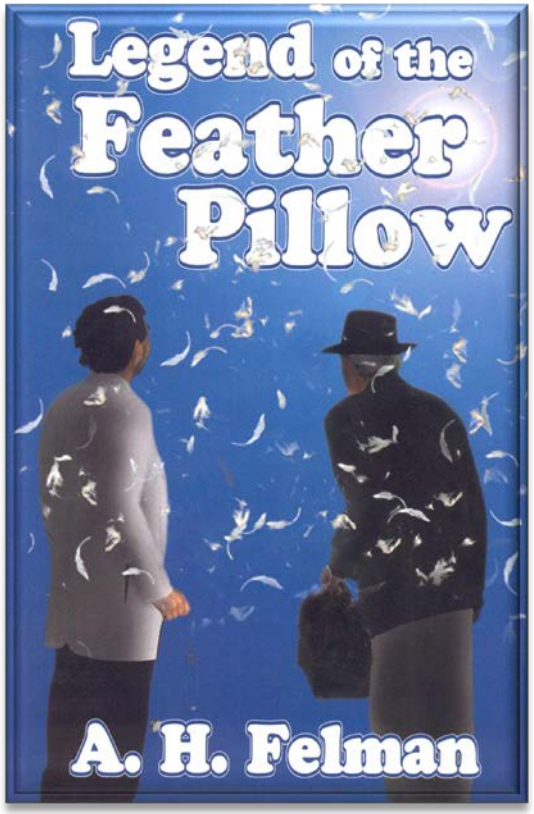
How Do We Make Privacy Protection Tractable?



Cybersecurity Framework

- EO required inclusion of privacy methodology
- Roadmap identified technical privacy standards as an area for future work

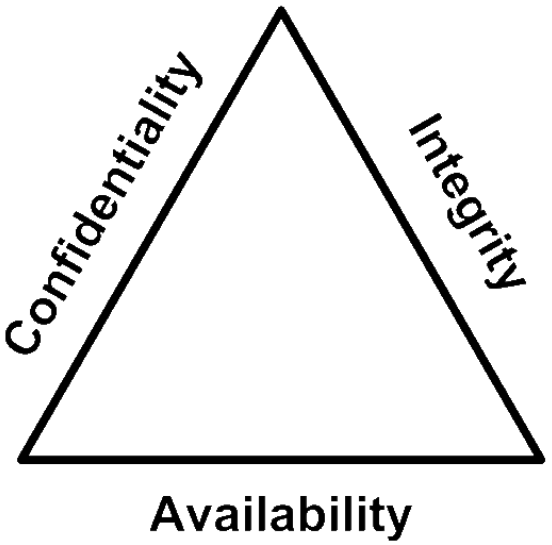
Analogy: Secure by Design

Can the principles of secure design serve as a guide for privacy? Security risk is the likelihood of vulnerability's exploitation by a threat, and the impact of potential harm.

Vulnerability (NIST 800-53r3): Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source.

