iapp

Invisible risk:

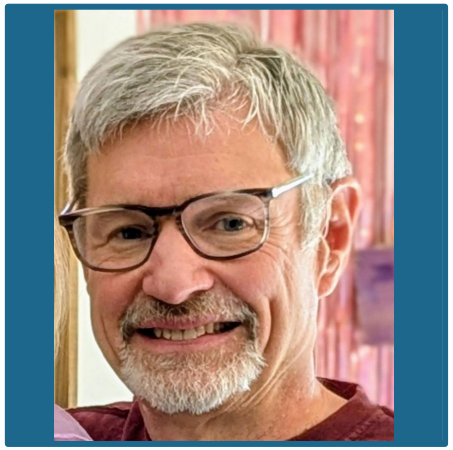
Algorithms, Implications and the New Scope of Personal Data

Tuesday, 11 November
08:00–09:00 PDT
11:00–12:00 EDT
17:00–18:00 CEST

Welcome and Introductions

Panelists

Emmi Bane
Principal – Data Ethics and Emerging Technologies
HP



Carl Mathis
Principal Privacy Architect
HP

Agenda

- Personal Data 5
- Implicative Data 10
- Risks and Governance 21
- Privacy Context 23
- Operationalization 24
- Areas of the Future 31
- Conclusion 33

Introduction: La Soupe

Image credit Pablo Picasso via the Art Gallery of Ontario

Why Personal Data is not Enough

- Lack of full visibility into the entire data ecosystem
- Non-identifying data can yield personal insights
- Privacy Safeguard Gaps – Process and Technology
- Focus on single data elements ignoring combinatorial effects

Personal Data

- Under GDPR, means “any information relating to an identified or identifiable natural person”

- Results in artificial definitions of personal data: direct, indirect, and quasi-identifiers. These are based on the following,

    - “who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”

    - These artificial categories do not completely cover the “ANY” in the definition.

- Places focus on individual data elements ignoring combining data sets and context of the data.

→ Refers to “ANY” information that implies personal attributes or behaviors without explicit or even indirect identification, but which is linkable or inferred,

→ Suggests non-personal traits or actions have the potential to be related to an identified or identifiable a natural person

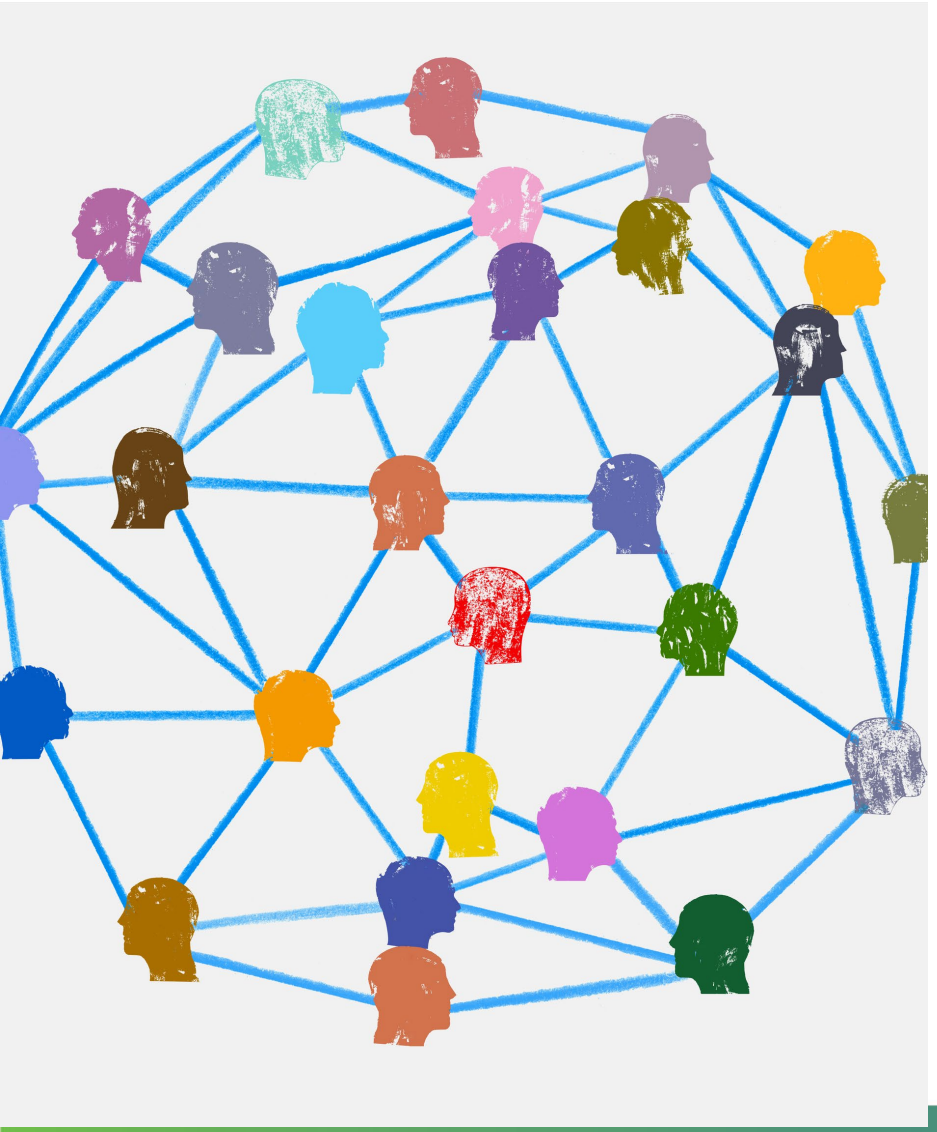
→ Does not capture the full expanse of personal data under GDPR and ignores combinatorial and contextual factors

Risks of the Narrow Governance approach

- Reidentification Risks
- Ethical Risks
- Contractual Risks
- Compliance Risks

What is Implicative Data?

