



Briana Vann



Sarah Downs

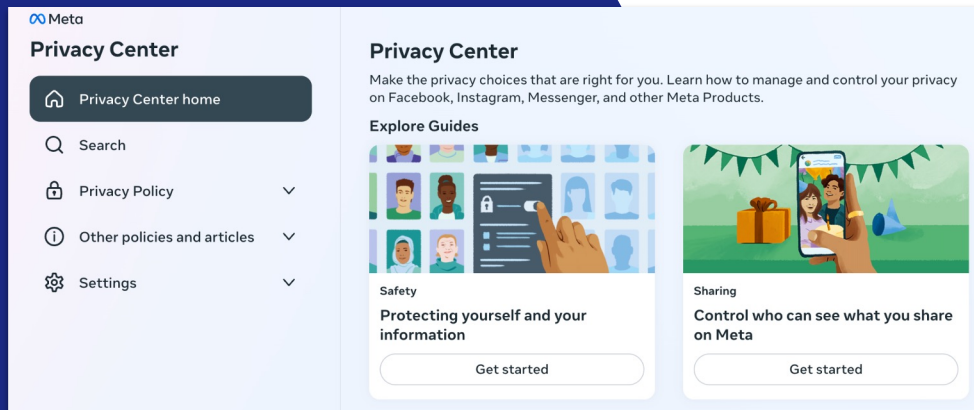
Taxonomy & Ontology as Privacy-Enabling Technology

Our Topics Today

What is privacy and why does it matter?

How can enterprise taxonomies and ontologies support privacy policies and enforcement? What are the pros and cons of each approach?

What best practices should you follow when adapting your taxonomies and ontologies for privacy enforcements?



Privacy tools that put you in control.

When it comes to privacy, we know one size does not fit all. That's why we build controls that are easy to use so you can choose the privacy settings that are right for you.



LinkedIn Privacy

[Privacy Settings](#) [Privacy FAQs](#) [Regional Info](#) [Privacy Policy](#)

Without our members, there is no LinkedIn.

This is the place you come to build professional relationships, explore new opportunities and find success with the help of your LinkedIn communities. To explore your full potential on LinkedIn, we know you need to trust us with your personal data. We are committed to working hard every day to maintain that trust.

What is privacy?



Conditions established in Terms of Service or statements made in user privacy resources



Transparency and user control over data

Consent
Customization and management of data collection
Personalization



Enterprise safeguarding of user data

Encryption
Data transformation: de-identification, aggregation, or anonymization
Anti-scraping
Retention & deletion
Data understanding

Why does privacy matter to organizations?

Privacy

From “Heavy Purchasers” of Pregnancy Tests to the Depression-Prone: We Found 650,000 Ways Advertisers Label You

