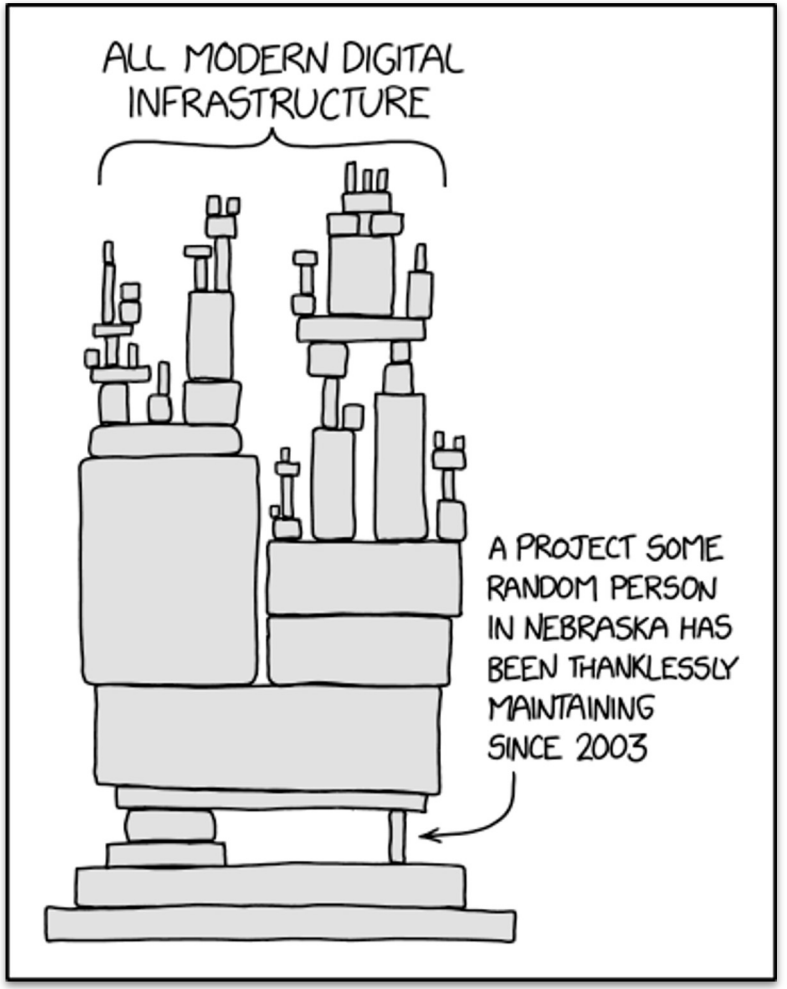
Can Subsidiarity Save Decentralization?

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

"Trust is **shared vulnerability** to **consequences**."

– Allan Foster

"Trust **is** a **vulnerability**."