- Implicative data refers to information that, while not directly or indirectly identifying individuals, can influence perceptions, decisions, or outcomes related to them.



Benefits of Implicative Data

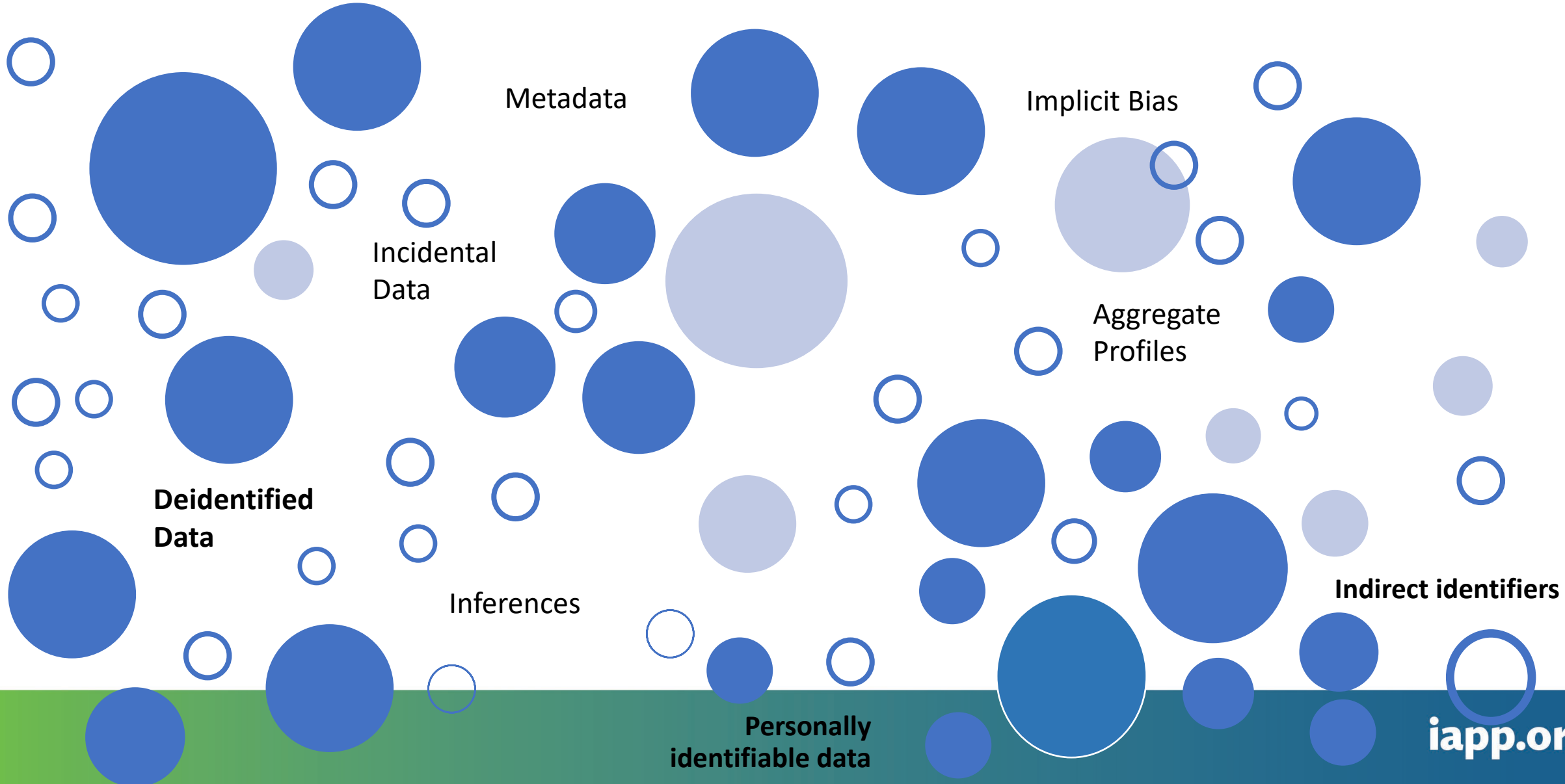
- Extends data governance to entire data ecosystem with no artificial boundaries, where any data has the potential to be personal
- Surface previously unknown privacy risks at the individual, group, and organization levels
- Align with the level of data protection mandated by GDPR and other data protection regulations and laws

