

# Can Subsidiarity Save Decentralization?

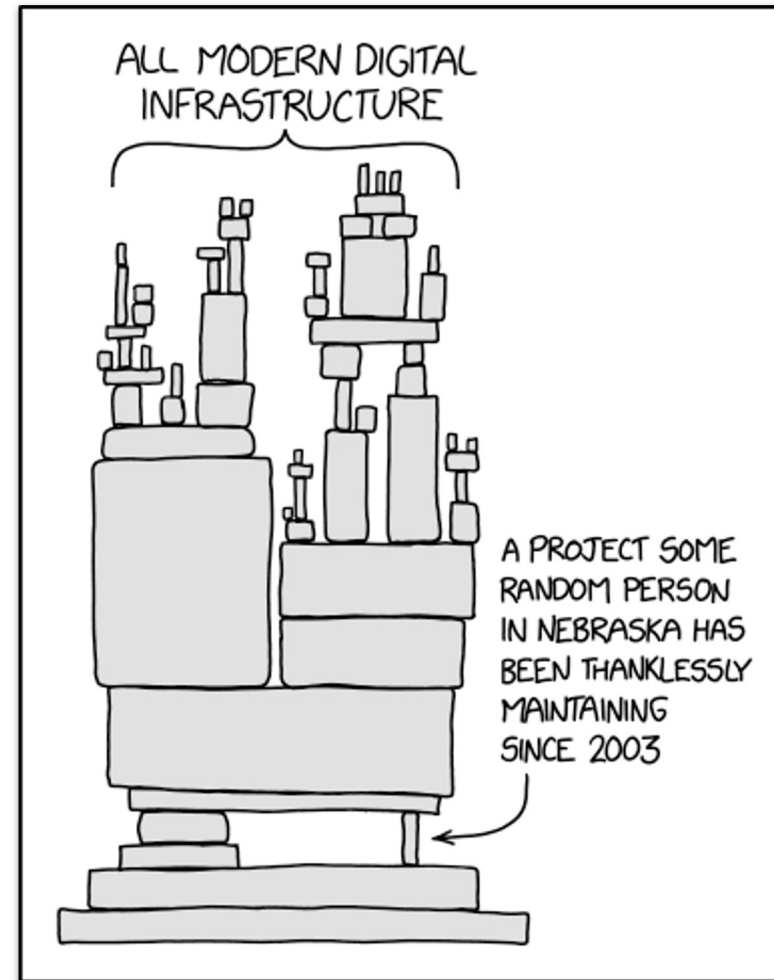


**Eve  
Maler**

CTO

ForgeRock

# Single points of failure are problematic



[xkcd](#)

# Single points of failure dependency are problematic

**“Trust is a  
confident  
relationship to  
the unknown.”**

*– Rachel Botsman*

[TED.com](https://www.ted.com)