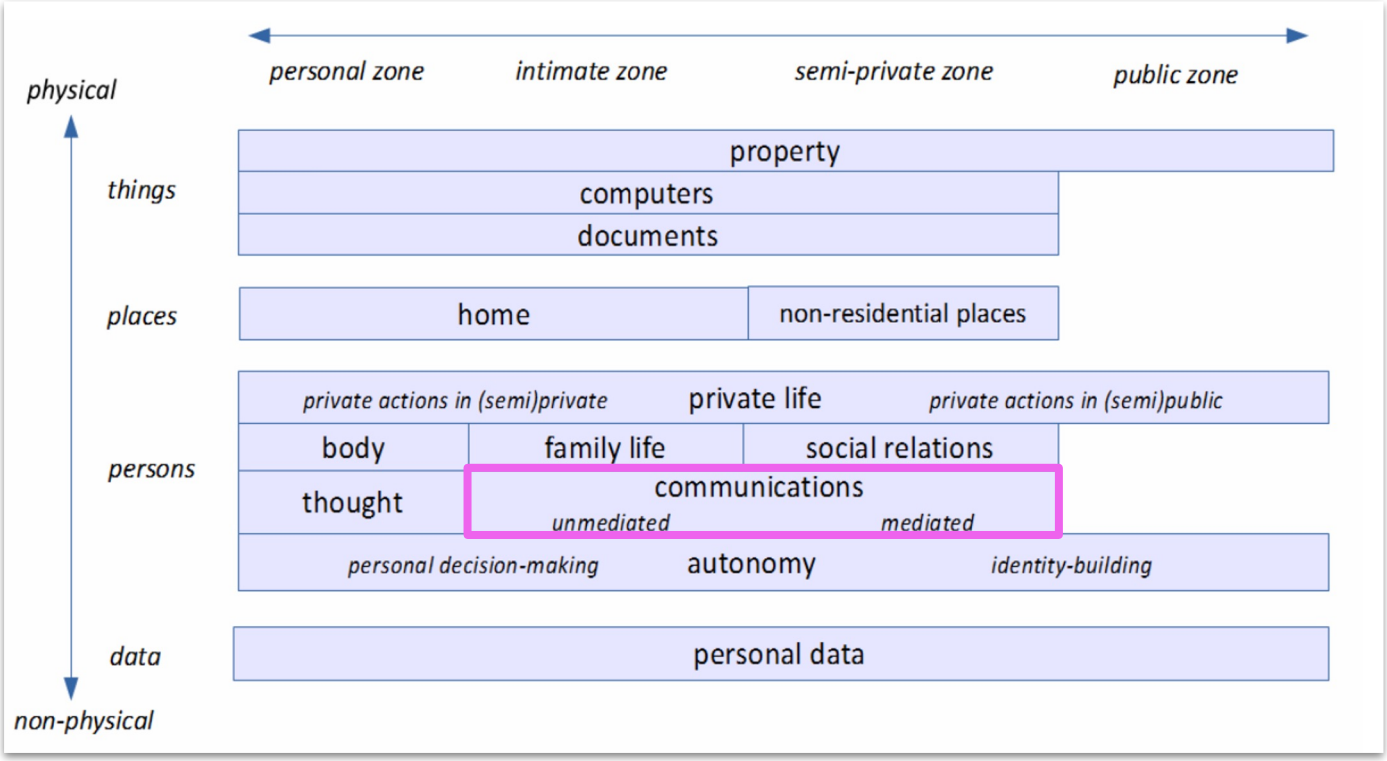
– John Kindervag

T-shirt

Humans are not just another Internet endpoint

Even when they're a network "peer"

