Redefining Access Control: A Human-Centric Perspective on Identification, Surveillance, and Economic Value Chain

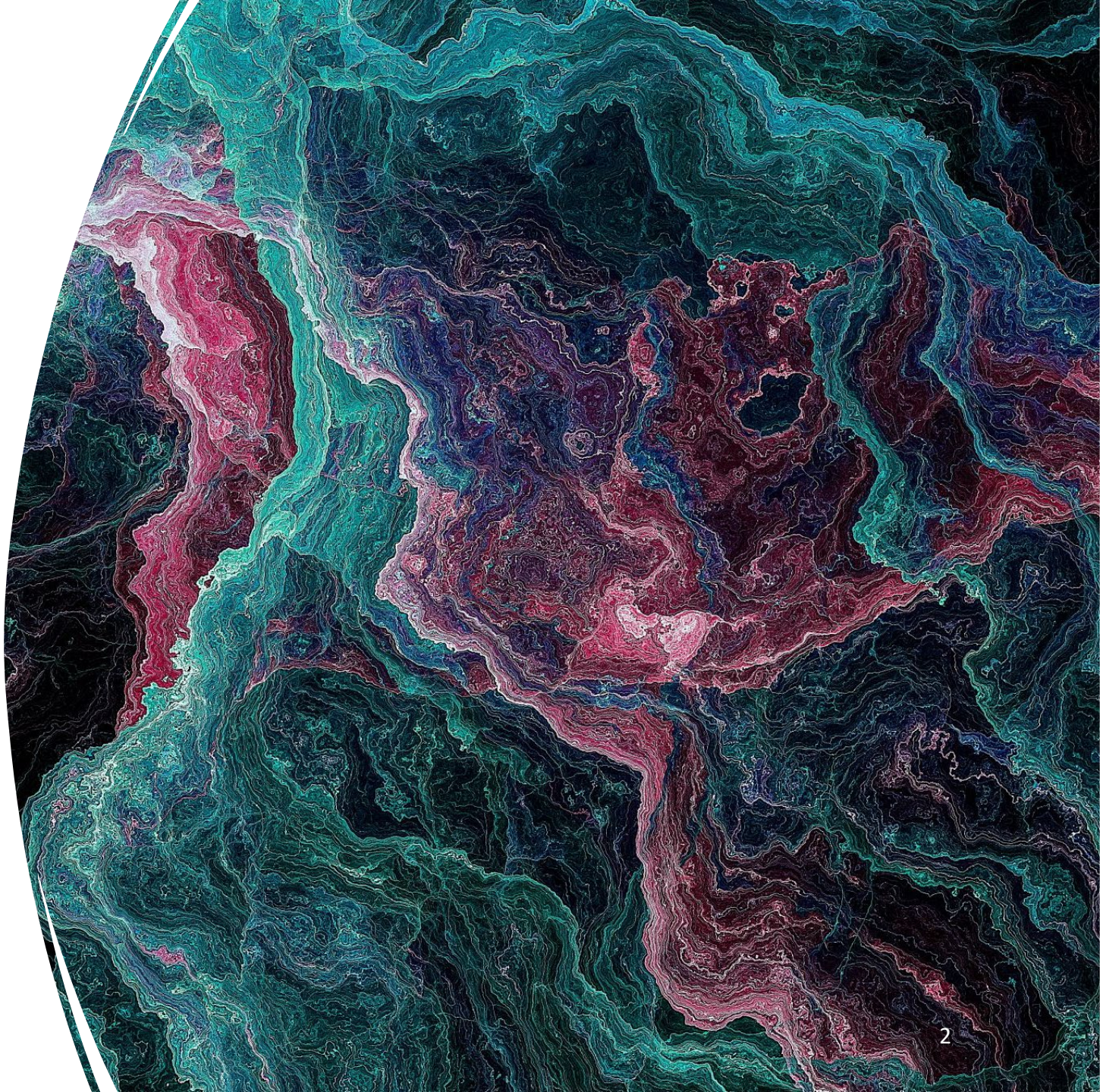
Cyber Security for Next Generation Connectivity Systems

