Trust in the Post-Identity World

Stephen Wilson, Lockstep Consulting

with George Peabody, Glenbrook Partners

Identiverse 2022, June 23, Denver.

The Internet, e-commerce and digital discourse are dominated by identity. Until recently, identity was all we had to go on when trying to trust anyone or anything online. We developed a terrible habit of over-identifying: Relying Parties collect circumstantial clues (like credit card verification codes and social security numbers) instead of properly verifying what really matters; people divulge excessive personal data, often unwittingly, which leaks and gets abused by criminals. Thus, too much identity is sloshing around.

Is there a paradigm shift coming? The most important developments in our industry — Self Sovereign Identity, the FIDO Alliance and cryptographically Verifiable Credentials — are not about Identity, but authorship, provenance, integrity and control.

In this session, we will move the conversation beyond Identity and imagine a world where cryptographic infostructure is as universal as electricity or clean water, and all the data we need is hall-marked, traceable and trustworthy thanks to authentication technologies.

Obsession

I say this with love and respect for my dear friends in the industry: we have to end our obsession with identity. For thirty years, identity has dominated digital practice and discourse. We overcook the Peter Steiner cartoon; it was a fantastical gag about dogs getting up to mischief, not a commentary on digital trust.

For all that time, when trying trust anyone online, identity was all we had to go on. When faced with higher risk, we would seek higher trust and ask for more identity. We put quantity of identity ahead of quality. We put identity first.

Received wisdom in our industry holds that a "missing identity layer" is the Internet's "original sin".

CartoonStock.com
"On the Internet, nobody knows you're a dog."
P. Steiner

Bad habits

We developed terrible habits. Instead of verifying the particulars that really matter about people we deal with, we drag in extra identifying data from unrelated contexts, such as CVVs and SSNs, much of which is then stolen and bought and sold and replayed by fraudsters. Consider Knowledge Based Authentication, which places a premium on “out of wallet” details which should be less likely to be known to criminals. But personal information is everywhere on the Internet and KBA backfires by motivating a black market for personal data. Identification for digital risk management can be like putting out fire with gasoline. We should do more to secure the facts & figures transactions depend on.

WORLD BANK GROUP

Data as a utility

Meanwhile data has become the lifeblood of modern society. The World Bank recently called for a “new social contract for data” to protect citizens against harm arising from the information and power asymmetries created by big tech.

Data is now a resource almost as important as clean drinking water. Yet we access, accept and recommend data on an ad hoc basis; outside certain professions and intelligence circles, data is handled without any standards for quality or provenance.

Ref: *Data for better lives: world development report*, World Bank, 2021.