**“Trust is shared  
vulnerability to  
consequences.”**

*– Allan Foster*

**“Trust is a  
vulnerability.”**

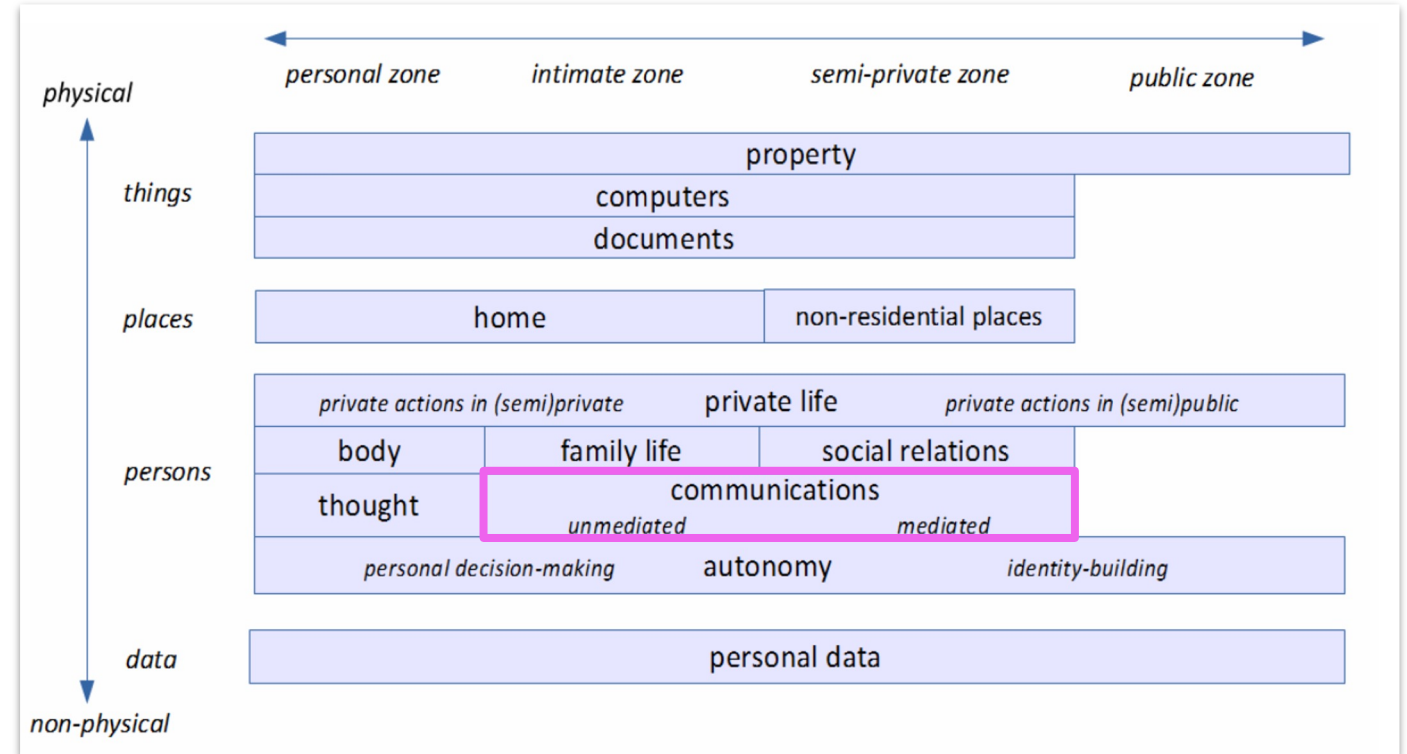
*– John Kindervag*

[T-shirt](#)

# Humans are not just another Internet endpoint

Even when they're a network "peer"