Sal D'Agostino

Rajesh Murthy

Guiding Principles

- **Human Centricity**
- **Decentralization**
- **Distribution**
- **Heterogeneity**
- **Self Healing**




ECONOMIC
REGULATORY
LEGISLATIVE
BEHAVIORS
INFERENCES
IDENTITIES
TRANSACTIONS
TECHNICAL
LEGAL
CONFIDENTIALITY & INTEGRITY
ACCESS & OBSERVABILITY
EXPECTATIONS OF PRIVACY
SOCIETAL & CULTURAL
INDIVIDUAL
INFLUENCES ON DIGITAL PRIVACY
digitalprivacy.ieee.org
© IEEE 2023. All rights reserved.

Technology unnecessarily presently circumscribes and grossly limits digital privacy, transparency, and as a result human expectations, and digital identity expression and security. - personal observation…

Digital Privacy is Key to Next Generation Cyber Security

Human to technology governance (human trust and control)

Requires an inversion of the present situation

Security/surveillance technology -> human abuse

Human uses -> security/surveillance technology utility

Identification as the means of access control

- **Identifier**
  - ***Centrally*** issued, inherently a risk, (seldom **Authoritative**, e.g., I-9 number)
- **Authentication**
  - Requires exchange of keys/secrets and key management
- **Authorization**
  - Permissions in a system, ***controlled and operated by a 3rd party*** (authorization and resource servers/services)
  - Policy Information Point (Rules) ***not under personal control***

Notice and Consent Receipts

Oldest known form of writing was a business receipt.

Kantara Initiative - Consent Receipt

- **2012** Open Notice
- **2018** Consent Receipt v1.1
- **2020** ISO/IEC 29184 Online privacy notices and consent
- **2023** ISO/IEC 27560 Consent record information structure
- **2023** ANCR WG
  - Transparency Performance Scheme and Indicators
  - Notice/Receipt Record and PII Controller Notice Credential
  - Transparency Code of Conduct (Convention 108+)
  - AuthC (Authorization from Consent), v2 ANCR Credential Set

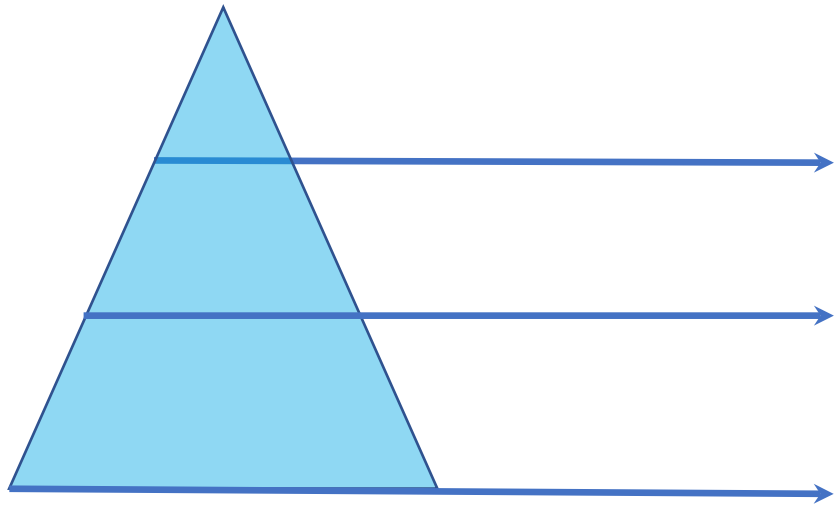
Transparency Performance

- **Timing of Notice (of Risk by Controller)**
  - Before, At the time of, After (identification/surveillance is taking place)
- **Content of Notice**
  - Controller and ***legally required information*** (Company, Owners, Security/Privacy Contact/Policy Information, Risk Assessment)
- **Usability of Notice**
  - Access to and usability of the Content of Notice
- **Security Evidence (to support Notice)**
  - Are security controls relevant to the Content of Notice and Risk Assessment