Consequences of ignoring Implicative Data

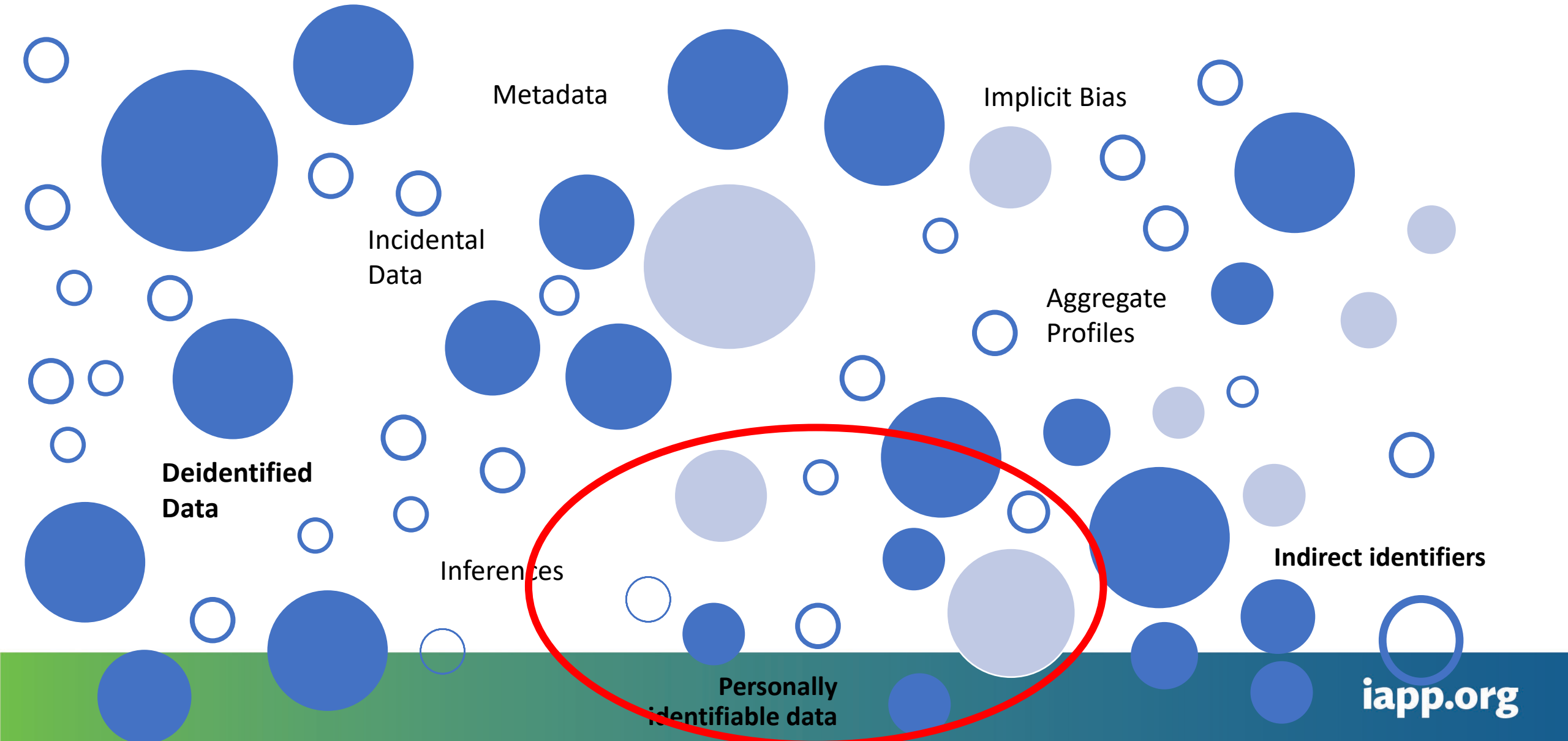
- Failure to trigger a privacy or security review when it is needed
- Inadvertent Revelation and/or Creation of Personal Information
- Bias, Erroneous Conclusions, and Misleading Narratives
- Regulatory Non-Compliance
- Larger Unprotected Data Landscape for Attack