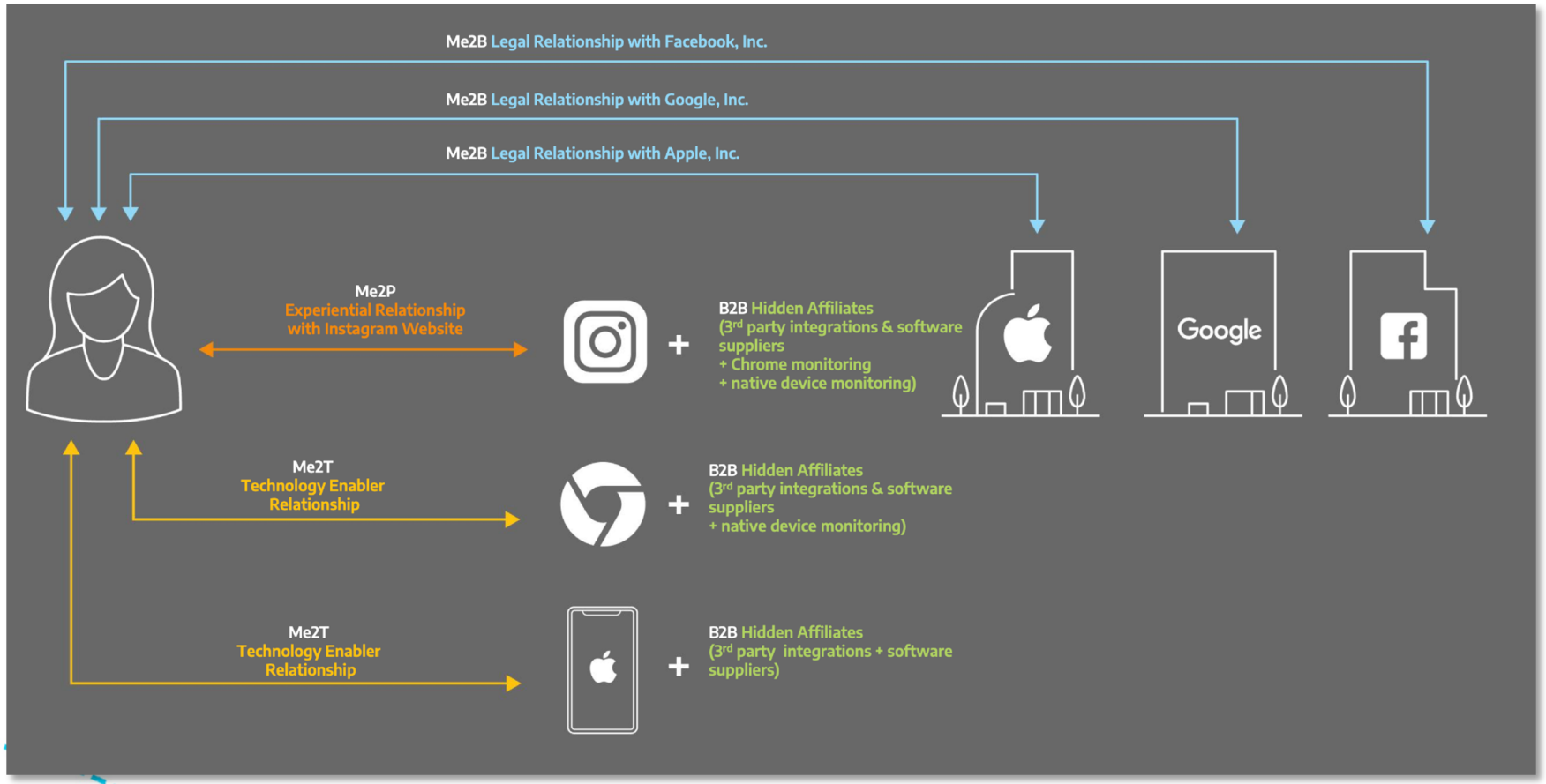
- Adhesion contracts
- Dark patterns
- Privacy as a business risk
- Exclusive design
- Human as micro-repo



