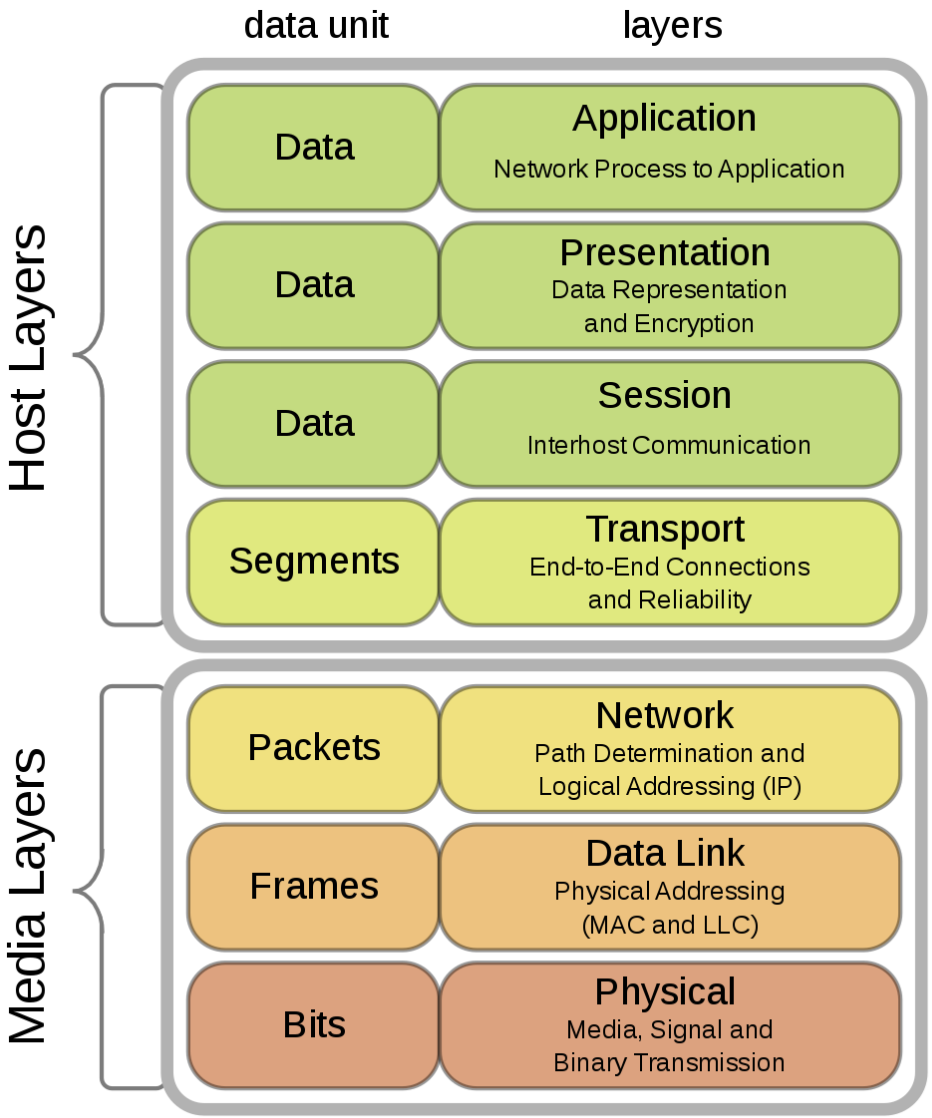
https://www.identityblog.com

"The Internet Identity Layer"

http://openid.net

"The purpose of Identity Commons is to support, facilitate, and promote the creation of an open identity layer for the Internet"