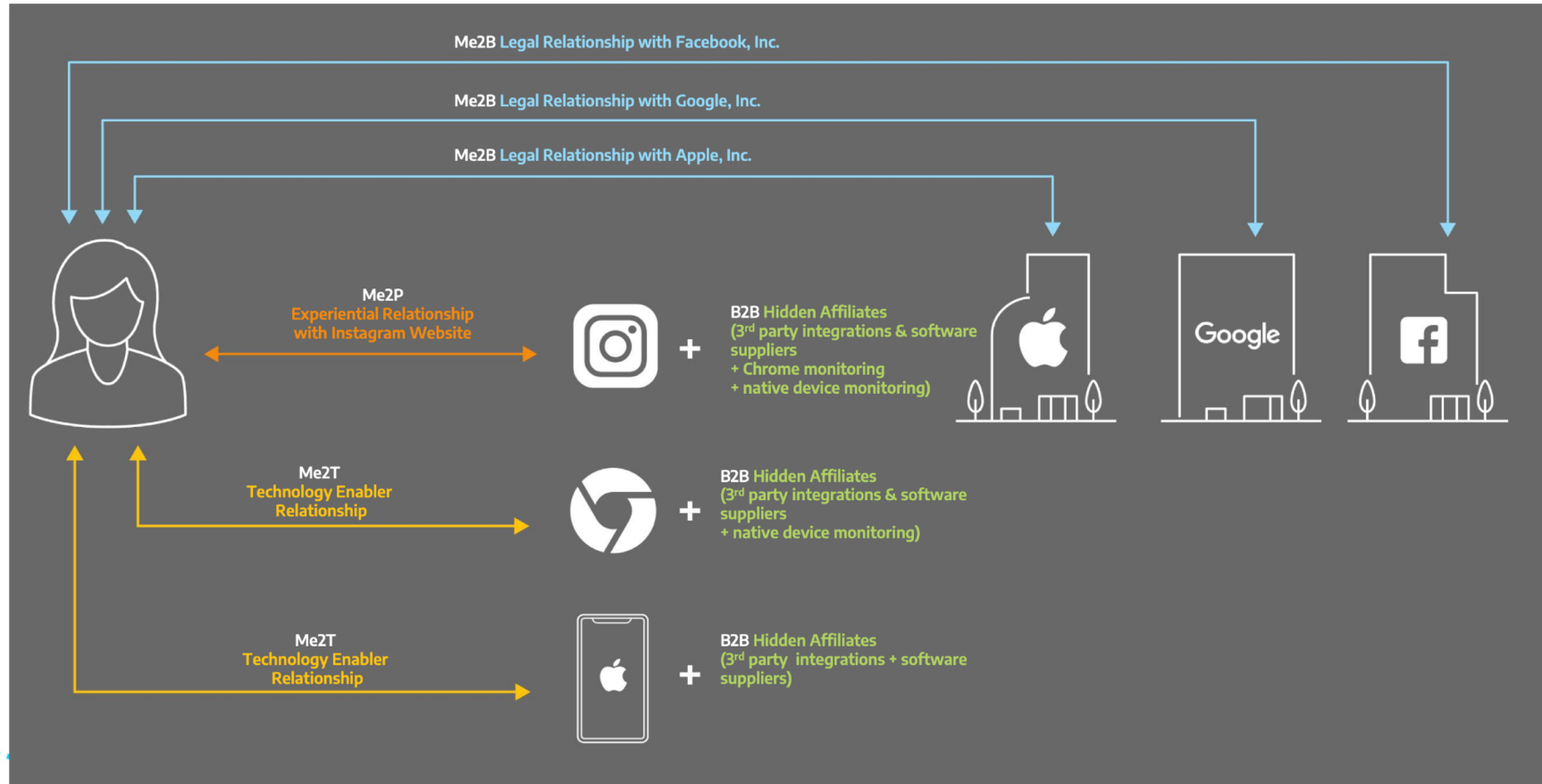
- Adhesion contracts
- Dark patterns
- Privacy as a business risk
- Exclusive design
- Human as micro-repo



[A Typology of \(the Objects of the\) Privacy](#)

# It's dependencies all the way down

Says the research



[Internet Safety Labs](#)



# Decentralization can mitigate these risks

**But has other costs**

**decentralization**

**The  
identity  
trilemma**

**privacy**

**Sybil resistance**

*...or simply*  
**reducing anonymity abuse**

**decentralization**

**The  
blockchain  
trilemma**

**scalability**

[Molly White blog](#)

**security**



# Some centralization risk mitigation strategies

*...or simply decentralization techniques*

## Federation

*“new instances of a function are easy to create and can maintain interoperability and connectivity with other instances”*

- Examples: federated identity protocols, decentralized identity protocols

## Multi-Stakeholder Governance

Delegate beneficial centralization functions to “an institution that includes representatives of ... stakeholders ... in an attempt to make well-reasoned, legitimate, and authoritative decisions”

- Example: trust frameworks

## Distributed Consensus

*“distributing functions to members of a sometimes large pool of protocol participants ... typically using cryptographic techniques”*

- Proof of work or stake to mitigate Sybil attacks

[Internet Centralization: What Can Standards Do?](#)