A Typology of (the Objects of the Right to) Privacy

It’s dependencies all the way down

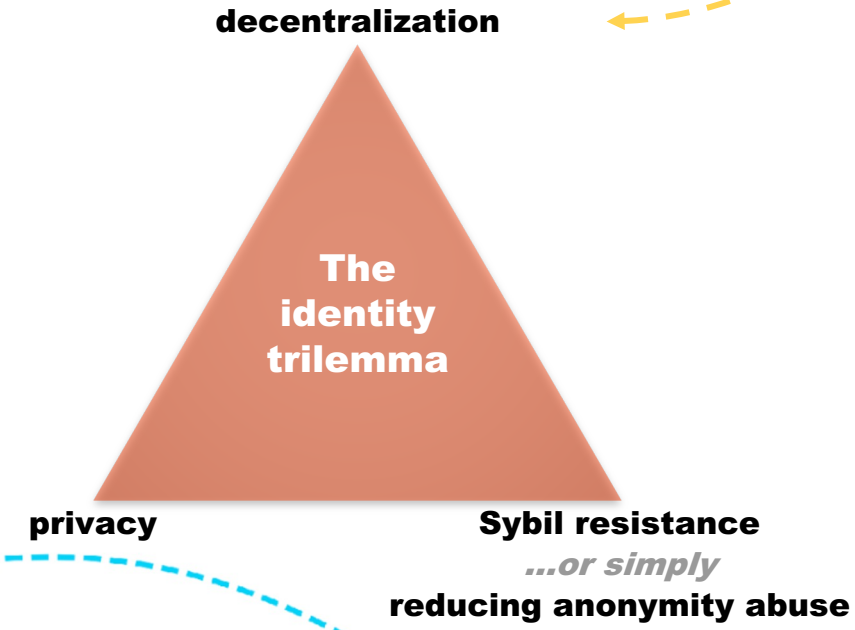
Says the research



Internet Safety Labs

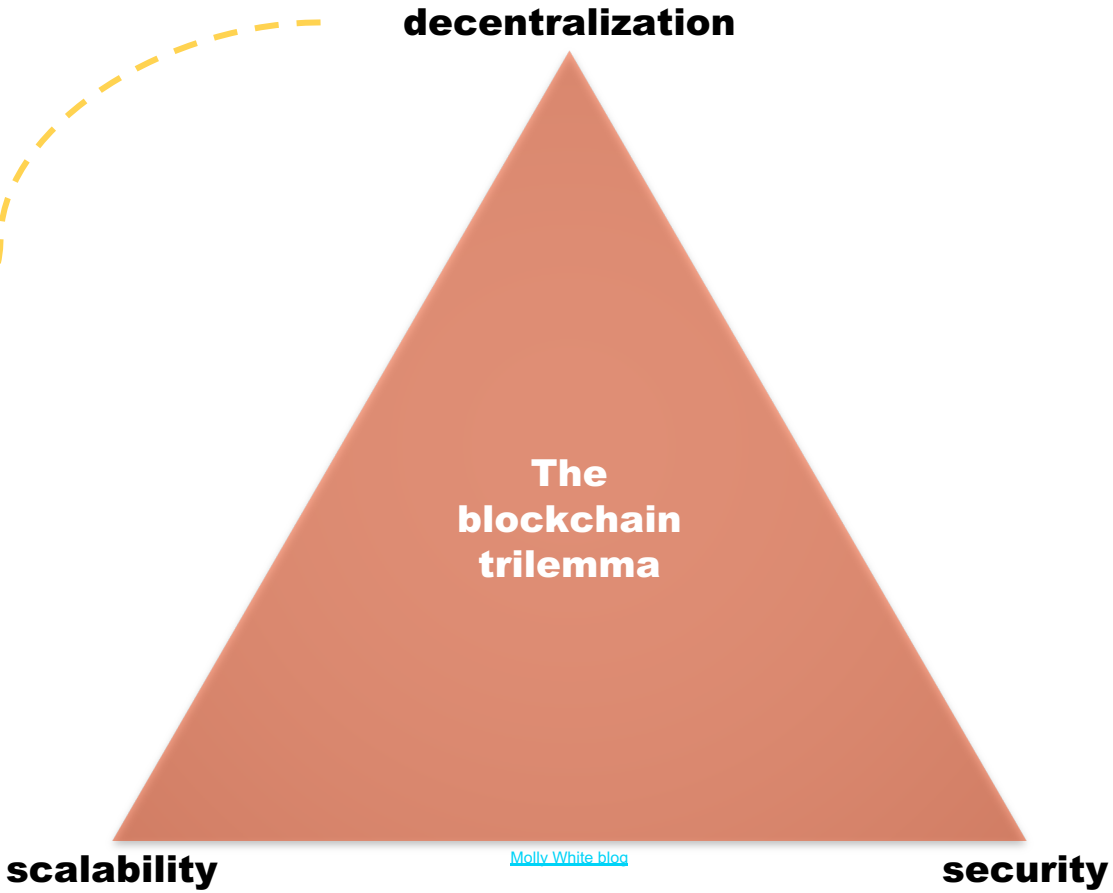
Decentralization can mitigate these risks

But has other costs



...or simply

reducing anonymity abuse



Some centralization risk mitigation strategies

***...or simply* decentralization techniques**

Federation	Multi-Stakeholder Governance	Distributed Consensus
"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	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	*"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?