Controller Credential

Made by a human (Person, Data Subject, PII Principal) of the Controller (3rd Party/Org, Data Controller, PII Controller)	Initially a receipt specific to the controller type – 2FN	Then used to make a record of the relationship with the controller
• Created independently of the controller using digital transparency	• Surveillance notice receipt – Notice of Risk • Proof of notice	• Captures state (RoPA T) • Person (their digital agent) creates access tokens and maintains state • Personal access log

3 Vectors of Contextual Data Governance



Who Controls the Data Sources?

Is Data Protection Required ?

Is it Co-Regulated ?

Levels of Assurance

Level 0. **Same level of assurance as a privacy policy**

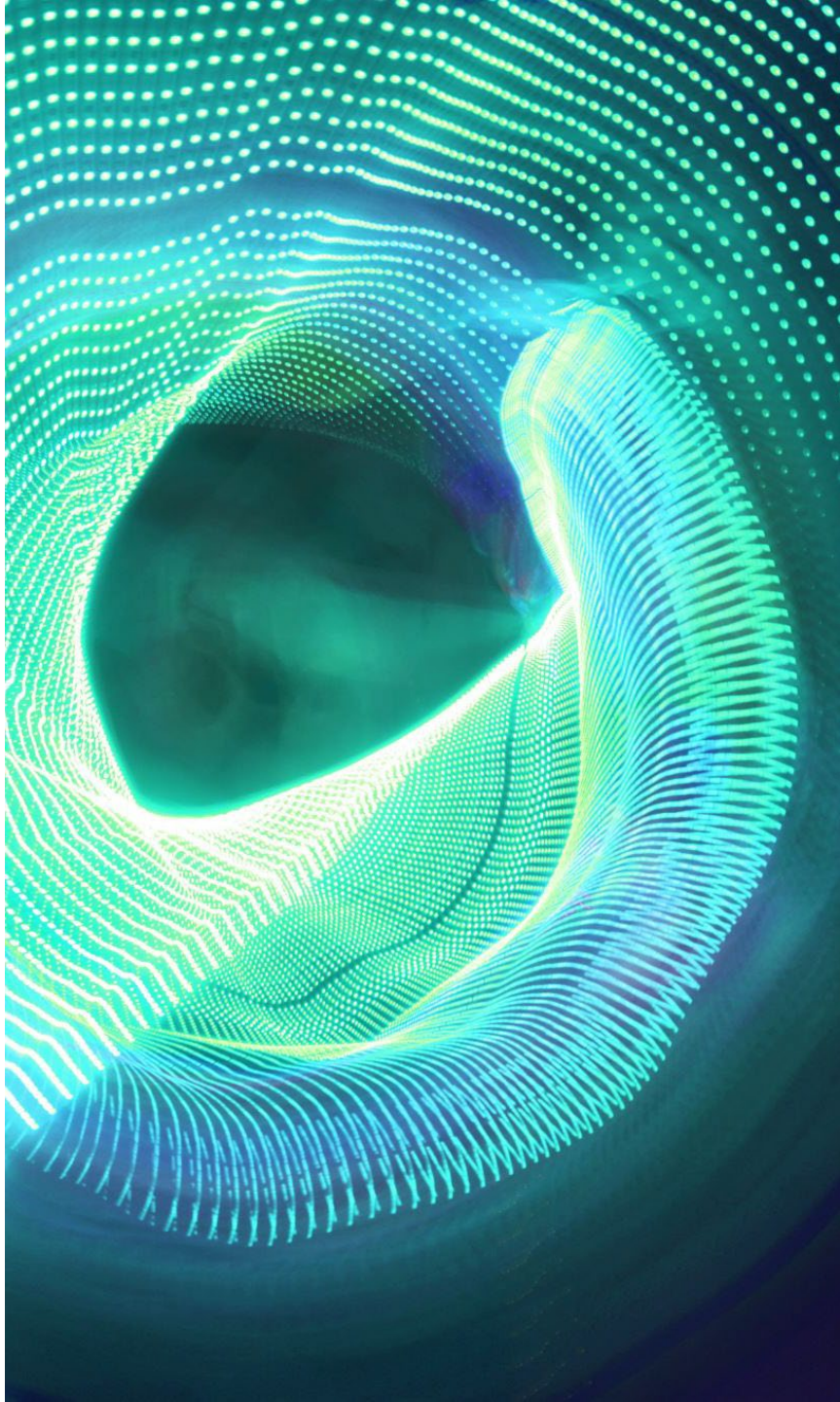