The classic stack



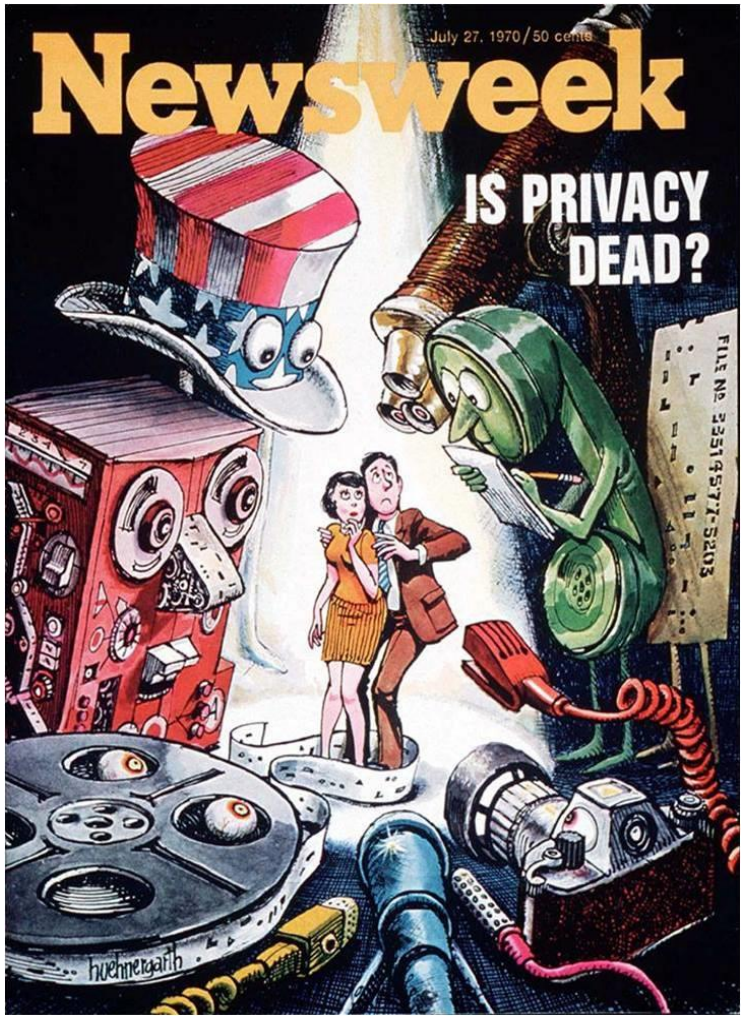
Presumably people calling for an identity "layer" have in mind something like the classic OSI Network Technologies stack.

Privacy Risks in the IoT

- *Monitoring via connected devices*
- *Non-consensual Capture of PI (often not understood)*
- *Medical Info from health & fitness products*
- *Breakdown of Informational Contexts*
- *Diversification of Stakeholders (appliance manufacturers morph into info business)*
- *Backdoor Government Surveillance*

Ref: Gilad Rosner 2016

Privacy for Engineers



We keep hearing "privacy is dead". This headline is from the 1970s. It's a rhetorical question, and the answer is no.

But technologists continue to be a bit confused or conflicted.