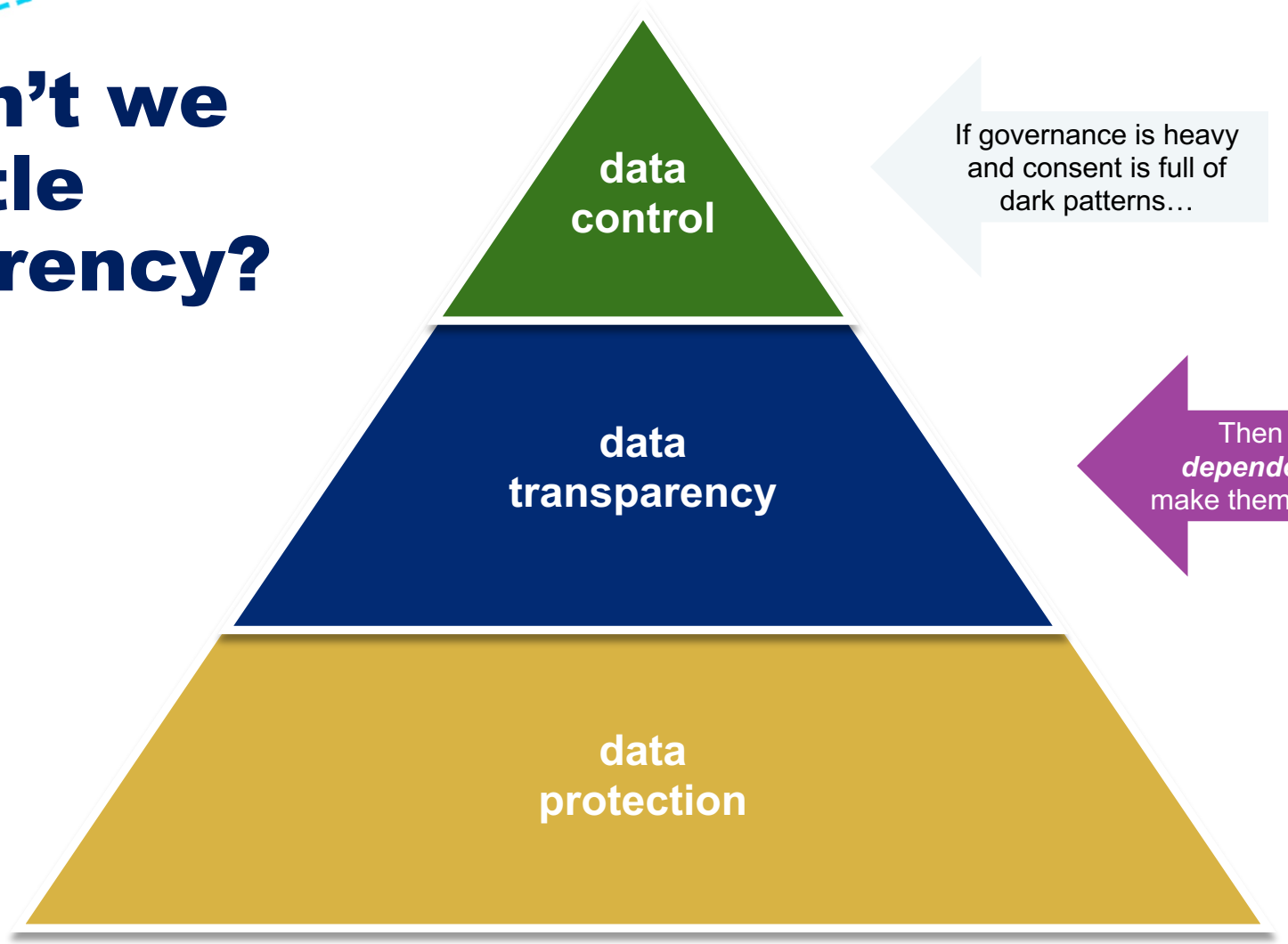
Even where decentralization is a great choice and well applied...