Regulatory pressure

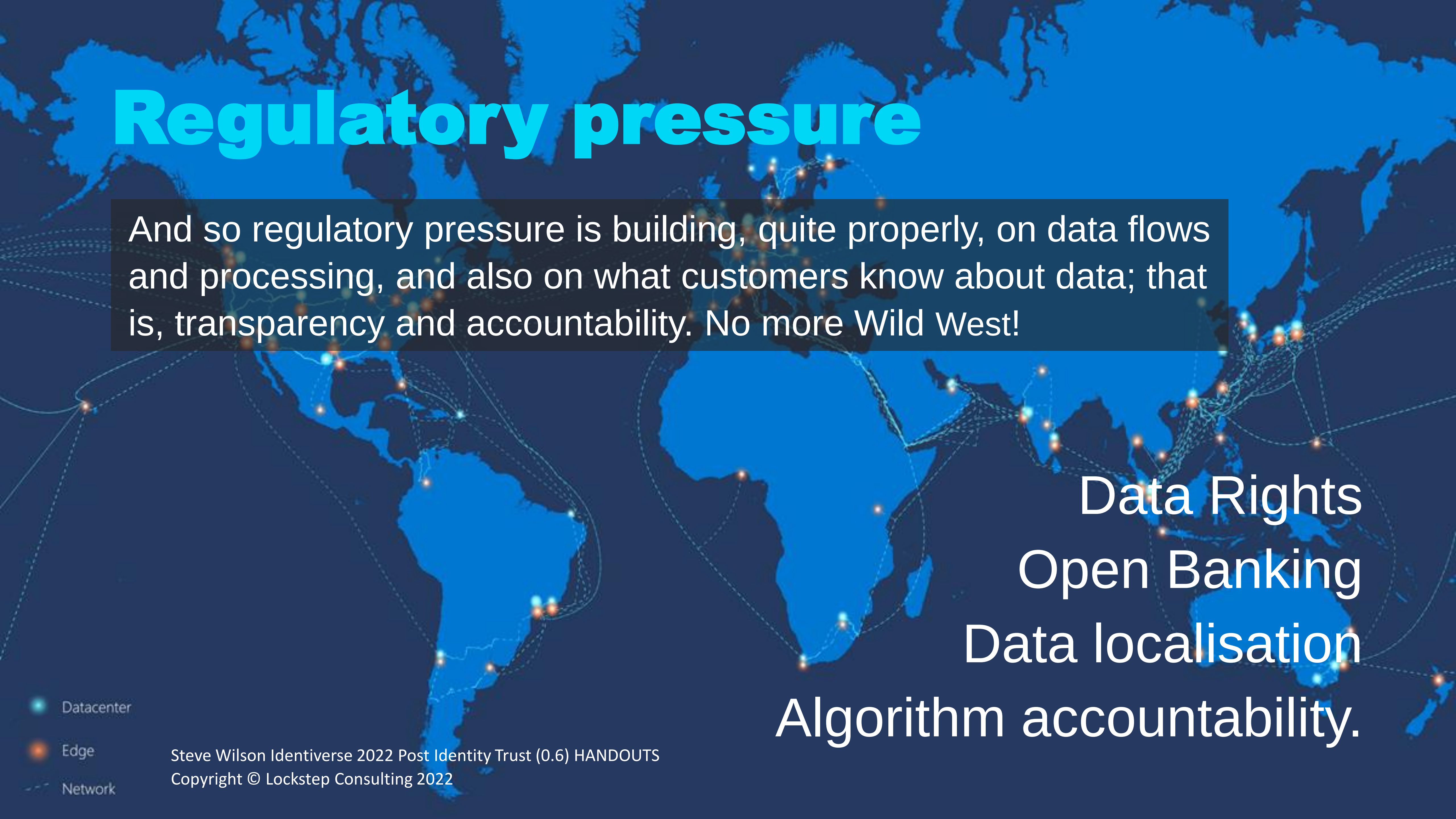
And so regulatory pressure is building, quite properly, on data flows and processing, and also on what customers know about data; that is, transparency and accountability. No more Wild West!

Data Rights

Open Banking

Data localisation

Algorithm accountability.



Digital truth

Cynics say we are *post truth* but surely the biggest challenge as cyberspace grows in importance really is digital truth. From payment card fraud and online scams through to misinformation and AI-driven Deep Fakes: every one of these problems is fundamentally about poor quality data. We can’t trust the evidence of our own eyes anymore. Are we really going to launch digital twins without taking better care of fidelity?

Card Fraud

Phishing

Romance Scams

Synthetic Identities

Weaponization of Information

Deep Fakes

Steve Wilson Identiverse 2022 Post Identity Trust (0.6) HANDOUTS

Concerted responses

The global information environment is a form of 'market' that needs exchange protocols and local standards — VIE.

C2PA

Coalition for Content Provenance and Authenticity

Verified Information Exchange

Concerted multidimensional responses to the data quality problem are underway (not to mention some narrow legislated bans on Deep Fakes). For one, several major mastheads have teamed with Microsoft Research in the content provenance coalition. The C2PA's first draft standard draws heavily on technical measures familiar to the identerati, such as digital signatures.

And the new *Verified Information Exchange* (VIE) is an interdisciplinary research program hosted by UW. The VIE work program suggests that network (i.e. scheme-based) business models are emerging for data supply.

Global Assured Interoperability Network

GAIN DIGITAL TRUST

How Financial Institutions are taking a leadership role in the Digital Economy by establishing a Global Assured Identity Network

With over 150 co-authors

D.3.2.3 Privacy Dashboard

Participating Identity Information Provider in GAIN will provide a dashboard from which the End-Users can find out easily where and which data has and is being shared for what purpose and how. End-Users can review where data has been shared and stop any persistent sharing from within the Identity Information Provider Dashboard.

