Trust and Inclusion

Information Architecture Roundtable
March 13-14, 2019
Noreen Whysel

What Is Trust?

Trust is relational

Throughout history, Trust has always been

- Contractual
- Relational
- Emotional
- Transactional
- Easy to revoke, hard to reinstate

Rules of Interpersonal Trust Are Complex

Digital Trust is Transactional

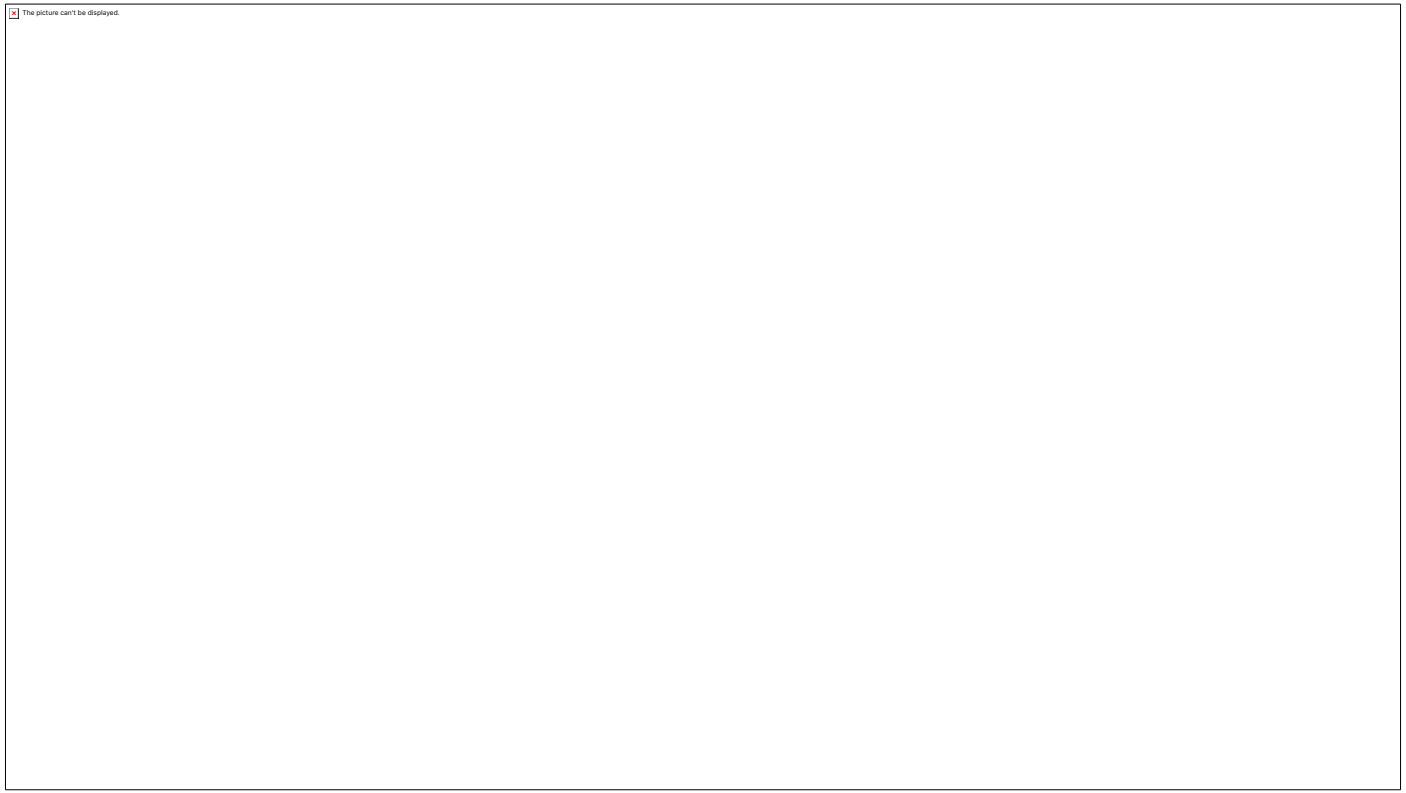
In digital systems, Trust is

- Contractual
- Transactional
- Instantaneous
- Easy to revoke and to reinstate

Rules of Digital Systems Are Less Complex

How About Inclusion?

Inclusion Is Both Among and Different



Trust and inclusion go hand in hand

- Without trust, a service provider will not provide service.
- Without trust, an individual will neither ask for nor receive needed services.
- Without services, vulnerable individuals are at risk.

What Are the Credentials Of Vulnerable Populations?

Who Are Vulnerable Individuals?

Who Are Vulnerable?

- Children
- Women
- Minorities
- LGBT+
- Immigrants/Refugees
- Homeless
- Disabled
- Mentally Ill
- Unemployed
- Incarcerated/Formerly incarcerated
- Aged

We All Have Some Experience With Vulnerability

Contexts of Vulnerability

- Registering for welfare benefits
- Online dating
- Accessing healthcare
- Applying for a passport or driver's license
- Registering to vote
- Registering for the military
- Etc.

Context may be very different if you are a minor, an immigrant or refugee or a member of another unprotected class

How Do I Know Who You Are?

Trusting Digital Entities

- Attributes
- Identifiers

All digital entities (users, service providers and relying parties) have identifiers composed of attributes

Handling of Attributes May Be Governed by Law

Example: Personally identifiable information or PII is information that, alone or in combination, can be used to trace a person's identity. PII risk is contextual.

Digital ID

A digital ID is used to authenticate individuals.

The authentication process collects data and matches it against attributes connected to the ID.

This might be a name, birthdate, Social Security Number, password, biometric data or it may require a second factor authentication external to the system.

Authentication is a result of an algorithm (rules) for matching an ID to an authenticated User.

Three components of Digital Trust

- Data Source: Where is the data from? Who else knows it?
- Coding: How is it coded? Does it recognize alternative categories or attributes?
- Device: What device is reading it?

Vulnerable Populations have Low identity assurance Often because they don't have credentials that match coded categories or attributes

Future Opportunities

Blockchain ID

“The humanitarian community exists in a bubble, so access to an existing community of experts and new technologies to help us better serve communities in crisis is an amazing opportunity,” said Nathan Cooper, Senior Adviser at Red Cross.

“We hit the realization that we can no longer do this with a spreadsheet and beneficiary ID cards. We need something more sustainable, something people can establish, create, hold, and access their identities. It brings dignity, choice and economic stimulus to the local markets where humanitarian aid is needed,” said Caroline Holt, head of global cash distribution, Red Cross.

Trustmarks and Ratings

- Regulations: FINRA, HIPPA, COPPA, GDPR
- National Institute for Standards and Technology 800.63
- Consumer Reports
- Identity Ecosystem Framework: idefregistry.org
- RDR Corporate Accountability Index: rankingdigitalrights.org
- Trustable Technology Mark (IoT): trustabletech.org

Bibliography

Identity Ecosystem Steering Group, IDESG.org

IDESG, Vulnerable Populations, https://wiki.idesg.org/wiki/index.php/Vulnerable_Populations

GSA Privacy Program, Rules and Policies Protecting PII, http://gsa.gov/reference/GSA-privacy-program/rules-and-policies-protecting-pii-privacy-act

THANKS!

@NWHYSEL

Who Authenticates the Service?

Identity Service Provider: Do you know what data they collect on you?

How do they protect you from:

- Phishing: Do you know if the entity collecting your data is who they say they are?
- Identity Theft: How easy is it to access and use your data?
- Transfer: Is your data being sold to third parties?

Is the Identity Provider Regulated? How Is Your Data Protected?