themarkup.org

MONEYWATCH >

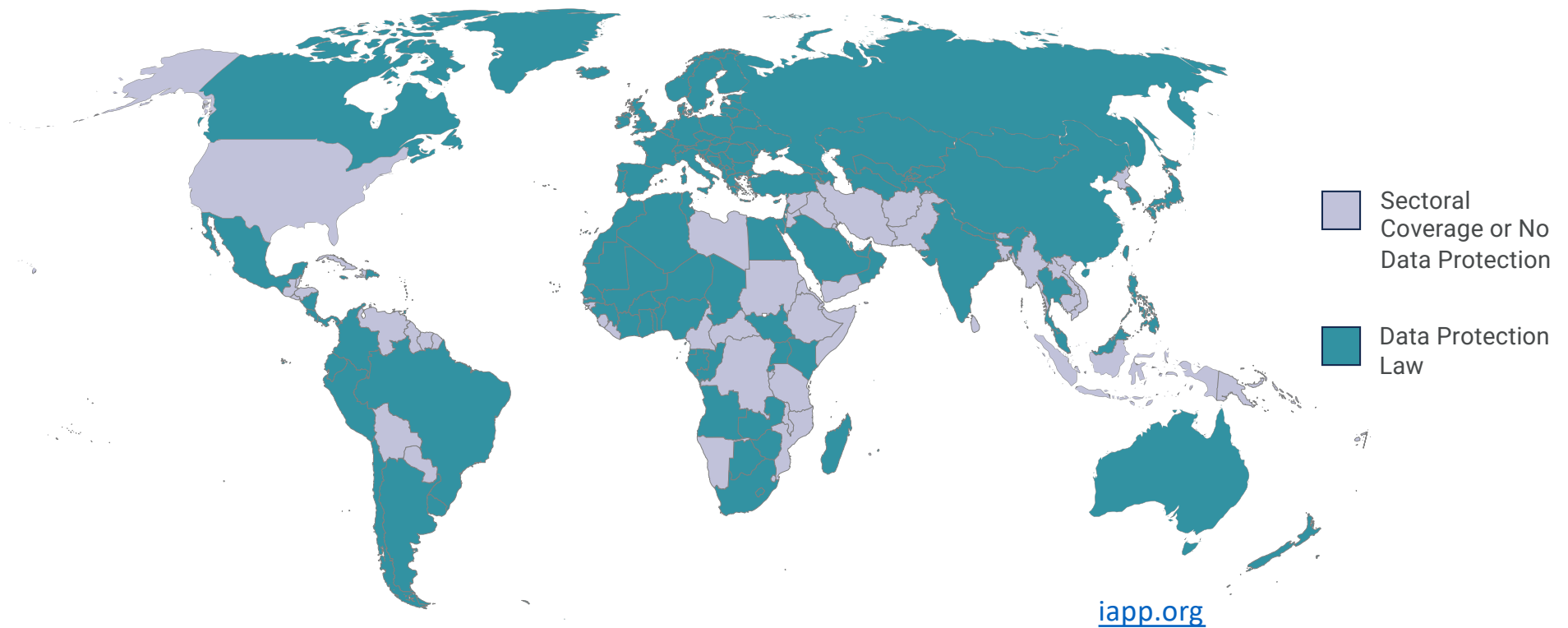
H&R Block and other tax-prep firms shared consumer data with Meta, lawmakers say

[cbsnews.com](https://www.cbsnews.com)