D.3.3 Data Flow View

Data Flow View provides how the Information including user and administrator direction flows and stored among the roles to be implemented in GAIN.

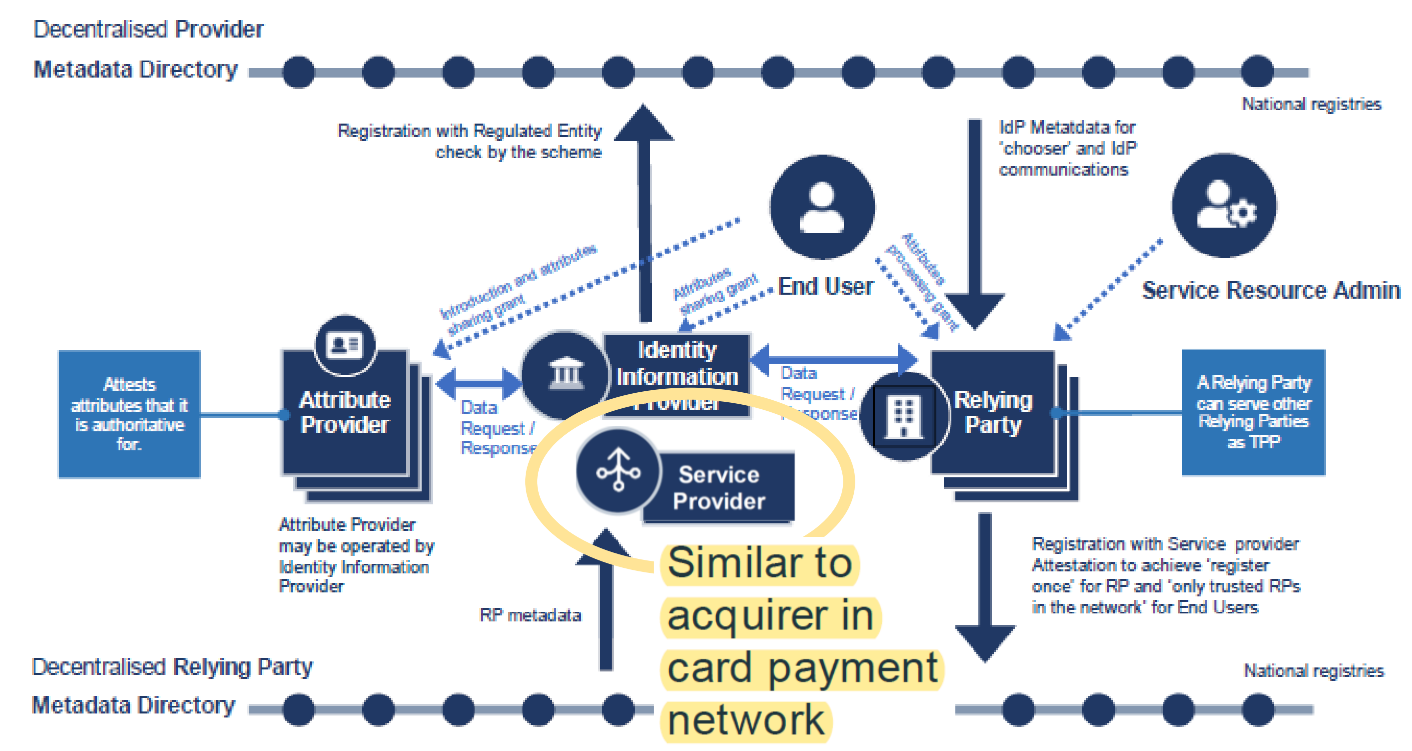
Figure D.4: Data Flow in the GAIN

Note: RP Onboarding requirements may differ from jurisdiction to jurisdiction and it probably requires multiple levels of identity proofing and verification.

