Facilitating Personal Data Transactions in a Secured Manner on a Global Scale

World Economic Forum

Rethinking Personal Data Workshop

Scott L. David

Sept. 30, 2010

OIX OPEN IDENTITY EXCHANGE

Question: What is the international law of personal data/identity?

Answer:

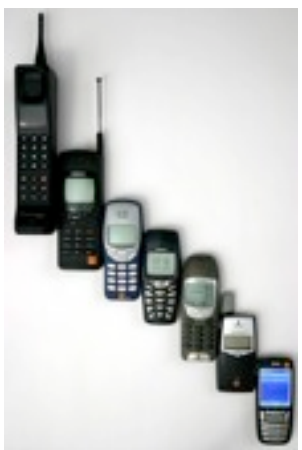
There is none. Use consensus-based rules to “fill gaps.”

OIX OPEN IDENTITY EXCHANGE

Question: What should the Rules

Answer:

That depends. What do we want "identity" systems to do?



OIX OPEN IDENTITY EXCHANGE

Question: What should all personal

Answer:

Address system participant needs.

OIX OPEN IDENTITY EXCHANGE

Question: What are examples of

Answer:

- **All participants are system "users,"** with different needs in different contexts
- **Data subjects** (people or entities described by personal data) - **"need" identity integrity**
- **Relying parties** (people or entities relying on personal data) - **"need" assurance**
- **Identity providers** (people or entities handling data) - "need" risk reduction

OIX OPEN IDENTITY EXCHANGE

Question: What "needs" are common

Answer:

All users require:

- Reliability
- Predictability
- Interoperability
- Security
- Easy user interfaces (UIs)
- Cost effectiveness
- Risk reduction
- Transparency
- Simplicity

OIX OPEN IDENTITY EXCHANGE

Question: What does this have to do

Answer: Plenty.

•**Tools and Rules address user needs** as a protective virtual "skin" of your digital identity, "wrapped around" personal data about you, wherever it is located.
•**Technology Tools guide data movement** and protect data at rest.
•**Legal Rules create duties** to cause every other identity system user to take "data actions" consistent with each other system user's needs.
•Every other system user is a personal data guardian;
•they are your digital identity's "immune system."

Question: Why don't we just rely on

Answer:

- **Human actions (or failures to act)**, not technology failures, cause 80-90% of data breaches.
- Technology tools cannot do everything alone.
- Rules (in law and contracts) guide people's discretion to align behavior with system requirements

OIX OPEN IDENTITY EXCHANGE

Question: How do you create "Rules"

Answer:

- Trust Framework = Term Sheet

  Trust Frameworks document and standardize mutual, consensus-based, contracts, TOUs and laws that establish enforceable "data action" duties among system users

Question: Is there existing guidance

Answer: Yes.

- To benefit relying parties
- **LOA** – OMB/NIST/GSA

- To benefit identity providers
- **LOP** – 37 US laws, EU, OECD

- To benefit data subjects
- **LOC** – Some FIPP

Current guidance is not perfect for every user,
but it's the "low hanging fruit of interoperability"

OIX OPEN IDENTITY EXCHANGE

Question: What about liability?

Answer:

Liability is the system "tailpipe."

Address liability, but don't obsess.

Control liability with contract provisions for

- **Duties**
- Breach
- Causation
- Damages
- ... and liability "management"

OIX OPEN IDENTITY EXCHANGE

Question: How do standardized duties

Answer:

Duties **reduce discretion** of other system users

Users handle personal data more reliably

OIX OPEN IDENTITY EXCHANGE

Question: Needs …Duties …Contracts … Liability? How does this all work?