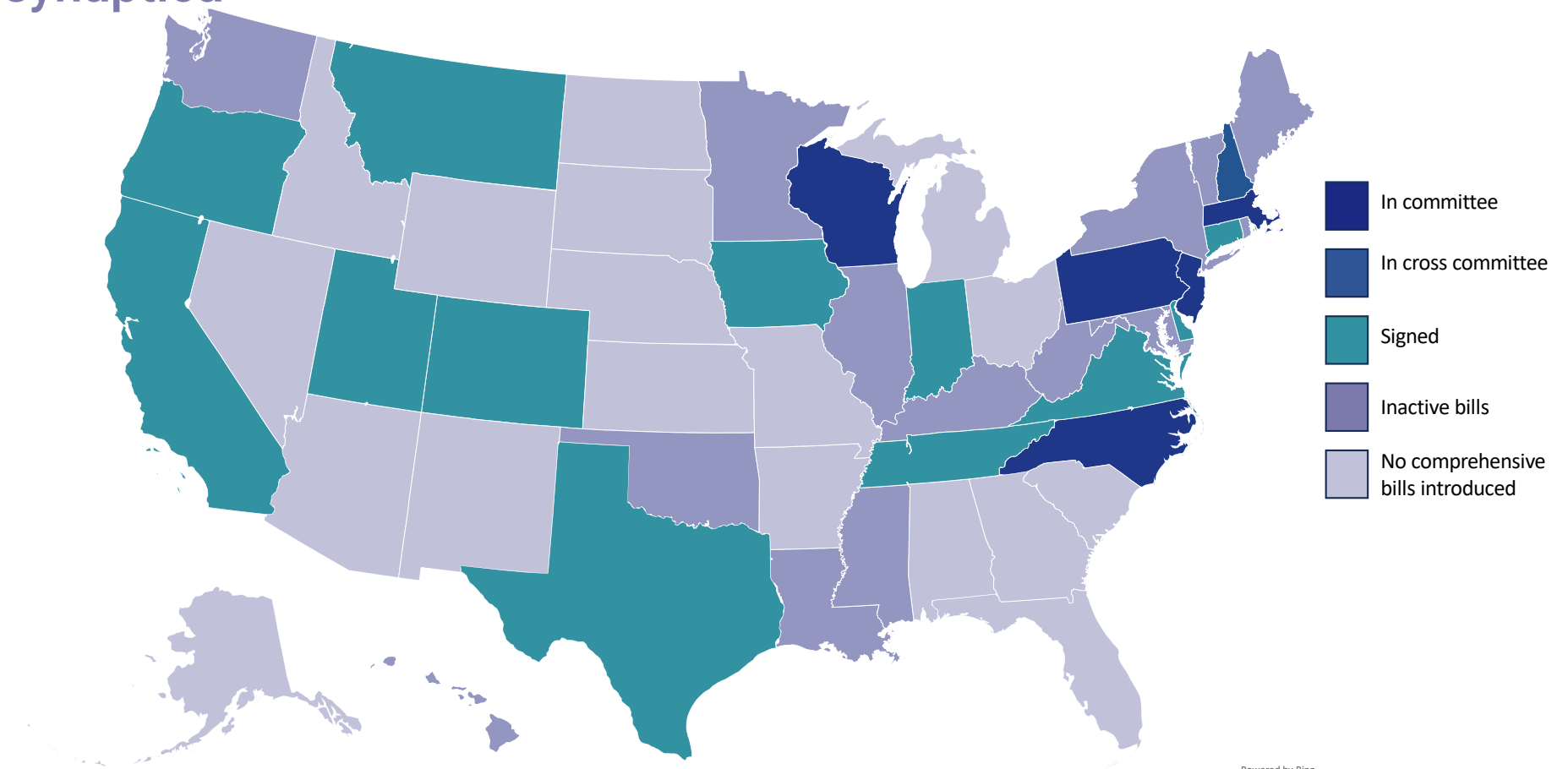
Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information

[pewresearch.org](https://www.pewresearch.org)