Level 1. **Registered in a Directory**

Level 2. **Data Governance – Certified Operator**

Level 3. **Data Governance – Regulated Operator Registrar**

Consented Surveillance

- Human Concentric
- Recognize the difference between access and enforcement
- Recognize that access control as security countermeasure is surveillance and has inherent identification risks.
- Recognize the difference between surveillance for people, not of people.
    - Purpose and justification drive the function of technology



AuthC Flow

Notice is captured in a Receipt

This is used to create a 2 Factor Notice (2FN) w/ optional Cyber Notary

Notice of Risk

Proof of Notice

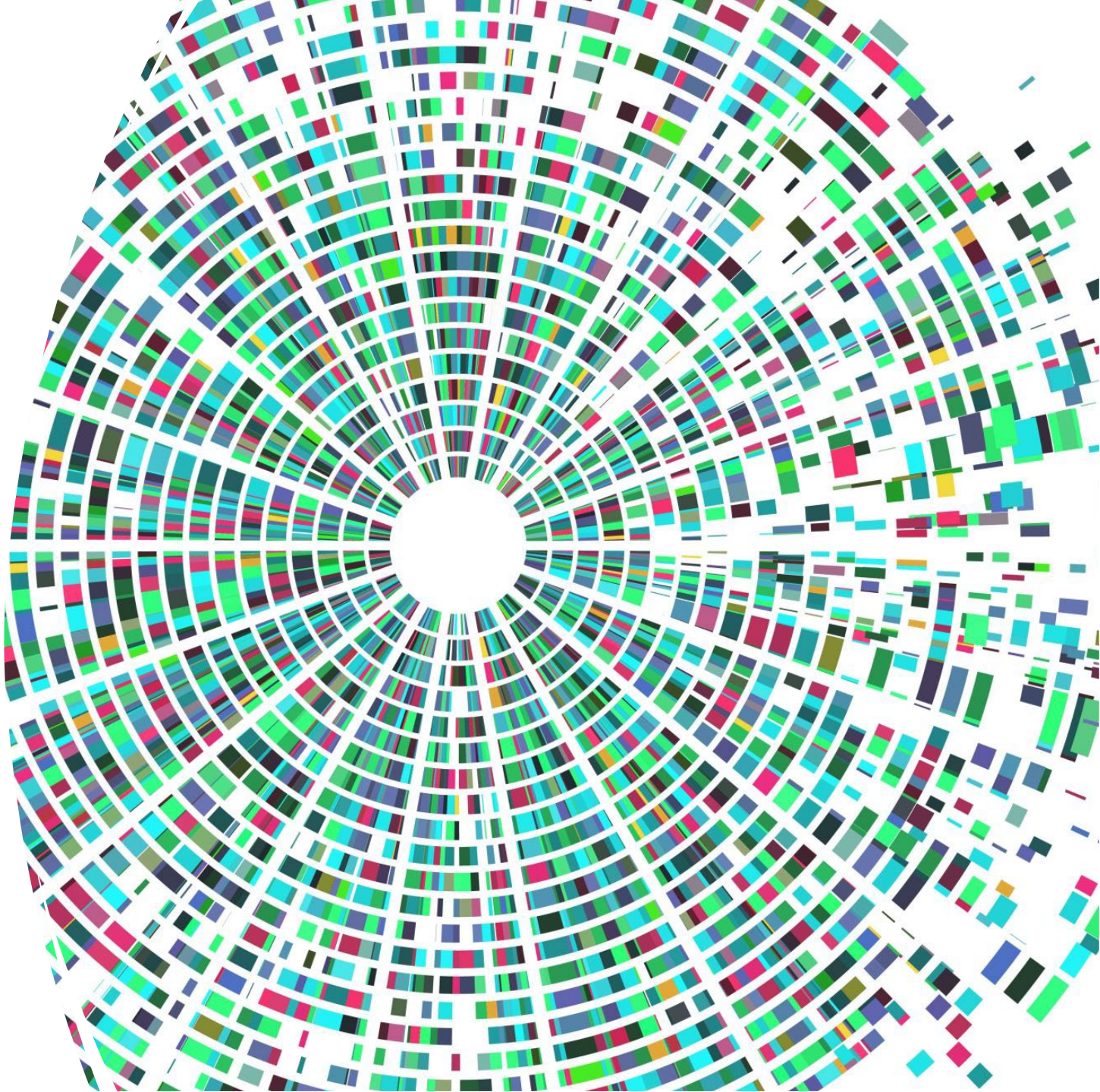
The is used to create a Record and Relationship that can have a Digital Twin

