Confirmation bias in the privacy profession: common misreading of the NIST Privacy Framework

Privacy Engineering Practice and Respect 2023

Nandita Narla
Doordash

Member, Advisory Board

Member

Chair, Standards Committee

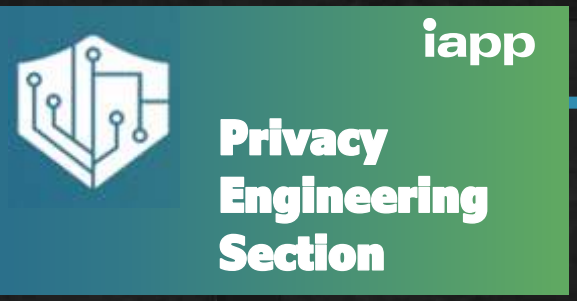
Jason Cronk
Enterprivacy Consulting Group

Former Member, Advisory Board

Former Section Leader

Member

President



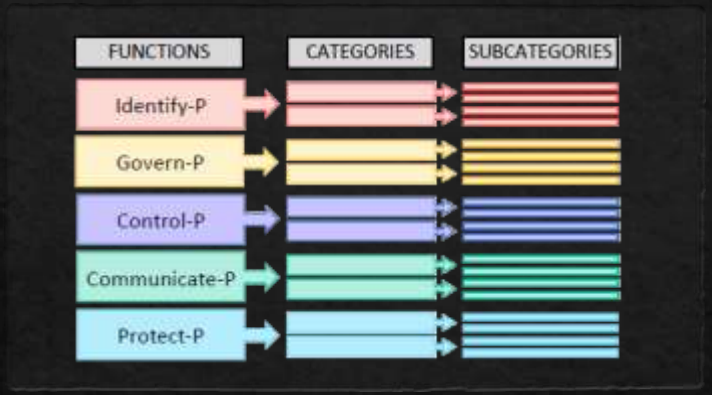
NIST PWWG

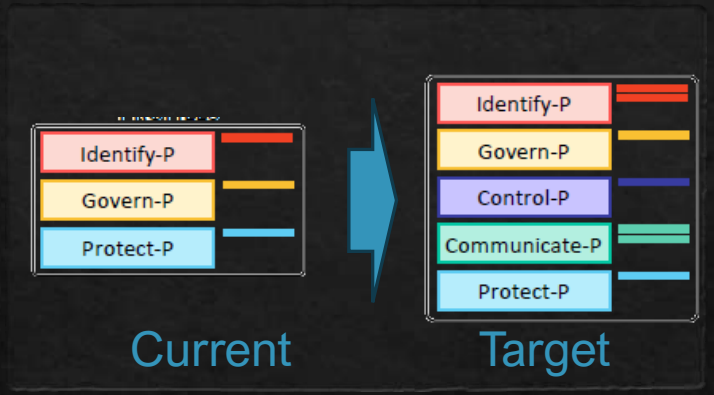
Privacy Workforce Working Group

IOPD
Institute of Operational Privacy Design

NIST Privacy Framework:

A TOOL FOR IMPROVING PRIVACY THROUGH ENTERPRISE RISK MANAGEMENT





Core

The **Core** provides an increasingly granular set of activities and outcomes that enable an organizational dialogue about managing privacy risk

Profiles

Profiles are a selection of specific Functions, Categories, and Subcategories from the Core that an organization has prioritized to help it manage privacy risk

Implementation Tiers

Implementation Tiers support communication about whether an organization has sufficient processes and resources in place to manage privacy risk and achieve its Target Profile

Appendix B Glossary

- **Data** - A representation of information, including digital and non-digital formats.
- **Privacy Risk** - The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur.
- **Subcategory** - The further divisions of a Category into specific **outcomes** of technical and/or management activities.
- **Privacy Control**- The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks. *(NIST 800-53)*