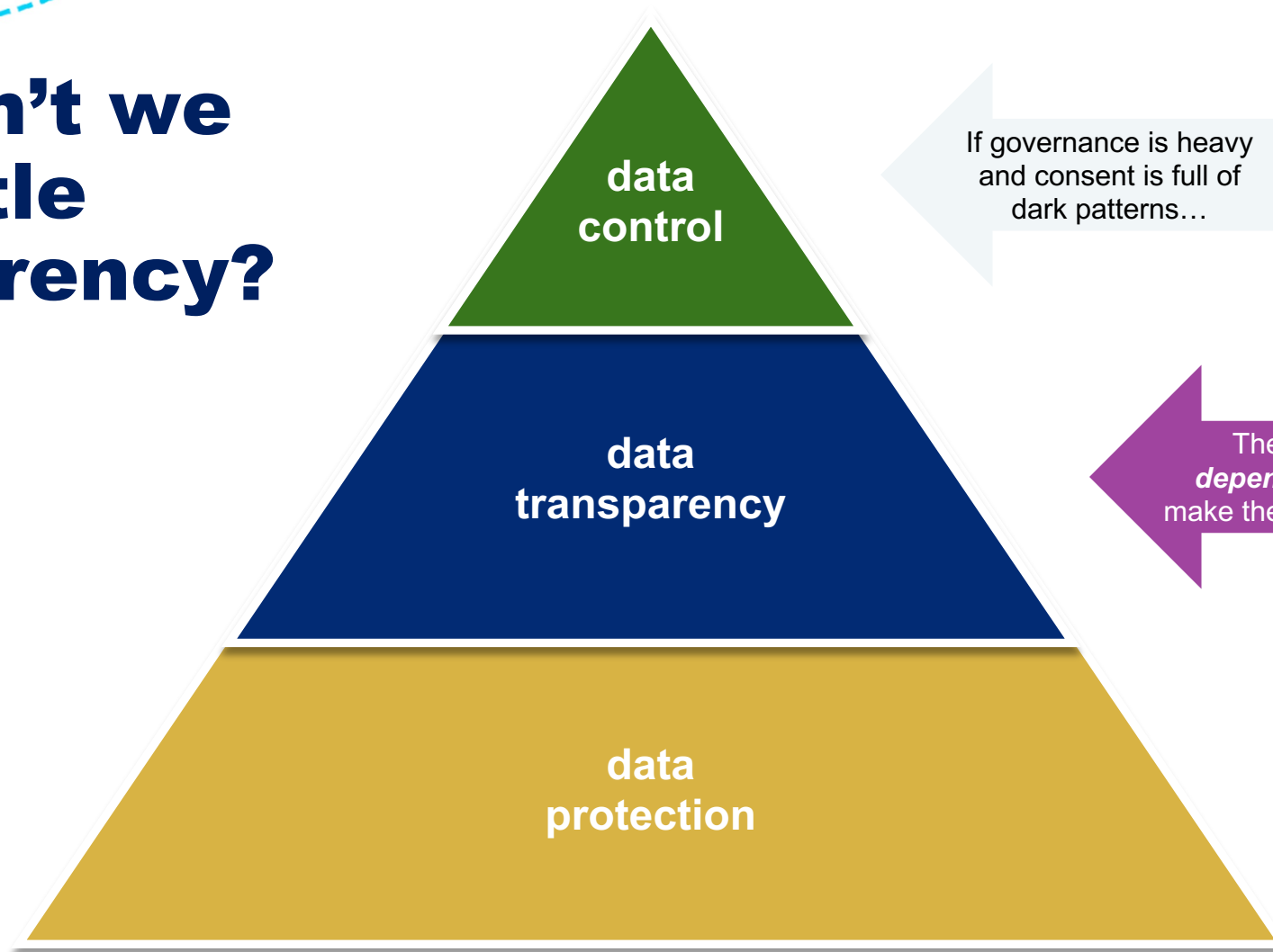
Even where decentralization is a great choice and well applied...

## Centralization risk is relentless

Mark Nottingham's research discusses:

- A **proprietary** role for one party
- A **beneficial** single source of truth
- **Concentration** in practice
- **Inheritance** from lower layers
- A **platform** allowing layered consolidation

# Why don't we try a little transparency?



If governance is heavy  
and consent is full of  
dark patterns...

Then *expose*  
*dependencies* and  
make them *measurable*

If cryptographic  
techniques don't  
guarantee success...