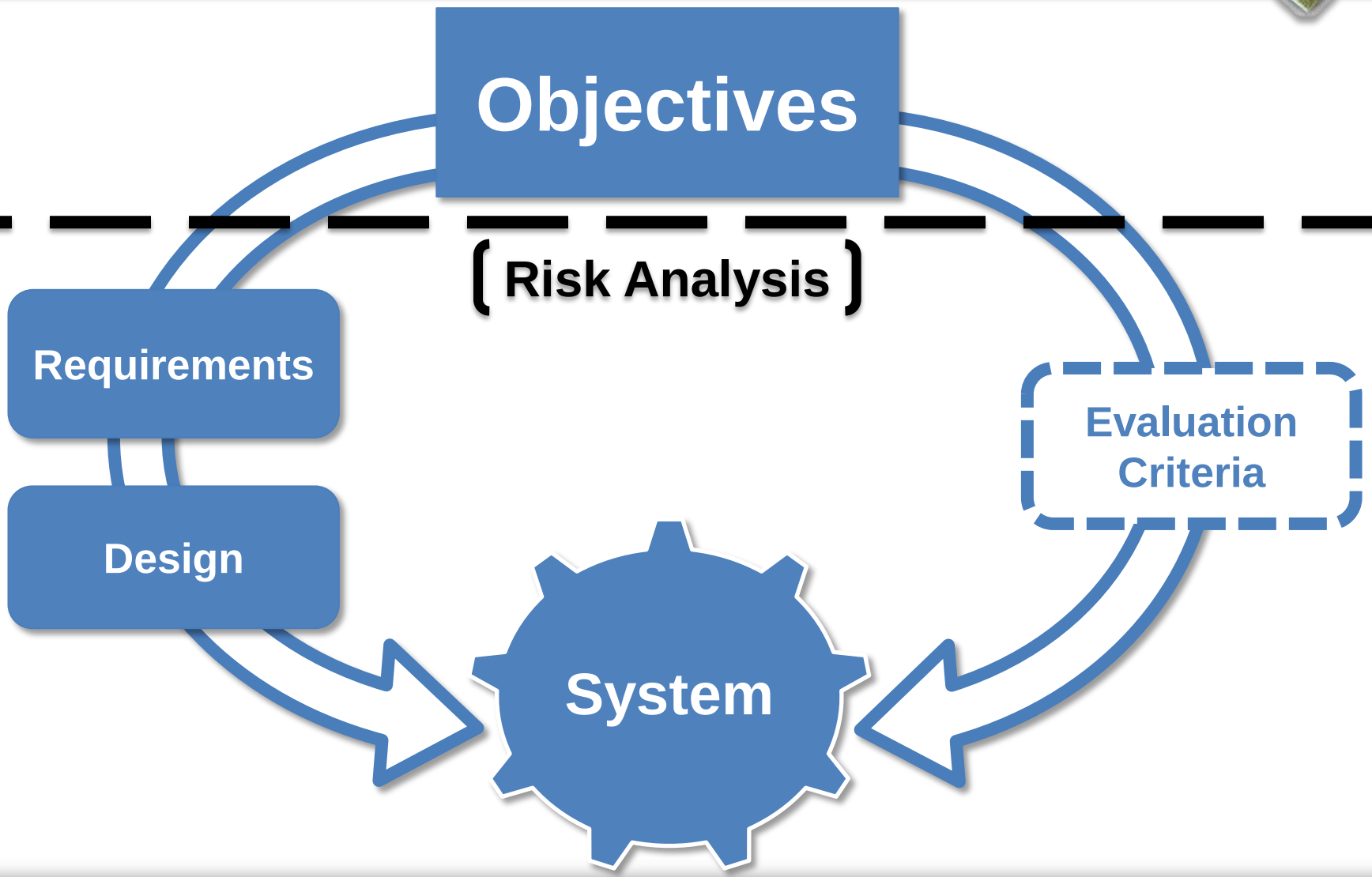
Threat (NIST 800-53r3): Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Harm (NIST 800-122): Any adverse effects that would be experienced by an individual (i.e., that may be socially, physically, or financially damaging) or an organization if the confidentiality of PII were breached.