A Consent Receipt is generated and added to the Record (RoPA) to Govern processing (Access)

Does not require identification of the Person/PII Principal/Data Subject

Economic value chain

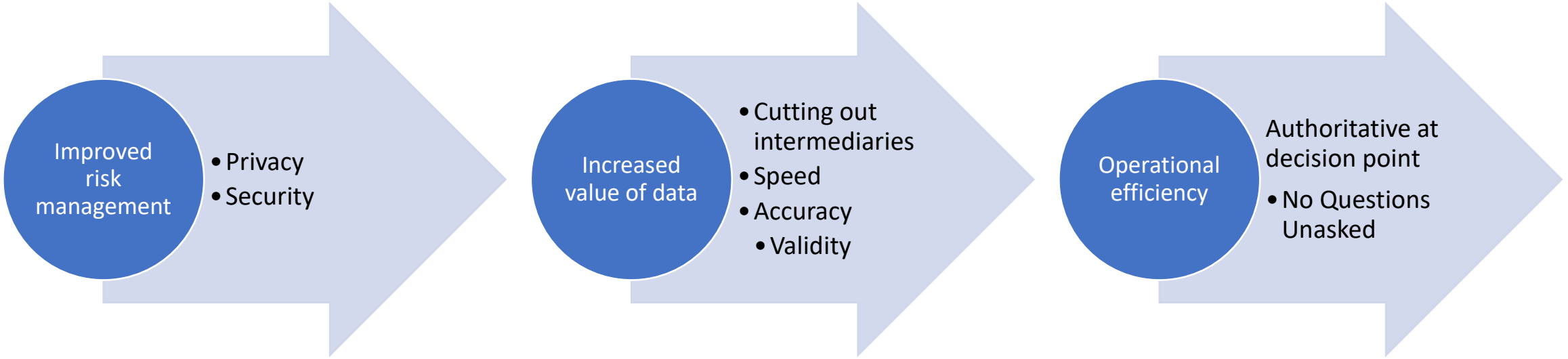
- **Creating an access control mechanism where authority is at the decision (access/transaction) point (e.g., with digital twin notarized receipts) may have orders of magnitude social, technical, and economic impact.**