Global privacy regulation is expanding

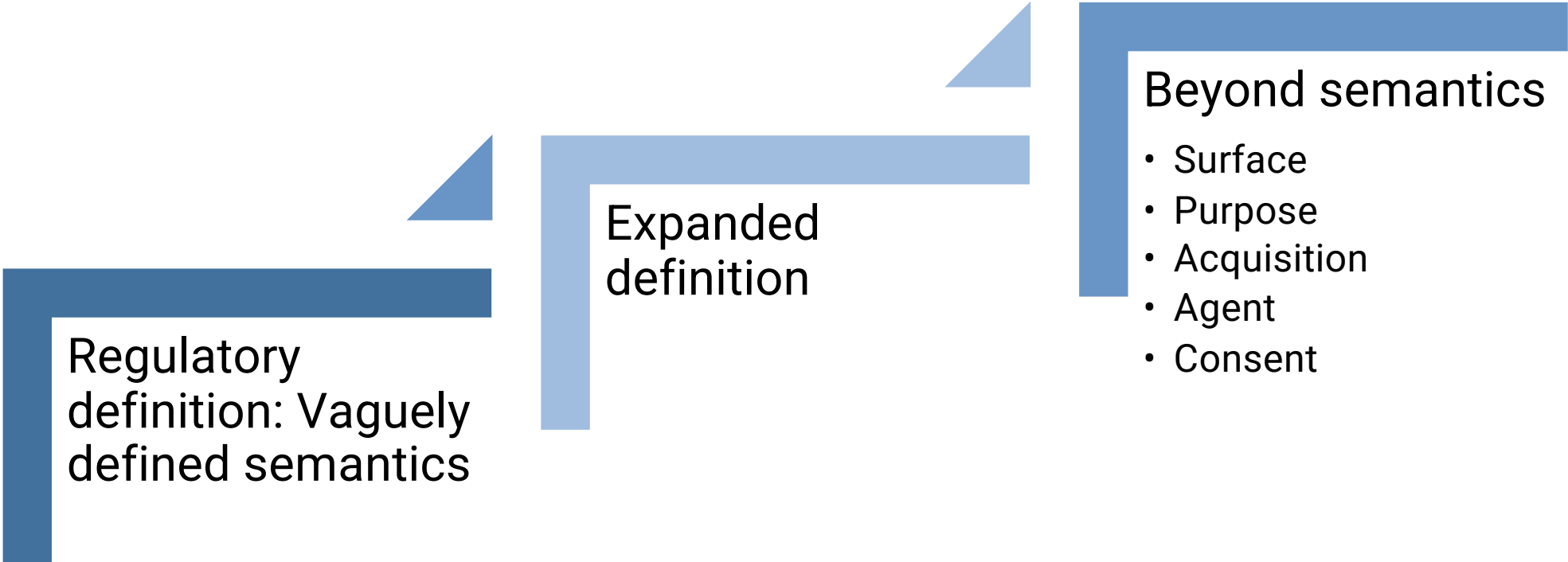


Powered by Bing
© Australian Bureau of Statistics, GeoNames, Microsoft, Navinfo, Open Places, OpenStreetMap, TomTom, Zenrin



Powered by Bing
© GeoNames, Microsoft, TomTom

Enforcements and sensitivity are multi-faceted



Regulatory
definition: Vaguely
defined semantics

Expanded
definition

Beyond semantics

- Surface
- Purpose
- Acquisition
- Agent
- Consent

GDPR: Article 9

Regulatory
definition: Vaguely
defined semantics

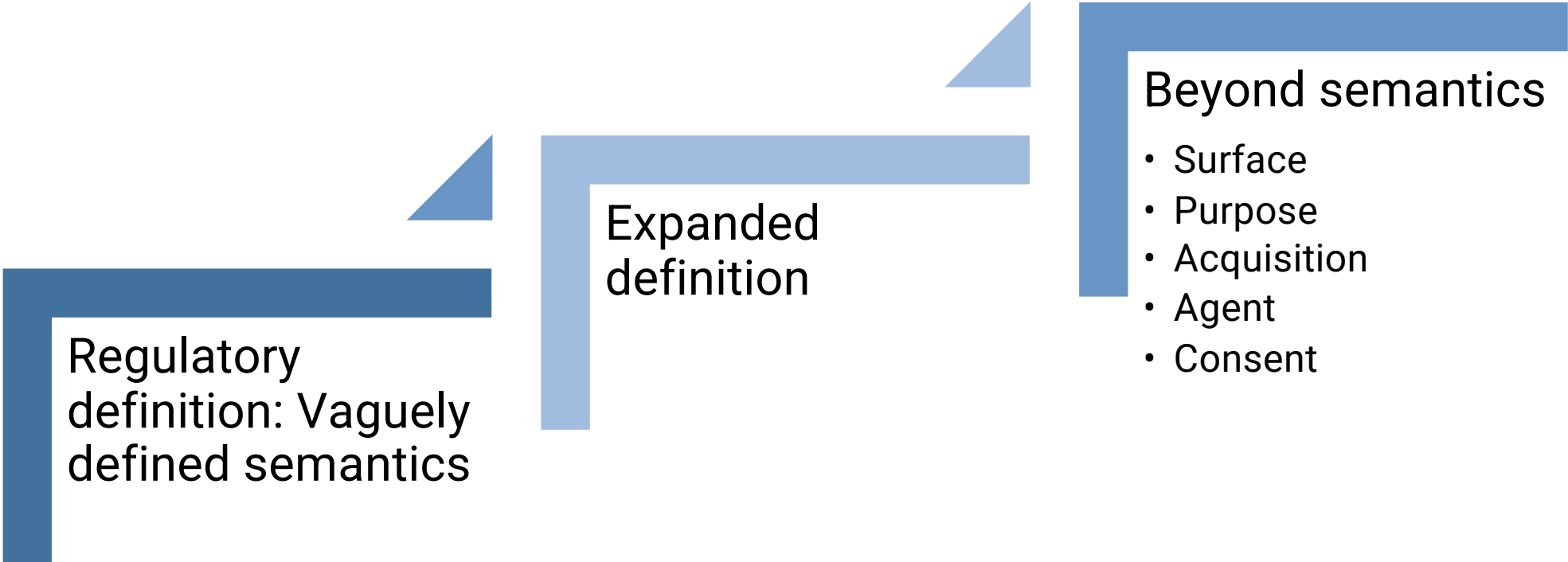
Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