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?



Software Bills of Materials are promising

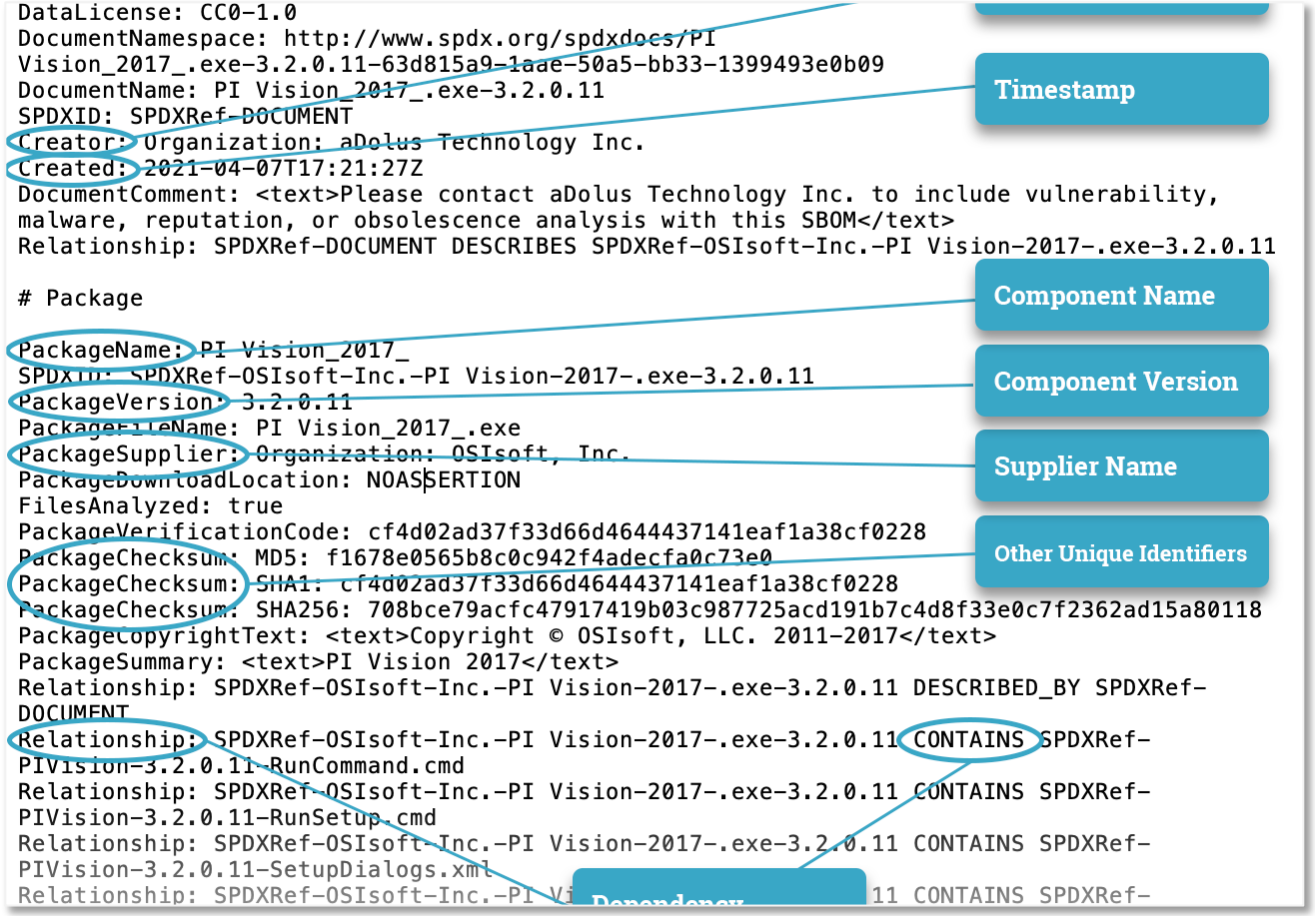
For encouraging useful transparency around (literal) software dependencies