Benefits of Ownership

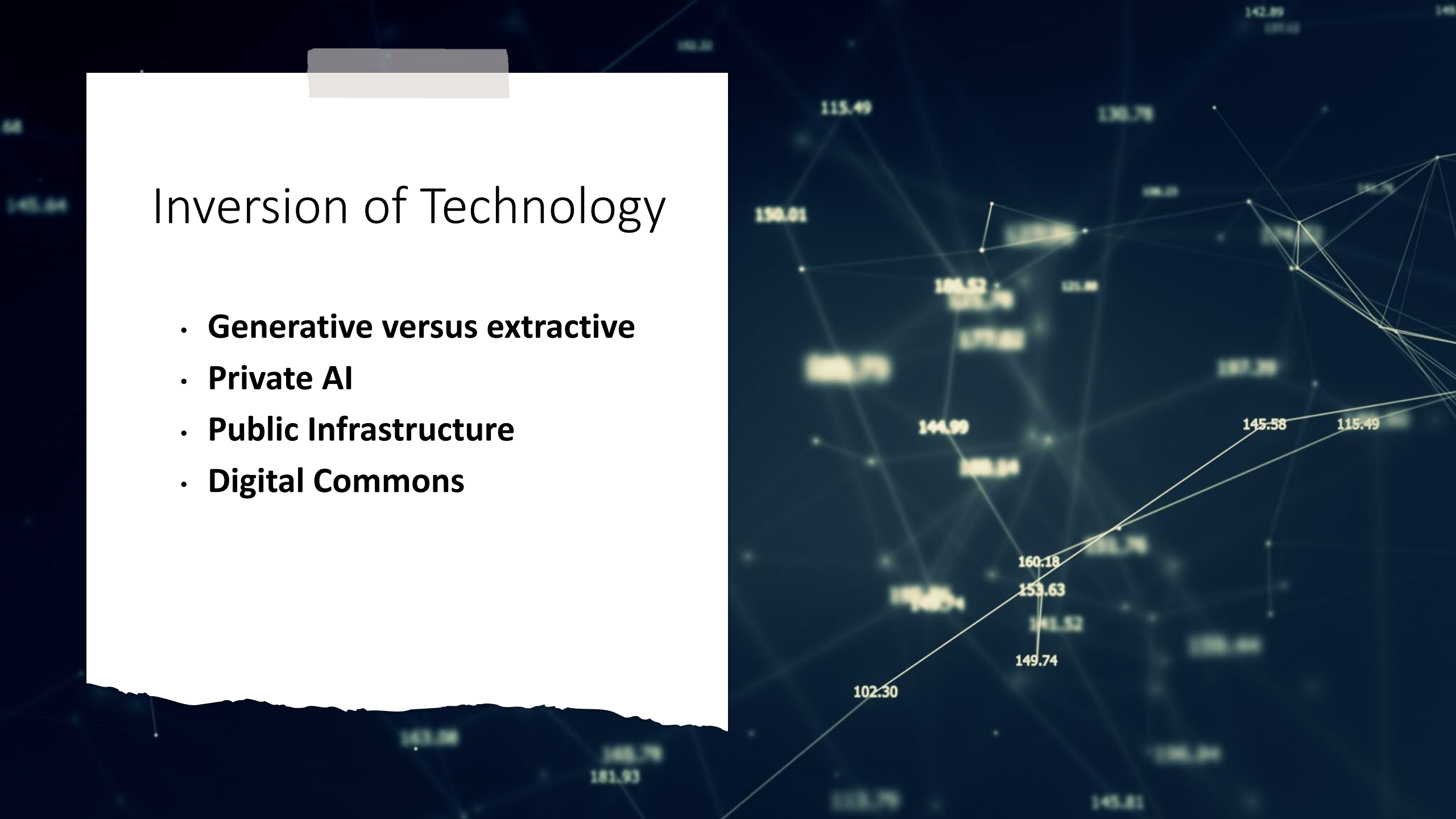
- **Personal Data Control**
- **Data Protection**
- **Co-Governance**

Benefits of Ownership and Control



Inversion of Technology

- **Generative versus extractive**
- **Private AI**
- **Public Infrastructure**
- **Digital Commons**



Thanks

IDmachines

IEEE SA STANDARDS ASSOCIATION

IEEE