Identifying individuals can be like detective work

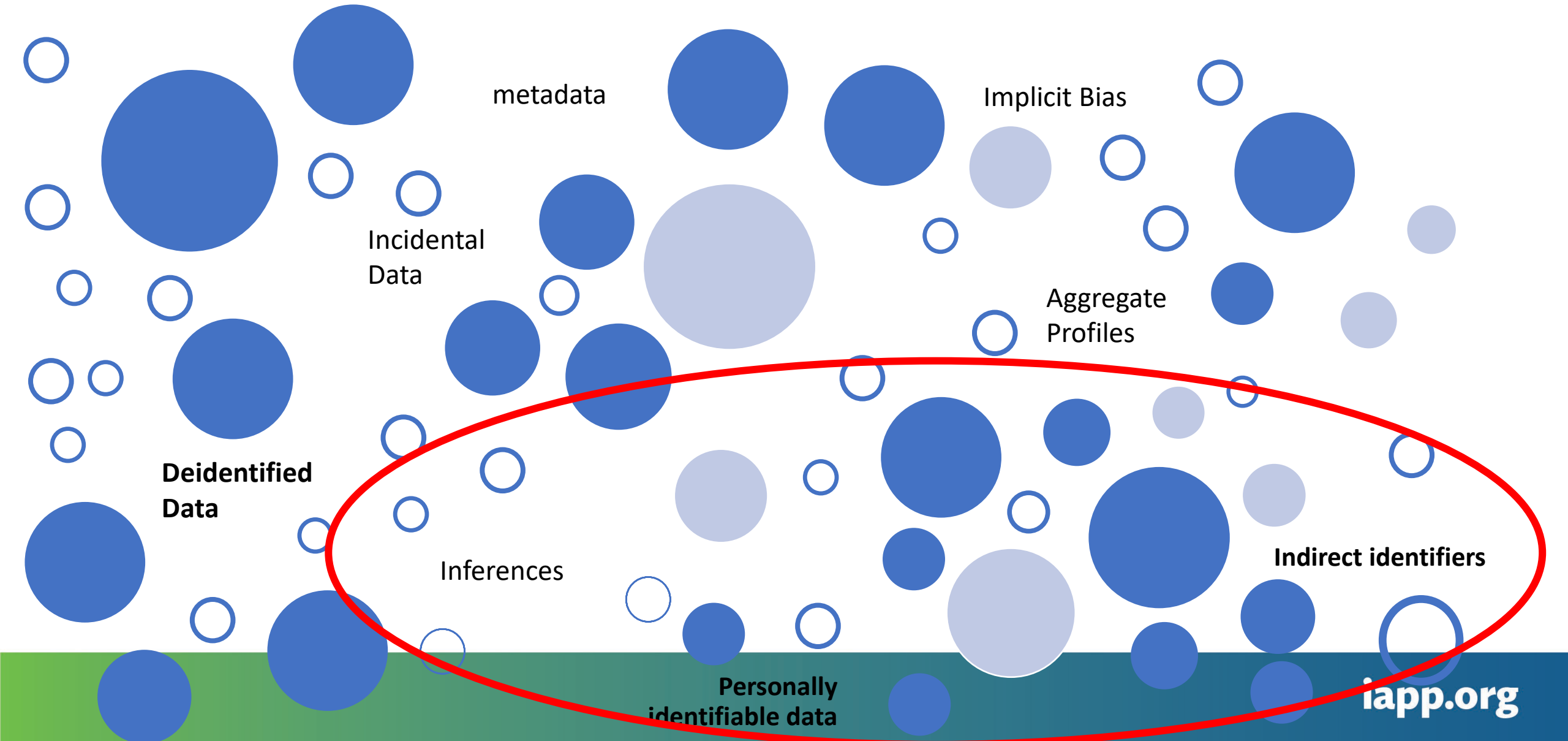
Implicative data



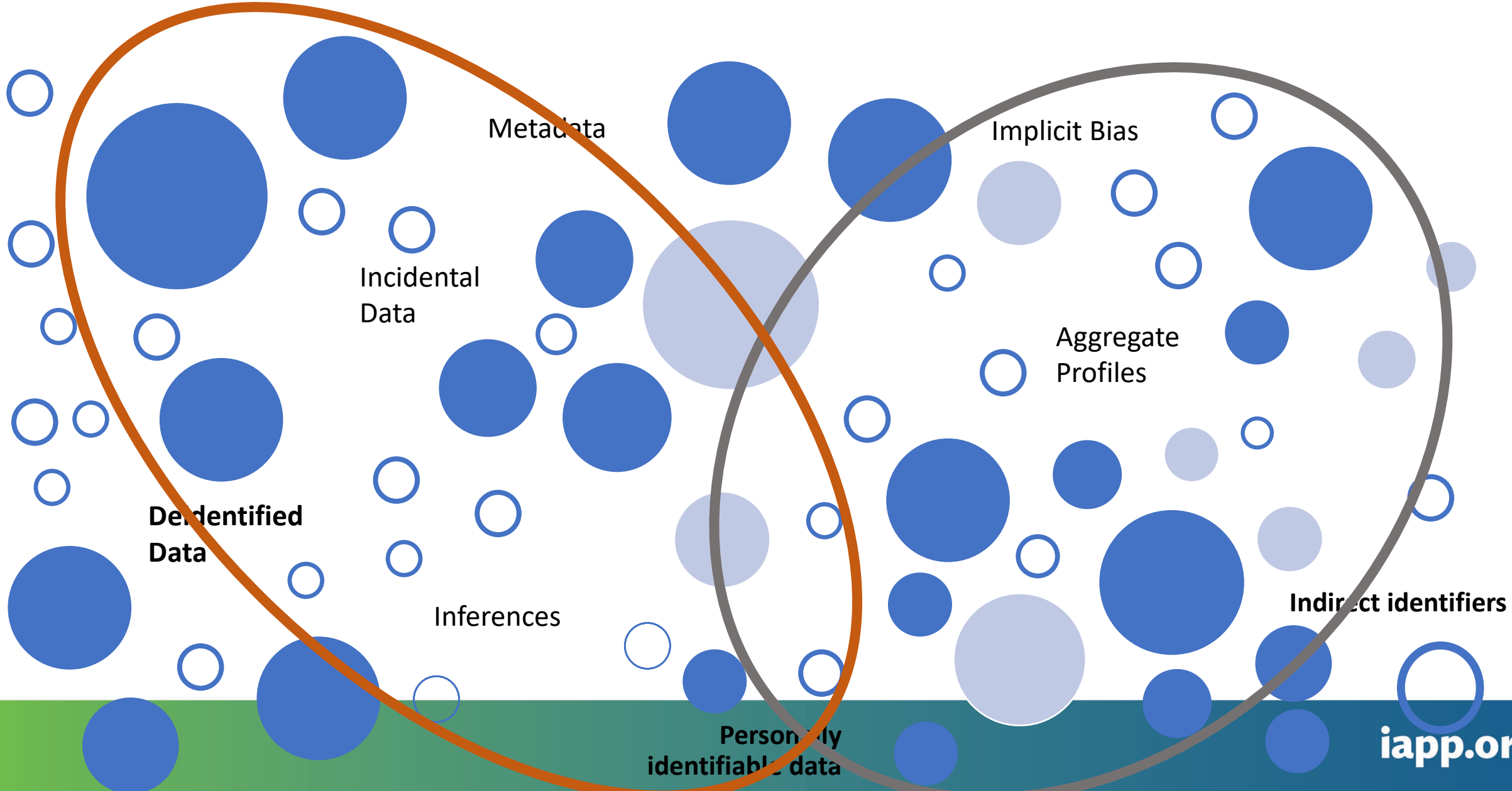
Personally Identifiable data



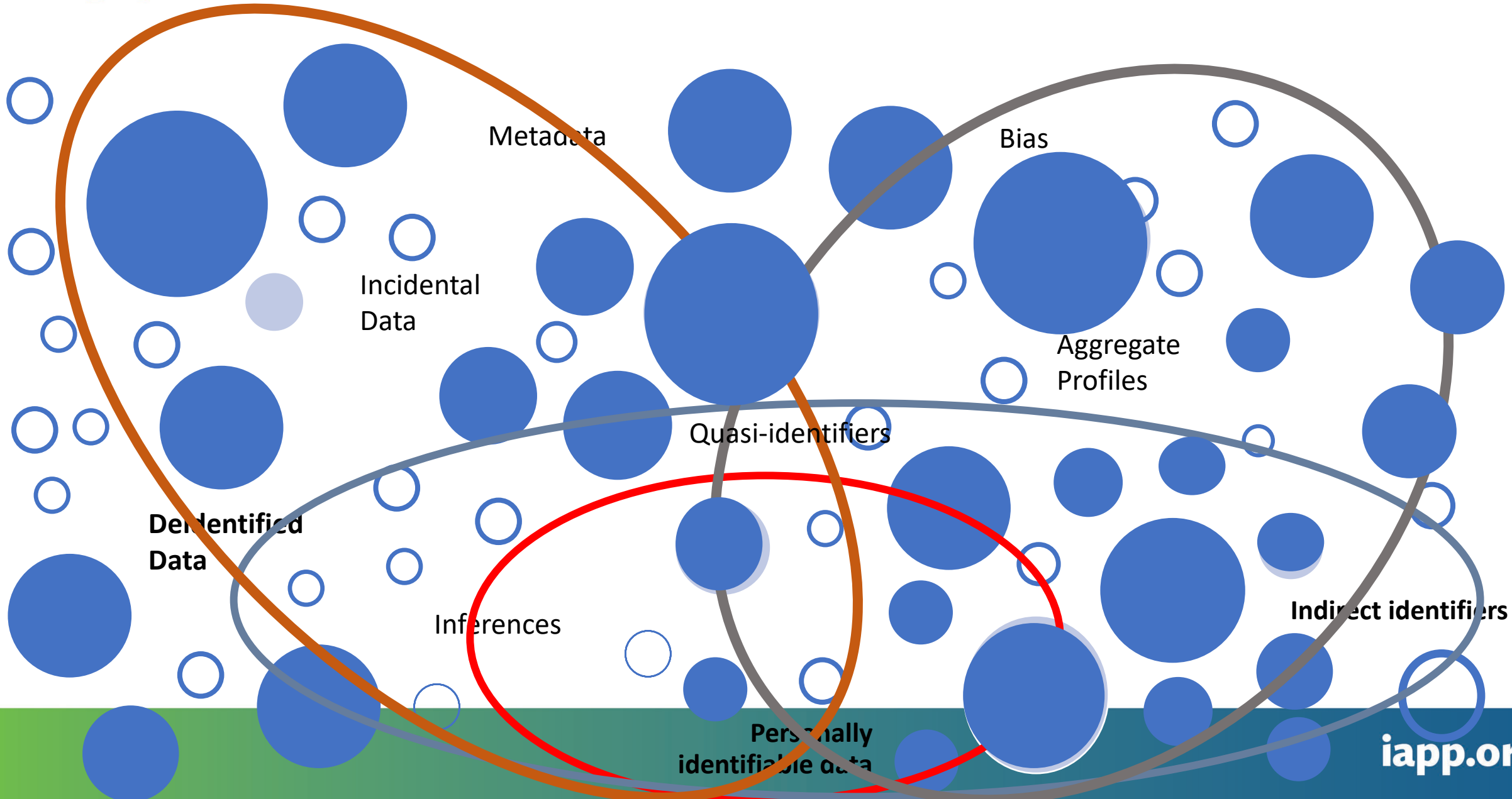
iapp "Personal" data



Other Types of Data



Implicative data – connecting the dots