"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



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 Lapes

What if we had…

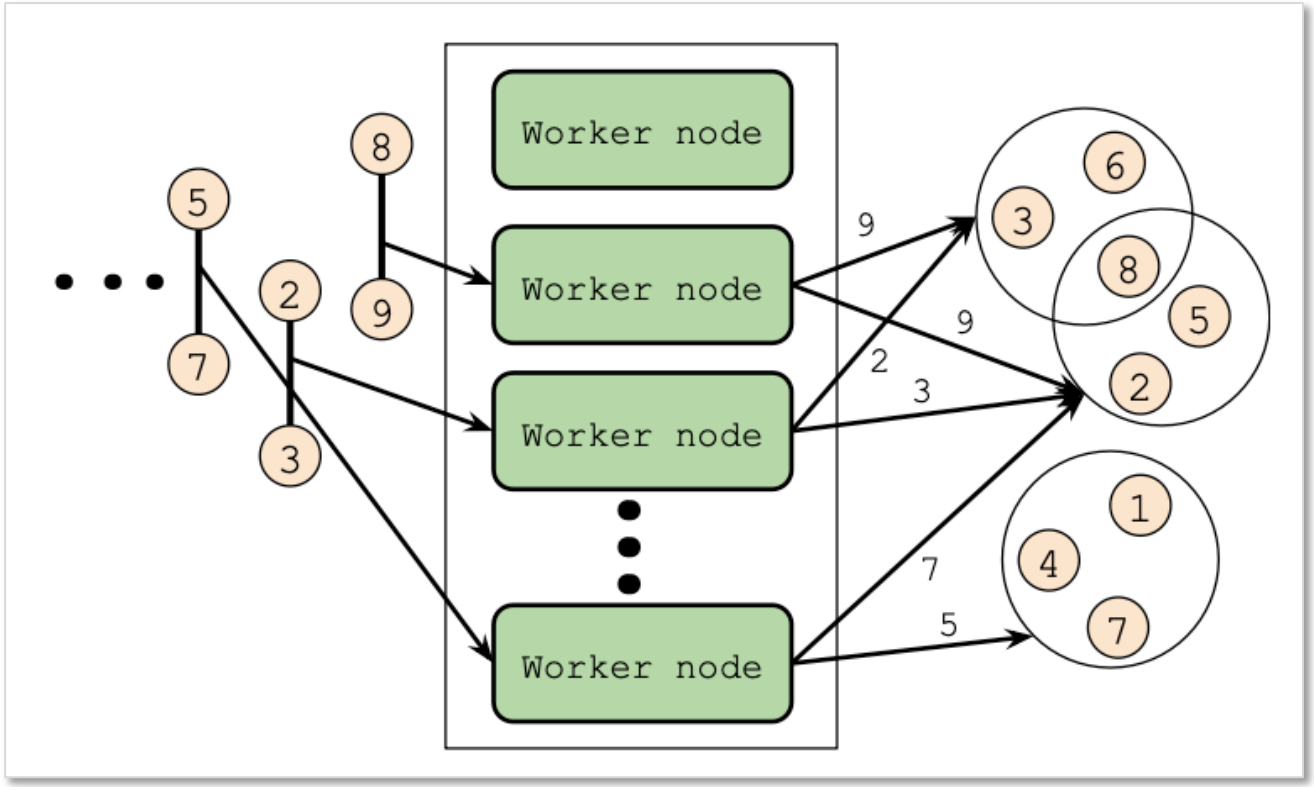
***Subsidiarity* Bills of Materials**

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