Confirmation Bias

Confirmation bias is the tendency to search for, interpret, favor, and recall information in a way that confirms or supports one's prior beliefs or values. People display this bias when they select information that supports their views, ignoring contrary information, or when they interpret ambiguous evidence as supporting their existing attitudes. The effect is strongest for desired outcomes, for emotionally charged issues, and for deeply entrenched beliefs. - WIKIPEDIA

Common misreadings

Outcomes

Confused with
Controls

Data

Confused with
Personal Data or
Personally Identifiable Information

Tiers

Confused with
Maturity

Privacy Risk

Confused with
Organizational Risk

NIST PF Outcomes ≠ Controls

are not

- **NIST PF Subcategory** - The further divisions of a Category into specific **outcomes** of technical and/or management activities. *(Source: NIST PF Appendix B)*

- **Privacy Control-** The administrative, technical, and physical safeguards employed within an agency to ensure compliance with applicable privacy requirements and manage privacy risks. *(Source: NIST 800 53)*

Privacy professionals commonly equate the NIST privacy framework sub-categories to controls, leading to using the framework as a conformance or auditable standard. A control can help you achieve an outcome.

NIST PF Data ≠ PII

is not

- **NIST PF Data** - A representation of information, including digital and non-digital formats. *(Source: NIST PF Appendix B)*

- **Personal Data** - any information relating to an identified or identifiable natural person (data subject).
- **Personally Identifiable Information(PII)** – Information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. *(Source: NIST CSRC Glossary)*

NIST Privacy Framework applies to any data that can cause problems for individuals. Most privacy professionals narrow the scope of data to their own world view. Personal Data, Personal Information, Personally Identifiable Information, Personal Health Information are all subsets of data.

Implementation Tiers ≠ Maturity Levels

are not

- **NIST PF Implementation Tier** - provide a point of reference on how an organization views privacy risk and whether it has sufficient processes and resources in place to manage that risk. (Source: NIST PF)
- **Maturity Level -** represent a staged path for an organization's performance and process improvement efforts based on predefined sets of practice areas. *(Source: CMMI Institute)*

Most privacy professionals read implementation tiers as organizational maturity levels, which leads to incorrect application in profile development. Implementation Tiers measure sophistication of risk incorporation, maturity levels measure formalization of processes and process improvement.

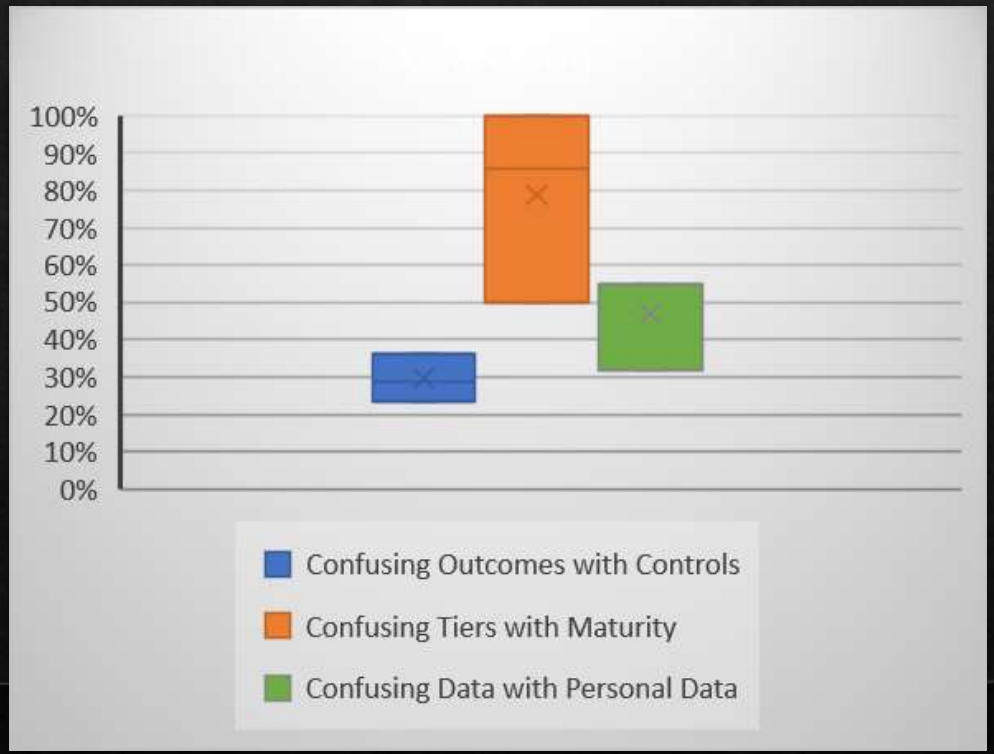
Privacy Risk is not ≠ Organizational Risk