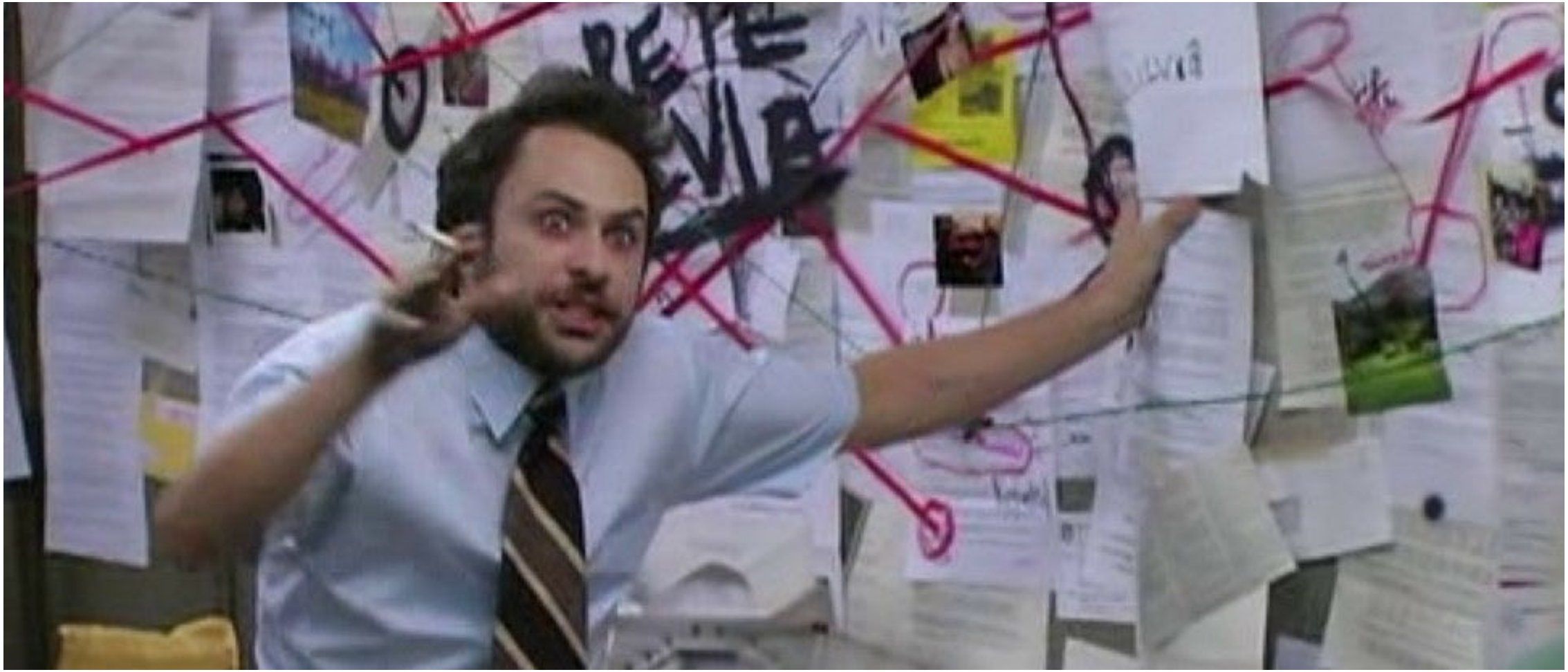


Examples: Calendar Entries, GPS Metadata, Behavioral Profiles and Beyond

The Scoring of America
World Privacy Forum
Report, 2014

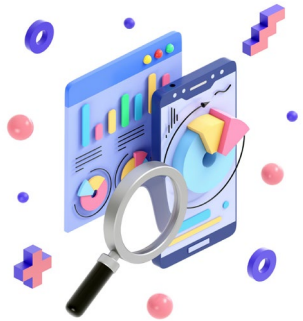
Voices in the code

David G Robinson, 2022



It’s all implicative!

Foundations of Implicative Data Governance