Expanded definition

*[Privacy] laws make a fundamental conceptual mistake – they embrace the idea that the **nature** of personal data is a sufficiently useful focal point for the law. But nothing meaningful for regulation can be determined solely by looking at the data itself. Data is what data does. To be effective, privacy law must focus on harm and risk rather than on the nature of personal data. The implications of this point extend far beyond sensitive data provisions. In many elements of privacy laws, protections should be proportionate to the harm and risk involved with the data collection, use, and transfer.*

Dr. Daniel Solove,
[**Data Is What Data Does: Regulating Use, Harm, and Risk Instead of Sensitive Data**](#) (2023)

Enforcements and sensitivity are multi-faceted



Regulatory
definition: Vaguely
defined semantics

Expanded
definition

Beyond semantics

- Surface
- Purpose
- Acquisition
- Agent
- Consent

How can taxonomy and ontology help?

Metadata Design

- Enforcement specific
- Point-in-time accuracy
- Limited change to existing infrastructure and design
- No future-proofing
- Limited knowledge-building

Privacy-Aware Taxonomy

- Enforcement agnostic
- Point-in-time accuracy
- Limited change to existing infrastructure
- Moderate evolution of design
- Partial future-proofing
- Knowledge-building
- Risk of bias
- Limited ability to address multiple dimensions of data

Ontology for Data Annotation

- Enforcement agnostic
- Long design timeframes
- Change to fundamental infrastructure and design
- Maximally future proof
- Knowledge-building
- Lesser risk for bias in design
- Can address multiple dimensions of data