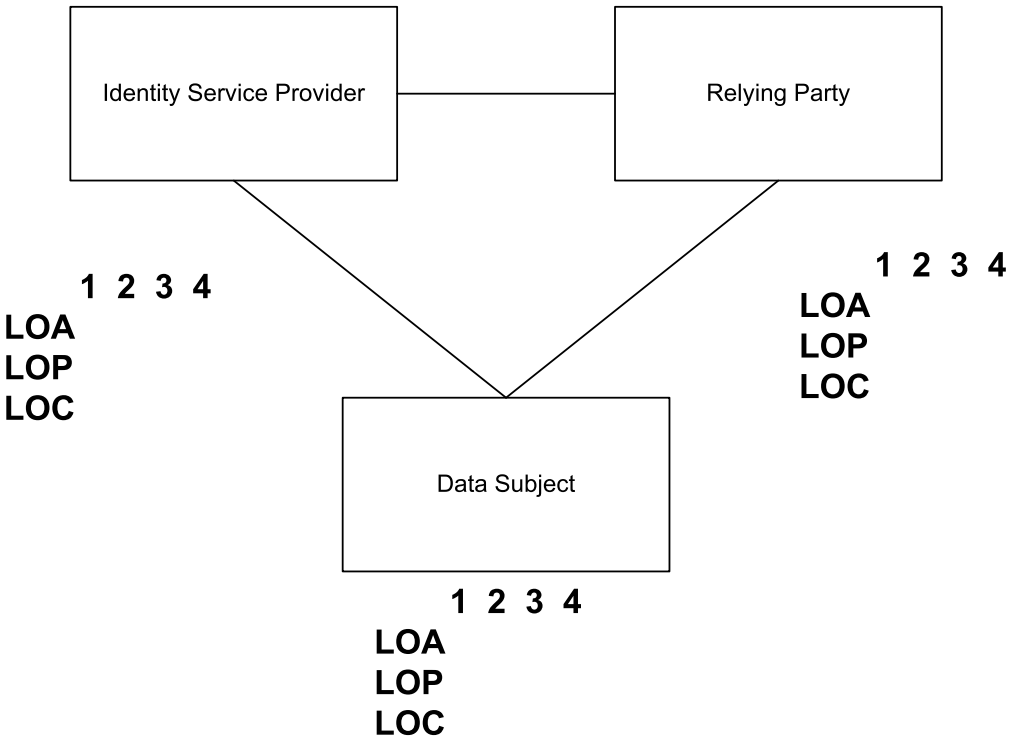
Answer:

Use the **Identity Rules Tool Kit**:

- Data Action Map
- OIX "Verb Taxonomy"
- OIX Risk Wiki
- OIX Listing Service
- ABA draft report materials

OIX OPEN IDENTITY EXCHANGE

Data Action Map – Draw data flows



OIX OPEN IDENTITY EXCHANGE

Question: Why use these tools?

Answer:

Common analytical framework for "liability"

Standardizes identity infrastructure across:

- Industries
- Jurisdictions
- Contexts and settings

Enables **common system metrics**

Connects personal data silos

OIX OPEN IDENTITY EXCHANGE

Question: What do common system

Answer:

Interoperability
Correlation
Measurement
Easy citizen access
Adoption
Valuation
Markets
Global scale infrastructure
Product innovation
System monitoring
User rights enforcement sub-systems

OIX OPEN IDENTITY EXCHANGE

Question: What else can system

Answer:

Simplify system complexity

LOA, LOP and LOC each on a 1-4 scale
can describe 64 possible data states
(4x4x4 = 64)

Metrics simplify complex personal data and system meta-data both “in motion” and “at rest”

OIX OPEN IDENTITY EXCHANGE

Simple presentation of complex

- UI Simplification Examples:

OIX OPEN IDENTITY EXCHANGE

The Near Future?

A symbol for healthcare (chart) personal data?

Red is LOP (4 as “HIPPA default”)
Blue is LOA (or 4, depending on risk of error)
Yellow is LOC (data subject control of chart is limited)

OIX OPEN IDENTITY EXCHANGE

Questions?

www.openidentityexchange.org

scott.david@klgates.com

don@openidentityexchange.org

OIX OPEN IDENTITY EXCHANGE