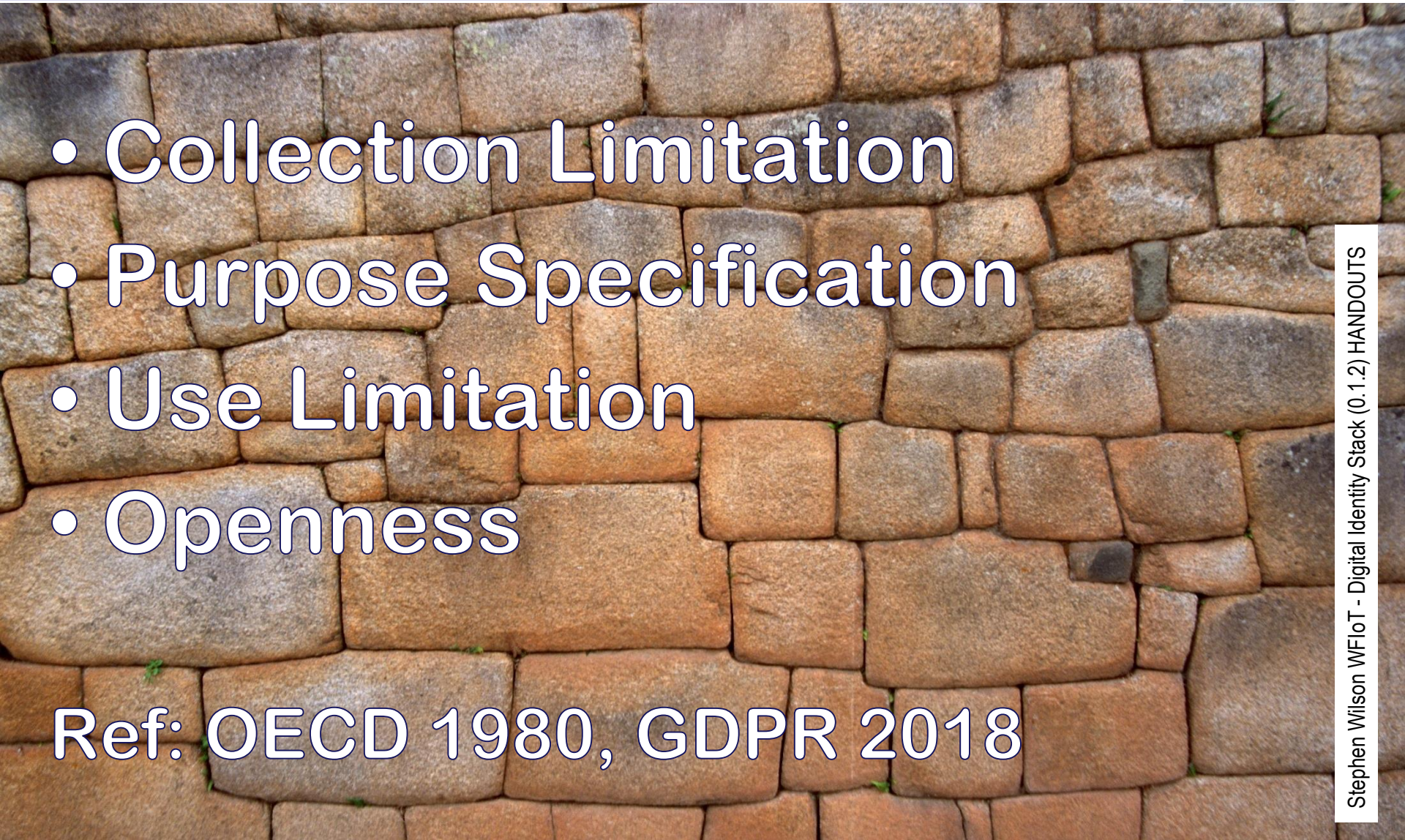
Privacy for Engineers

Privacy is not about Secrecy

Privacy is really about *Restraint*

Privacy can be at odds with other system goals. *Engineering* an information system entails resolving competing requirements, including privacy, security, convenience, efficacy, usability, cost and revenue.

Privacy Principles



- Collection Limitation
- Purpose Specification
- Use Limitation
- Openness

Ref: OECD 1980, GDPR 2018

“Digital Identity” is evolving

For all sorts of reasons, the focus in cyber security is dropping down from abstract identity to concrete matters of claims and attributes. It doesn’t matter who you are so much as what you are. The canonical definition of Digital Identity was actually always about attributes.

- **Digital Identity: “A set of claims” Ref: Kim Cameron 2005**
- **Identity shifting from *Who* to *What***
  - **FIDO Alliance www.fidoalliance.org**
  - **IETF Vectors of Trust (Justin Richer et al)**
  - **W3C Verifiable Claims (Manu Sporny at al)**