# Software Bills of Materials are promising

For encouraging useful transparency around (literal) software dependencies

“An SBOM is a formal, machine-readable inventory of software components and dependencies, information about those components, and their hierarchical relationships. These inventories should be comprehensive – or should explicitly state where they could not be. SBOMs may include open source or proprietary software and can be widely available or access-restricted.”

[NTIA, U.S. Department of Commerce](#)



# We're seeing concrete successes with SBOMs

- Its standard format is **generative**
- **Machine readability** aids in second-order transparency
  - Analytics
  - Automation
  - Research

```
DataLicense: CC0-1.0
DocumentNamespace: http://www.spdx.org/spdxdocs/PI
Vision_2017_.exe-3.2.0.11-63d815a9-1aae-50a5-bb33-1399493e0b09
DocumentName: PI Vision_2017_.exe-3.2.0.11
SPDXID: SPDXRef-DOCUMENT
Creator: Organization: aDolus Technology Inc.
Created: 2021-04-07T17:21:27Z
DocumentComment: <text>Please contact aDolus Technology Inc. to include vulnerability,
malware, reputation, or obsolescence analysis with this SBOM</text>
Relationship: SPDXRef-DOCUMENT DESCRIBES SPDXRef-OSIsoft-Inc.-PI Vision-2017-.exe-3.2.0.11

# Package
PackageName: PI Vision_2017_
SPDXID: SPDXRef-OSIsoft-Inc.-PI Vision-2017-.exe-3.2.0.11
PackageVersion: 3.2.0.11
PackageFileName: PI Vision_2017_.exe
PackageSupplier: Organization: OSIsoft, Inc.
PackageDownloadLocation: NOASSERTION
FilesAnalyzed: true
PackageVerificationCode: cf4d02ad37f33d66d4644437141eaf1a38cf0228
PackageChecksum: MD5: f1678e0565b8c0c942f4adecfa0c73e0
PackageChecksum: SHA1: cf4d02ad37f33d66d4644437141eaf1a38cf0228
PackageChecksum: SHA256: 708bce79acfc47917419b03c987725acd191b7c4d8f33e0c7f2362ad15a80118
PackageCopyrightText: <text>Copyright © OSIsoft, LLC. 2011-2017</text>
PackageSummary: <text>PI Vision 2017</text>
Relationship: SPDXRef-OSIsoft-Inc.-PI Vision-2017-.exe-3.2.0.11 DESCRIBED_BY SPDXRef-
DOCUMENT
Relationship: SPDXRef-OSIsoft-Inc.-PI Vision-2017-.exe-3.2.0.11 CONTAINS SPDXRef-
PIVision-3.2.0.11-RunCommand.cmd
Relationship: SPDXRef-OSIsoft-Inc.-PI Vision-2017-.exe-3.2.0.11 CONTAINS SPDXRef-
PIVision-3.2.0.11-RunSetup.cmd
Relationship: SPDXRef-OSIsoft-Inc.-PI Vision-2017-.exe-3.2.0.11 CONTAINS SPDXRef-
PIVision-3.2.0.11-SetupDialogs.xml
Relationship: SPDXRef-OSIsoft-Inc.-PI Vi
```

Timestamp

Component Name

Component Version

Supplier Name

Other Unique Identifiers

[Adolus blog](#)

# Subsidiarity is ***fine-grained*** dependency

Subsidiarity is “a principle in social organization holding that functions which are performed effectively by **subordinate or local organizations** belong more properly to them than to a **dominant central organization**”