- **NIST PF Privacy Risk** - The likelihood that individuals will experience problems resulting from data processing, and the impact should they occur. (Source: NIST PF Appendix B)
- **Organizational Risk** – includes the business, compliance, reputational, and other risks that collectively create uncertainty to the financial outcome of the organization.

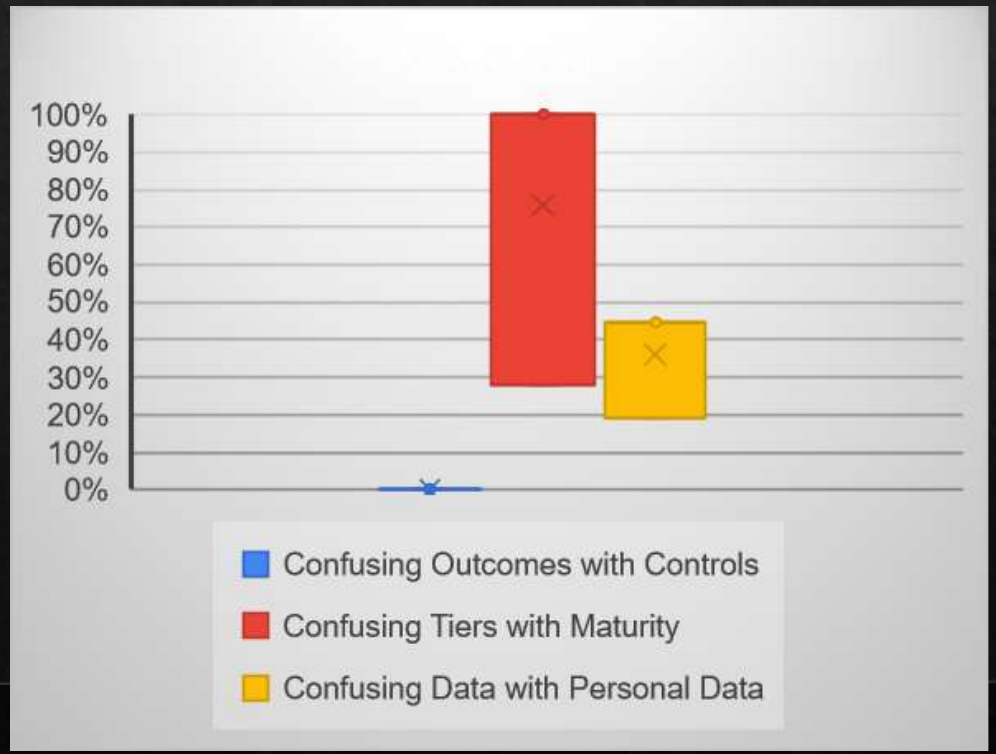
Privacy risk is about risk to individuals where problematic data actions can be equated to normative harms and problems can be equated to tangible consequences. Most implementers focus on compliance or organizational risk. Privacy risk for individuals can be a source of organizational risk.

Online Misinformation

Articles/Blogs



Videos



Communication is Critical

Speaking common language with others in the organization and outside.

When interpreting someone else's work, make sure you are understanding their interpretation and not yours.

Q&A