Metadata Design: Policy-Driven Labels

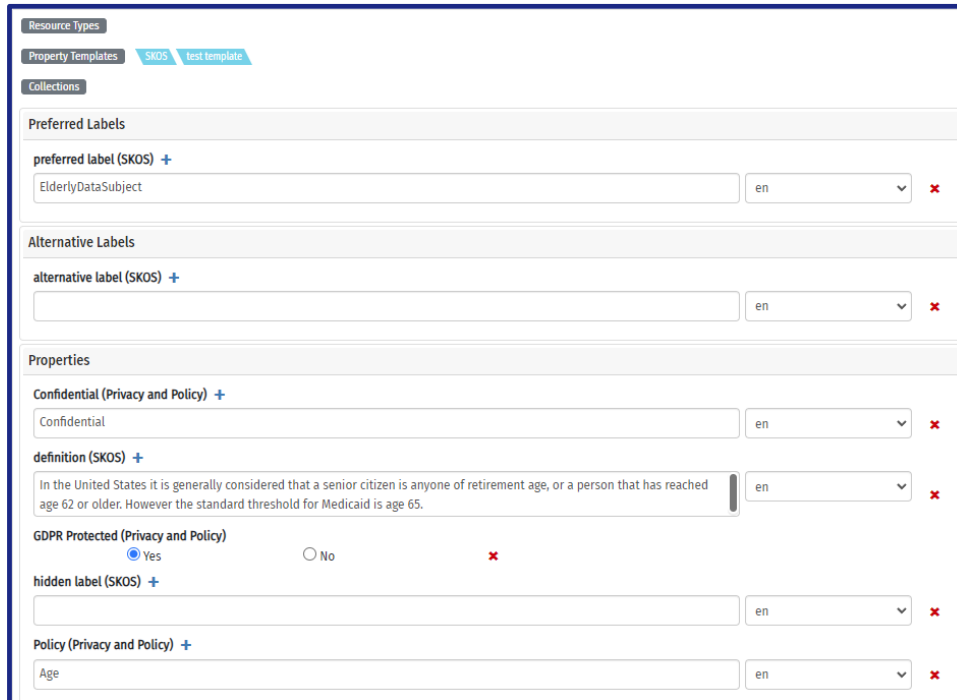


Rapid implementation

Supported with existing tooling

Point-in-time accuracy

Requires no taxonomy experience



No future proofing

No privacy knowledge developed by the taxonomy team

Metadata Design: Semantic Labels

Informed by existing and anticipated policies, but driven by data semantics (e.g., “Age” “Gender”)



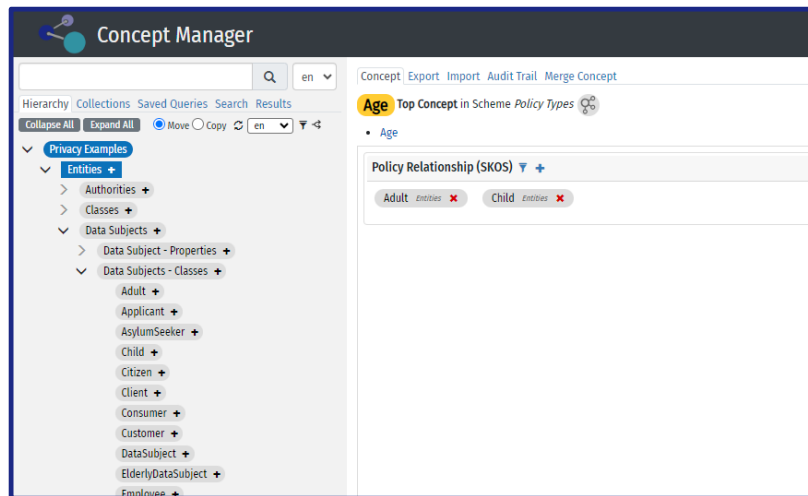
Rapid implementation

Supported with existing tooling

Point-in-time accuracy

Requires no taxonomy experience

Extensibility beyond regulation



Minor future proofing

Some privacy awareness developed by the taxonomy team

Policy (Privacy and Policy) +	
Age - Child	en ✖
Priority Level (Privacy and Policy) +	
Level III	en ✖

Privacy-Aware Taxonomy Design



Rapid implementation

Supported with existing tooling

Point-in-time accuracy

Privacy knowledge built in taxonomy team

Extensibility beyond regulation

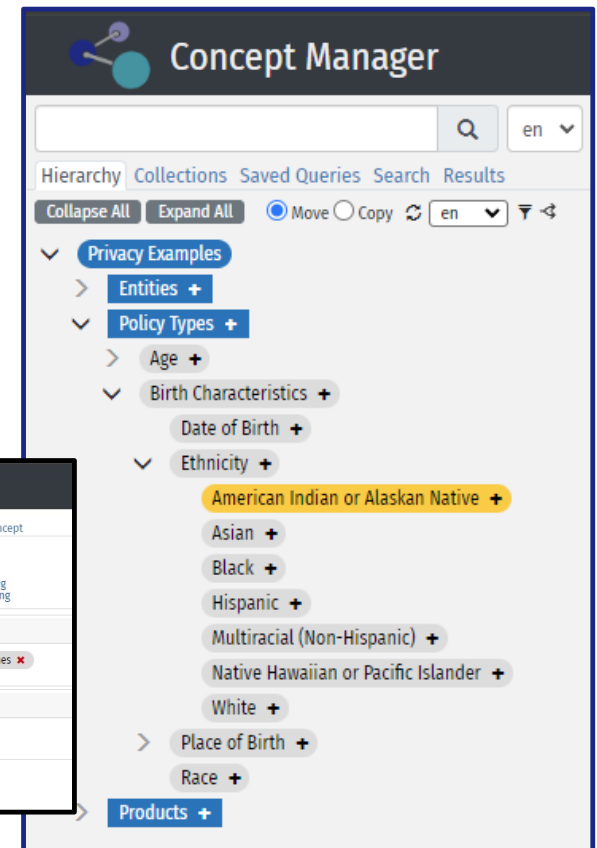
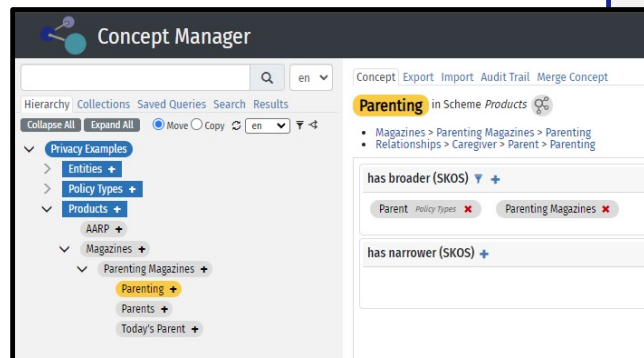