- **End-User:** End-User is a role primarily performed by individuals and is the central role in the GAIN. They are authenticated by User-AuthN and control how and where their data is being shared and used.
- **Service Provider:** It is a role that performs initial authentication (identity proofing) of the Relying Party and provides standardized attestation which Relying Parties can take and provide to the Relying Party Metadata Directory. This role is typically played by a regulated entity that has a requirement for identity proofing of the Relying Parties as their customer. It
  - implements the management system to achieve the assurance level expressed in the attestation;
  - support mapping of the Relying Party to a Legal Entity Identifier (LEI)[30] and a verifiable LEI (vLEI)[31] in partnership with the Global Legal Entity Identifier Foundation (GLEIF)[32]; and
  - support issuing the attestation in the standard format adopted by GAIN that include the information above.

42 of 49

Figure D.4: Data Flow in the GAIN


Decentralised Provider
Metadata Directory
National registries
Registration with Regulated Entity check by the scheme
IdP Metatdata for 'chooser' and IdP communications
End User
Service Resource Admin
Introduction and attributes sharing grant
Attributes sharing grant
Attributes processing grant
Attests attributes that it is authoritative for.
Attribute Provider
Data Request / Response
Identity Information Provider
Data Request / Response
Relying Party
A Relying Party can serve other Relying Parties as TPP
Service Provider
Attribute Provider may be operated by Identity Information Provider
RP metadata
Registration with Service provider Attestation to achieve 'register once' for RP and 'only trusted RPs in the network' for End Users
Decentralised Relying Party
Metadata Directory
National registries

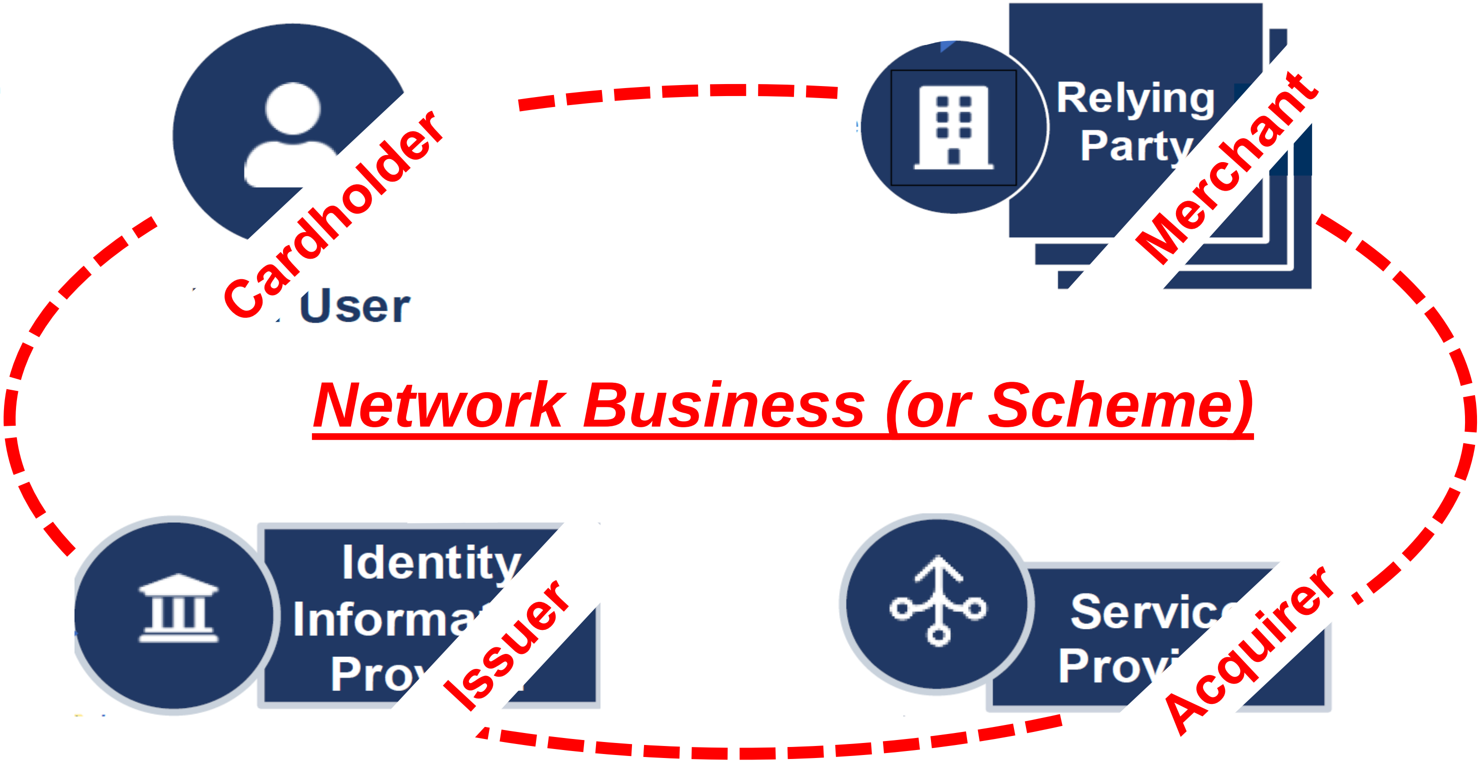
Similar to acquirer in card payment network