Contextual-based Risk Assessment

Data Minimization Principle

Context-aware by Design Privacy Engineering

Applications: Privacy Context

Definition

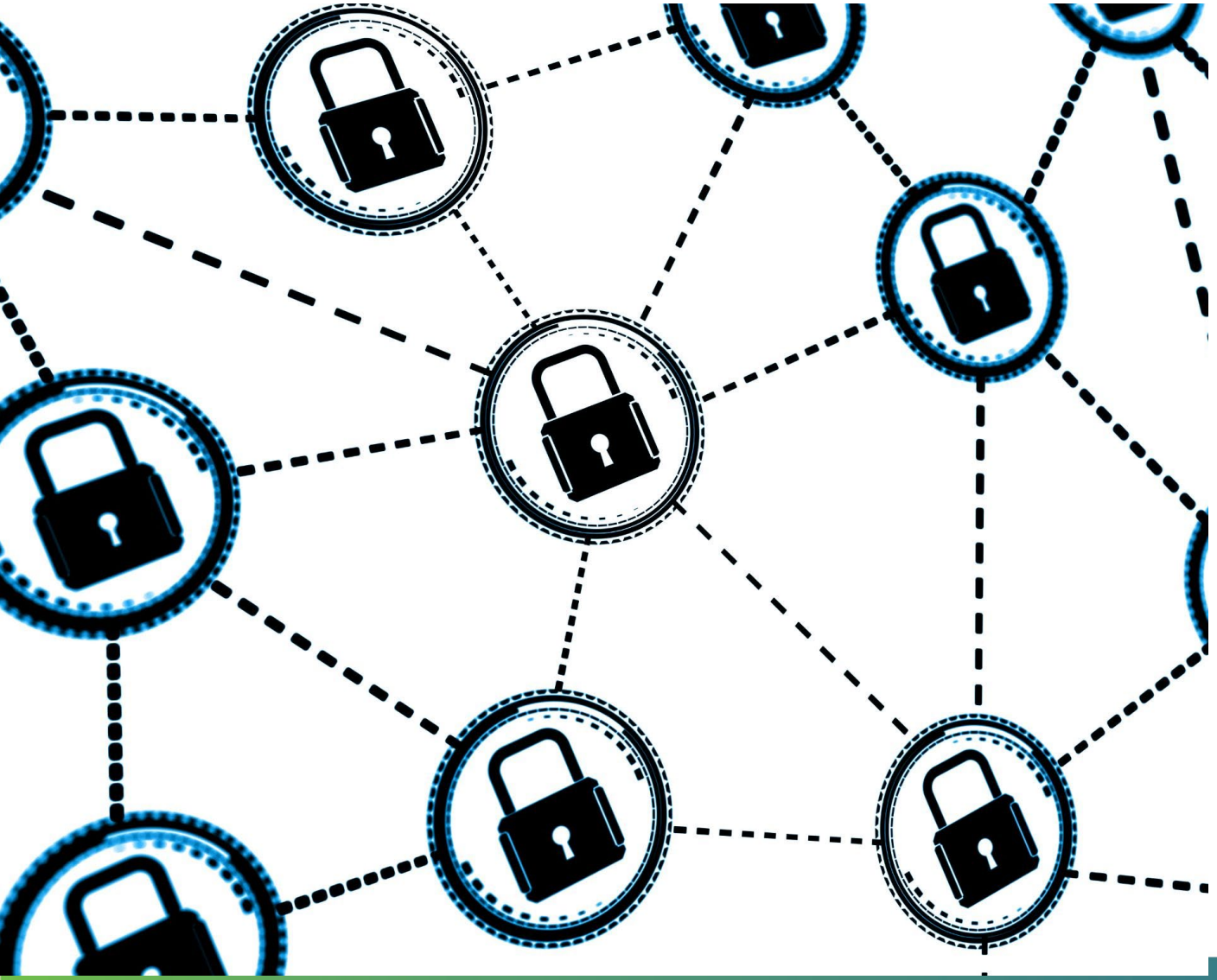
Full set of conditions that shape how personal data is collected, used, and governed at HP. It includes:

- **Source of data**: Where and how data was collected (e.g., app, region, notice).
- **Applicable rules**: Legal, regulatory, and policy frameworks tied to the data.
- **Context**: The purpose and environment in which data is used.
- **User and data collection context**: Who the data relates to and under what conditions it was gathered.

This context is captured through metadata, tagging, and system intelligence to enable precise privacy controls and avoid one-size-fits-all approaches

Why Privacy Context is Important

- **Precision in Controls**: High-context data enables tailored privacy protections, reducing both overreach and under-compliance.
- **Ethical Alignment**: Contextual privacy respects social norms and expectations, especially when handling sensitive or implicative data.
- **Global Consistency**: Privacy commitments transcend borders, requiring context-aware governance to meet and exceed legal standards worldwide.
- **AI and Emerging Tech**: As AI integrates across operations, contextual privacy ensures responsible innovation by aligning data use with ethical and legal expectations.



Benefits of Privacy Context

- Enables **automated decisioning** based on context.
- Supports **risk-based reviews** and **fast-track lanes** for low-risk use cases.
- Forms the foundation for **Privacy Statement as Code** and future-proof governance architectures.

Operationalization of Implicative Data

iappWhat is Context Operationalization?

Information operationalization is the act of defining what "information" means in a specific context and determining how it can be communicated and exchanged, understood, and Interpreted. This underpins the establishment of norms and expectations.

Technical operationalization refers to the process of defining privacy context in terms of a specific data model with associated technical procedures or systems that allow for consistent measurement and analysis at scale.

Issues

Informational

Information flow

Ethical assessment

Norms and expectations

Transparency/Interpretability

Technical

Technical definition of context

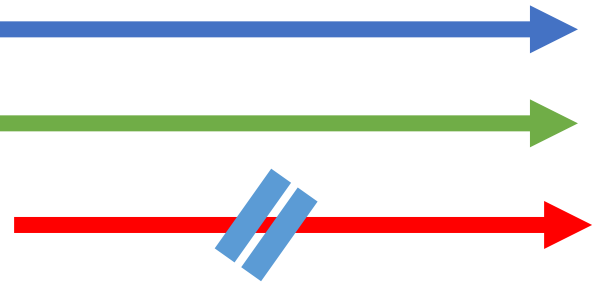
Dynamic vs Overlapping context

Context Partitioning: Micro/Macro

Elements of Consent: Analog to Digital

Belmont Report (1976)