Requires taxonomy expertise

More robust future proofing; addresses only certain dimensions of data



Risk of "othering" bias



Data Annotations Ontology



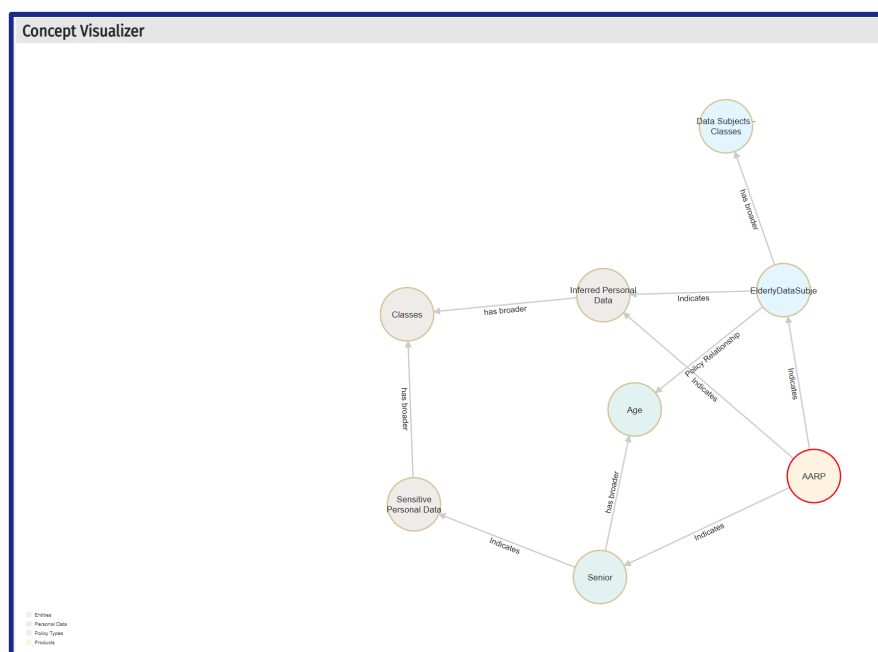
Rich privacy knowledge in taxonomy team

Maximally future proof and extensible

Addresses many dimensions of data for nuanced enforcement

No “othering” bias due to definition of individuals

Support for non-privacy uses cases (e.g., content audits)



Evolving point-in-time accuracy during build

Requires ontology expertise



Large-scale effort; long implementation

Requires ontology tooling and new design

Privacy Taxonomy & Ontology Best Practices

Pursue an enforcement-informed but enforcement agnostic approach

Partner with policy and legal colleagues

Develop privacy awareness on your taxonomy team

Ensure proper tooling:
Review, browse, label selection

Define false positive vs. false negative tradeoffs and thresholds

Product management support:

- Evangelism
- Conflict resolution with other non-privacy product goals

Thank You

Synaptica



info@synaptica.com



<https://www.synaptica.com/>



<https://www.twitter.com/synaptica>



<https://www.linkedin.com/synaptica-llc>



<https://www.youtube.com/c/Synaptica>