Another new effort, GAIN, was prominent at Identiverse. It means different things to different stakeholders; even the ‘I’ in G.A.I.N. since the initial publication has been reframed as *interoperability*. One of the best features of the concept is buried on page 42 of 59. The *Service Provider* is a fourth party in the data flow, joining the familiar End User, Issuer and Relying Party. It is explicitly likened to the *acquirer* in the global card payment network.

Steve Wilson Identiverse 2022 Post Identity Trust (0.6) HANDOUTS

Infostructure

Payment cards and the processing network exist purely so that certain customer data — account numbers and some metadata — can be reliably presented to merchants and verified. GAIN represents an extension of the four-party model for presenting and verifying data more generally.



The acquirer is the key to global scalability. The acquirer provides technology and legal support: merchant onboarding, methods to ingest customer details (card terminals, internet gateways and/or APIs) and, above all, a standard form of merchant service agreement with service levels, liabilities and fee structures which can be fine-tuned regionally.

Card schemes are a paragon of *infostructure*:

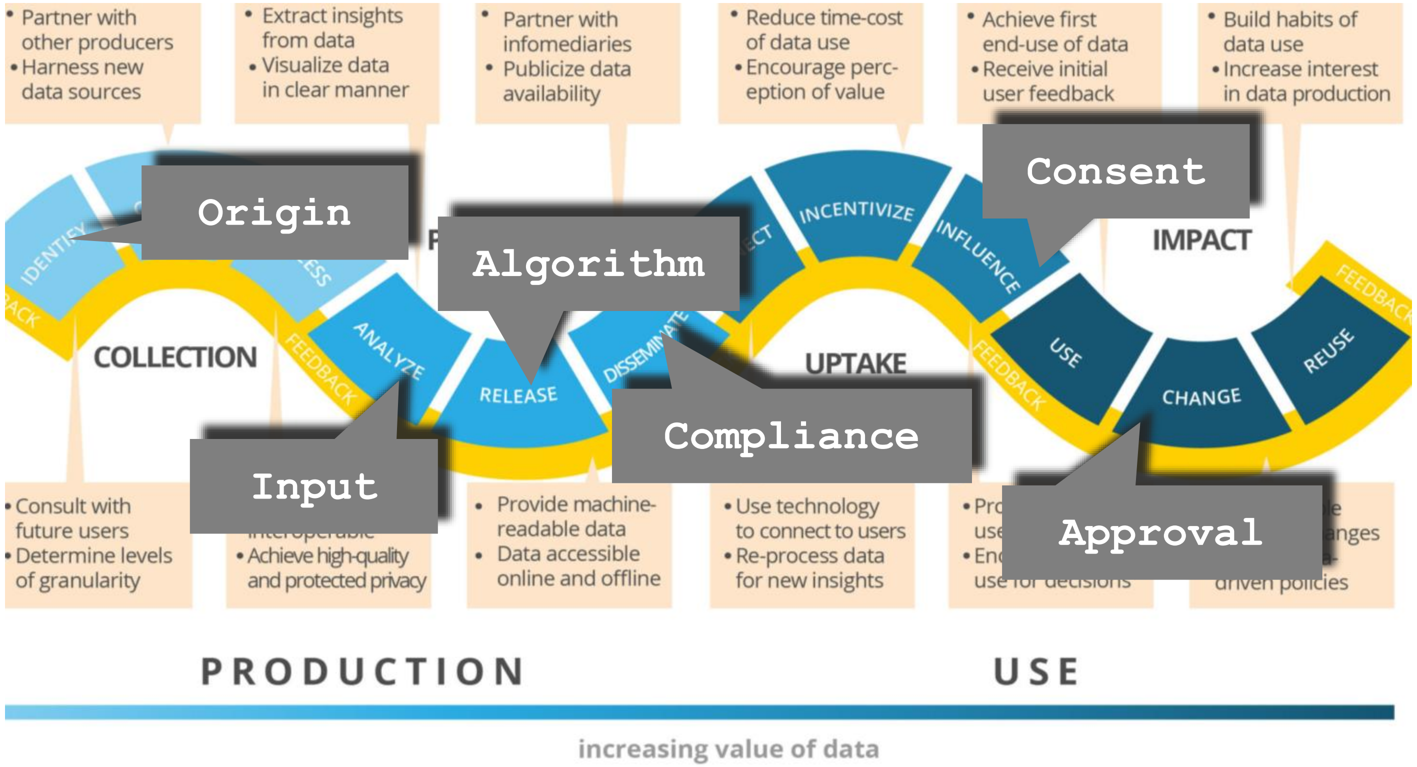
> *An organizational structure used for the collection and distribution of information (usually hardware, networks, applications, etc.) used by a society, business, or other group* (OED).