- **Voluntary**
- **Informed**
- **Comprehended**

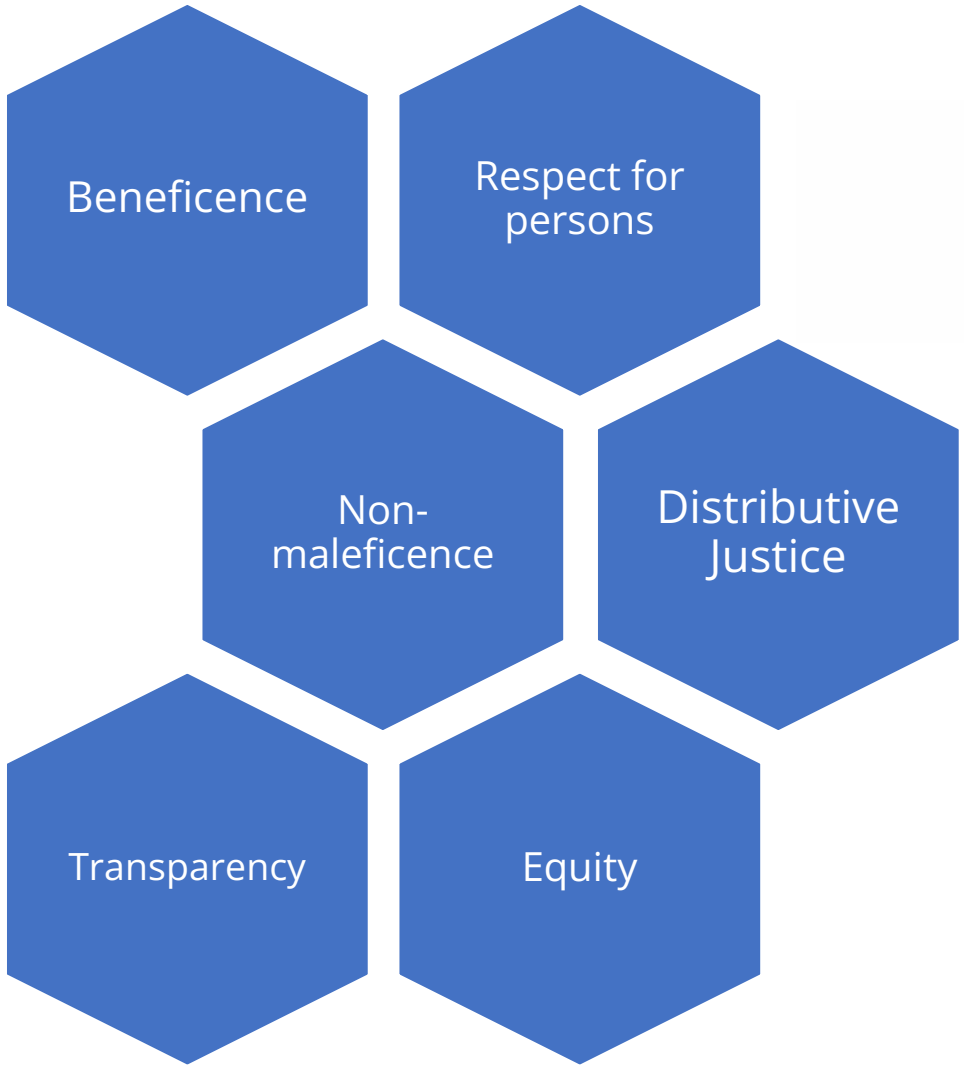


GDPR (2016)

- **Freely given**
- **Informed**
- **Specific**
- **Documented**
- **Retractable**

Reality evolves because of context

- What is gained and lost?
- How can we compensate for the limitations of our medium?
- How can we retain (and augment!) the integral function of consent: to respect persons?
- How can we meet changing expectations for expedience and comprehension?
- What is exceptional about emerging technologies?



Technical

Technical definition of context

Dynamic vs Overlapping context

Context Partitioning: Micro/Macro

Areas of the Future

Technical

Dynamic vs Overlapping Contexts

Defining and Detecting Contexts: What exactly constitutes a "context" in practice? Real-world contexts are fluid, overlapping, and can change dynamically.

Context Partitioning

Embed CI reasoning into AI assistants: Context aware AI models honor context-specific norms – effectively giving them a built-in "ethical guardrail" for privacy utilizing machine reasoning (to infer norms) and memory architectures that tag data with context.

Dynamic and Overlapping Contexts

Declarative Policy Language: Information flows expressed as temporal-logic formulas that can capture contextual constraints. This formalism allows reasoning about whether a sequence of actions violates or complies with contextual norms

Technical definition of Context

Context Taxonomy and Graph Database: Create a contextual element taxonomy and use a graph database to determine relationship and strength of the relationships. GraphRAG and RAG can be leveraged for this purpose.

Technical Definition of context

Standardize context for engineering: Standard definitions of contexts and data flows that engineers can reference (much like standards that exist for data protection terms).

Context Partitioning

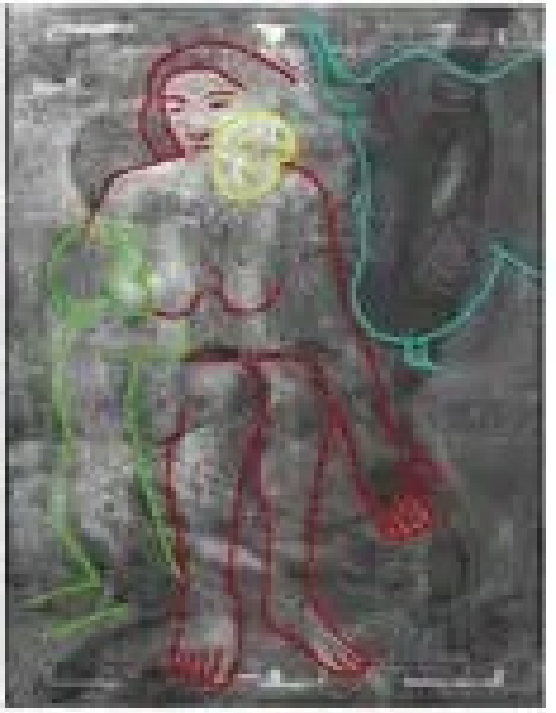
Contextual Privacy Rules (CPP): Adaptive policies that change based on context. Rather than a static privacy notice, a CPP would dynamically enforce rules depending on variables like who is requesting data and why.

Conclusion

Addressing Implicative Data

Robust, Holistic Governance Approach

Contextual Awareness Helps Meet User Expectations



Declarative Policy Language

Image credit: https://www.creatis.insa-lyon.fr/~letang/x-ray-book/conclusion.html

Connect with us!

- Emmi Bane
  - emily.bane@hp.com
- Carl Mathis
  - carl.mathis@hp.com

Web Conference
Participant Feedback Survey

Please take this quick (2 minute) survey to let us know how satisfied you were with this program and to provide us with suggestions for future improvement.

Click here: https://iappwf.questionpro.com/t/AbBPvZ7F25

Thank you in advance!

For more information: www.iapp.org

Attention IAPP Certified Privacy Professionals:

This IAPP web conference may be applied toward the continuing privacy education (CPE) requirements of your CIPP/US, CIPP/E, CIPP/A, CIPP/C, CIPT or CIPM credential worth 1.0 credit hour. IAPP-certified professionals who are the named participant of the registration will automatically receive credit. If another certified professional has participated in the program but is not the named participant then the individual may submit for credit by submitting the continuing education application form here: submit for CPE credits.

Continuing Legal Education Credits:

The IAPP provides certificates of attendance to web conference attendees. Certificates must be self-submitted to the appropriate jurisdiction for continuing education credits. Please consult your specific governing body's rules and regulations to confirm if a web conference is an eligible format for attaining credits. Each IAPP web conference offers either 60 or 90 minutes of programming.