[Merriam-Webster](#) – h/t Robert Lopez

## What if we had...

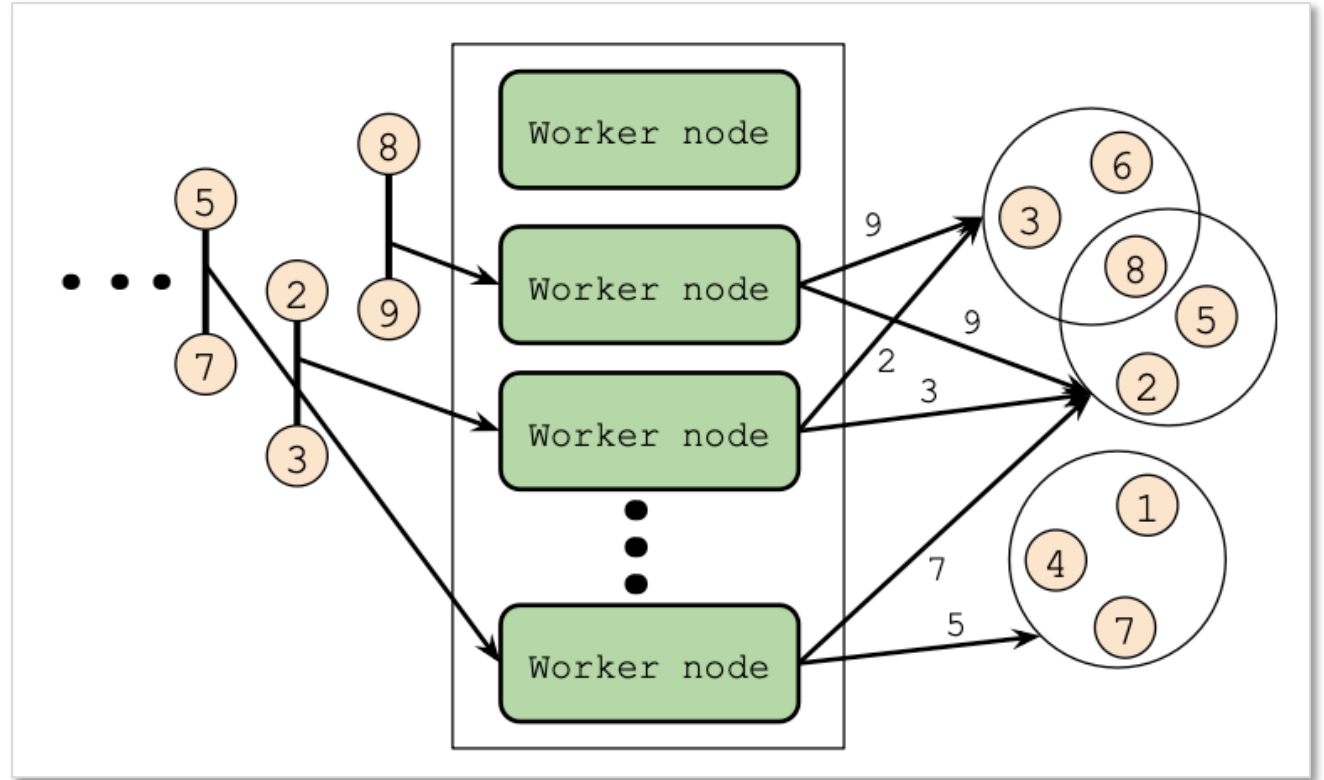
### ***Subsidiarity Bills of Materials***

Formal inventories of **third-party relationships** and **dependencies** that allow **independent** analysis and judgment of **alignment degree** in mutual business interests

# But can “alignment degree” be measured?

Why yes, yes it can

- Community detection algorithms do this for a living
- The right **dependency metadata** could point up risks
- Declaring it could **foster trust**



[CoDiS: Community Detection via Distributed Seed-Set Expansion on Graph Stream](#) | [DiCeS: Detecting Communities in Network Streams Over the Cloud](#)

# What to do if we like this idea?

Aside from figuring out what we call it – uh, subBOMs?

- Brainstorm **input data** and **desired insights**
- Assess how much of this data is **available**
  - Play around with **third-party** declarations
  - Could organizations like **GLEIF** contribute?
  - Could existing **trust frameworks** contribute need-to-know fields?
- **Test** if insights are sufficiently revealing
- **Popularize** (standardize?) a machine-readable format
  - For data that must be first-party sourced, map **ecosystem incentives** to use it



**Comments? Questions?**

**Thank You**



[eve.maler@forgerock.com](mailto:eve.maler@forgerock.com)