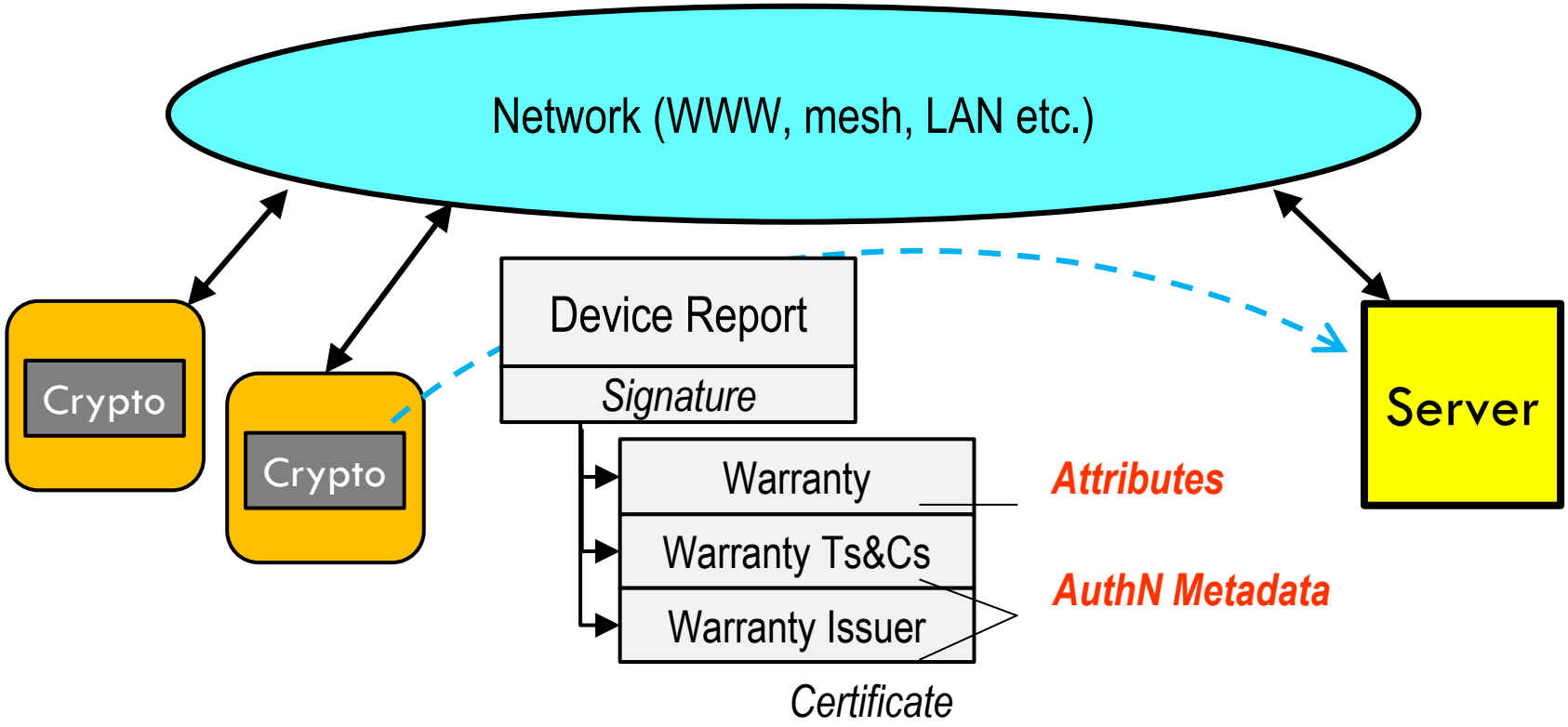
A Digital Identity Stack

Applications	*Employment, Retail, Banking, Payments, Insurance, Healthcare, Government Services, Education, Licensing, Membership, Professional Services etc.*
Digital Identities	*Account names, Legal names, Aliases etc.*
Attributes	*Account No., PAN, CRN, Policy No., License No., Employee ID, Student No., Degree, Exam Results, Professional Registration, SSN, DOB, Age, Home Address, Mailing Address, Zip Code, KYC data, Citizenship, Visa, Patient ID, Health Status, Clinical Trial ID, Medical Device No. etc.*
Attribute Metadata	*Verification, Attribute Issuer, Notary, Employer, School, Govt Agency, Issuance Date, Storage Device Type, Device Manufacturer, Consents, Applicable legislation, Terms & Conditions, Obligations and Constraints, Warranty etc.*
Protocols	*FIDO U2F, FIDO UAF, OAuth, OIDC, SAML, PKIX*

Privacy benefits of the Stack

- Better design patterns
- Focus of Need-to-Know
- Minimise disclosure
- Privacy enhancing metadata

Worked example



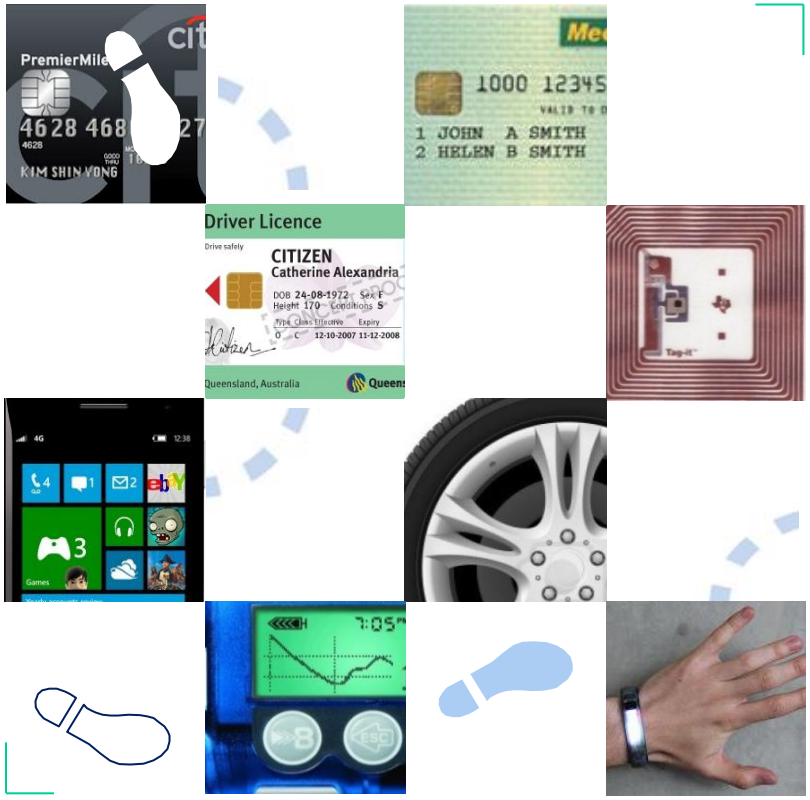
See paper for details.

Organising the Digital Economy

If data is "the new crude oil" then we need to start treating it more seriously, as critical raw material. Contrast data management with our mature petroleum supply chains which are properly and strictly regulated. We need to take care of the provenance of all data – where does it come from, what are we allowed to do with it, how are we allowed to process and distribute it? These are the core concerns of data privacy, but faced with ever-mounting data breaches and all the unaccountable data sloshing around cyberspace, data provenance needs now to be everyone's priority.

- **A stack helps shape the supply chains, clarifying how elements of digital identity can be sourced**
- **Helps define the critical infrastructure needed to protect the provenance of data and permissible information flows.**

Discussion



swilson@lockstep.com.au
http://lockstep.com.au