That is, verifiable data sharing will be underpinned by rules, technologies, and business models.

#identiverse

Information assays

We know data is big business — both good and bad — and that information is being organised into value chains and supply chains. We are still at the very early stages of digital transformation. As cyberspace becomes civilised, we need data business to be more orderly and more transparent.



Partner with other producers
Harness new data sources
Extract insights from data
Visualize data in clear manner
Partner with infomediaries
Publicize data availability
Reduce time-cost of data use
Encourage perc-eption of value
Achieve first end-use of data
Receive initial user feedback
Build habits of data use
Increase interest in data production
Origin
Algorithm
Consent
IDENTIFY
ACK
ESS
ANALYZE
RELEASE
DISSEMINATE
FEEDBACK
COLLECTION
ECT
INCENTIVIZE
INFLUENCE
UPTAKE
IMPACT
USE
CHANGE
REUSE
FEEDBACK
FEEDBACK
Input
Compliance
Approval
Consult with future users
Determine levels of granularity
Achieve high-quality and protected privacy
Provide machine-readable data
Data accessible online and offline
Use technology to connect to users
Re-process data for new insights
driven policies
PRODUCTION
USE
increasing value of data

Picture Credit: The Data Value Chain. Open Data Watch (2018)
Attribution 4.0 International (CC BY 4.0)

If there is any truth in the comparison of data and crude oil, then let's think in terms of *assaying data*.

That is, let's start to measure the properties of data that make it reliable, fit-for-purpose, and valuable. And then let's bind the assays to the data records as they move through the information value chains.

I envision a world with widespread crypto-graphic infostructure, so that verifiable data is available everywhere, just like stable electricity and clean drinking water. We have the tools. We IDpros know we have these tools, because we have already built them!

Steve Wilson Identiverse 2022 Post Identity Trust (0.6) HANDOUTS

The post-identity world

So let’s shift focus from the abstract to the concrete. Notice that I haven’t used the word “identity” since the start of this piece. The idea of identity is simply not helping. That might be counter-intuitive, or strike some as sterile but, pragmatically, it doesn’t matter. The digital identity industry has shown us how to design for verifiable facts and protect them cryptographically.

We can trust without identifying. We can break old habits. Instead of starting with identity, let’s ask:

What do you really need to know?

Where will you get the data?

How will you know if it’s true?

It is perfect timing for a paradigm shift. We have intelligent devices at the edge, we have mobile digital wallets that make ideal verifiable containers for data, and we have clouds full of APIs.

We can do better with digital identity; indeed we can do something *much bigger* for all of cyberspace. Let’s apply our proven tools to build infostructure that delivers data as a true utility.

If zero trust is a thing then so is zero identity.

identiverse

#identiverse