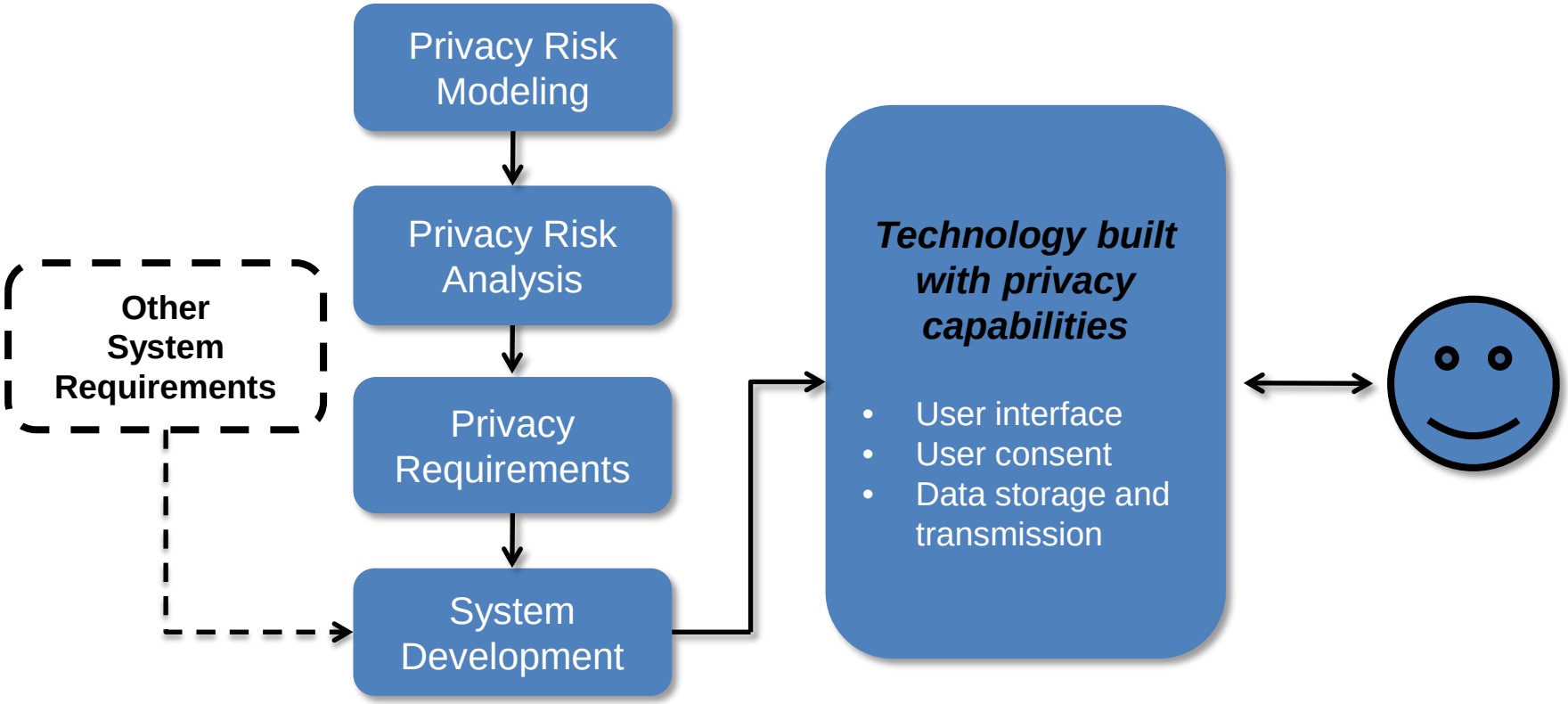


Risk = Threat × Vulnerability × Harm


iTL
VOTE
VOTE


Objectives
Risk Analysis
Requirements
Design
Evaluation Criteria
System

Security-analogous Privacy Engineering Model

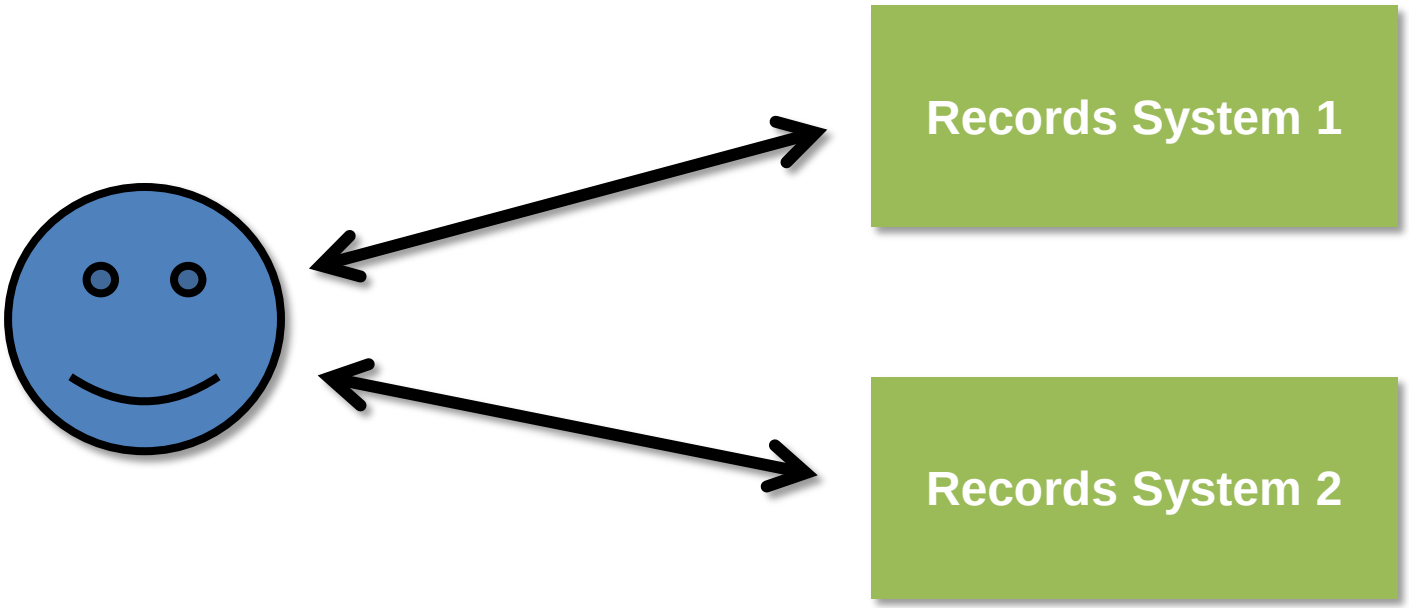


Security Analogy Divergences

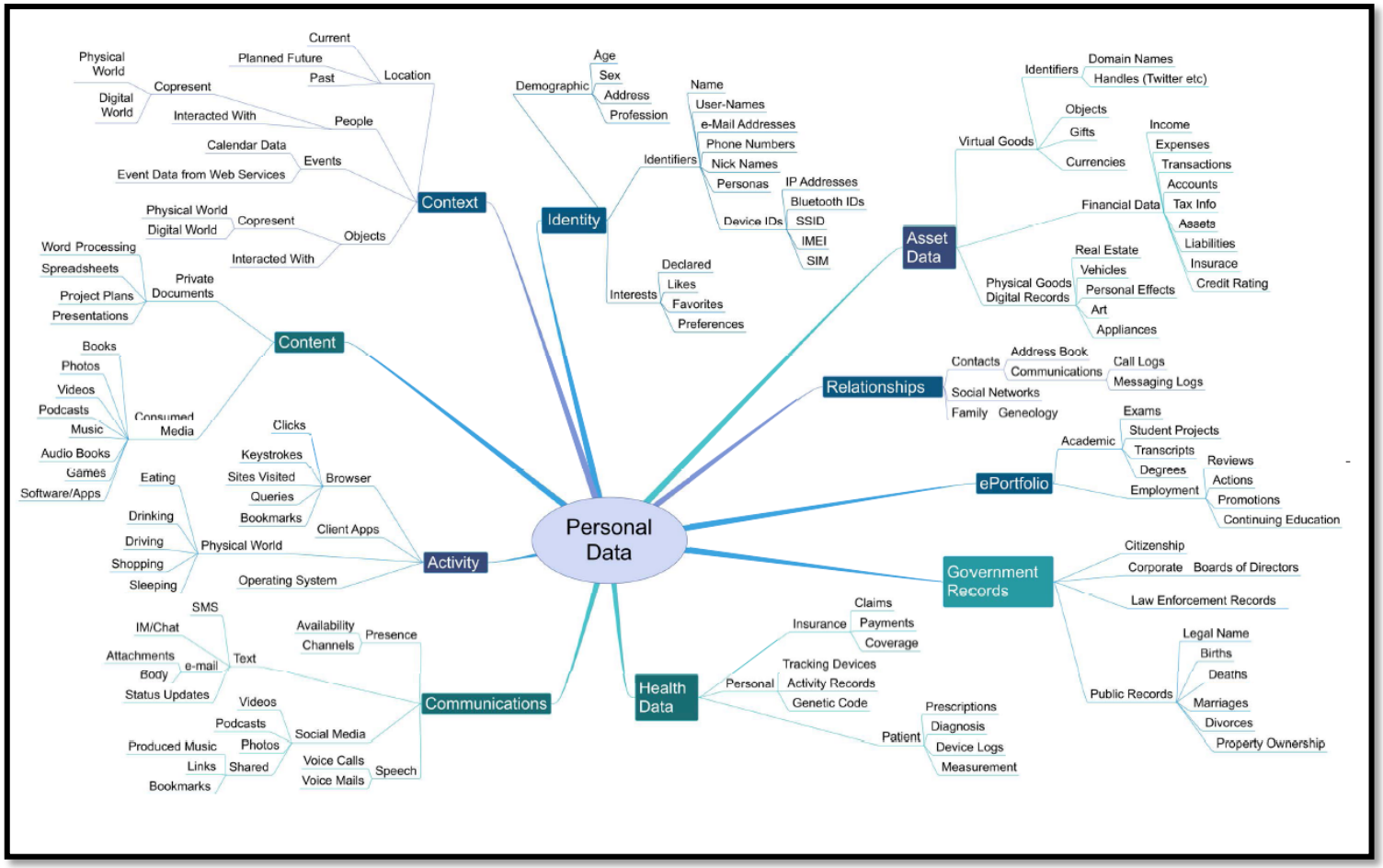
- **Vulnerability:** Perceived in security as a deficit in design. But design elements that open systems up to privacy risks are often integral to proper functioning of that system (data collection, analysis, etc.)
- **Threat:** Implies a malicious act or purposeful attack, but many privacy risks are unintended
- **Harm:** Focus on breaches of confidentiality of PII won't reach the full spectrum of potential harms in privacy.
- **Objectives:** Security has CIA, but what would be the equivalent, desirable outcomes for privacy engineering?

FIPPs at the Foundation

Rules for mutual decision-making about the nature and use of an individual's record held by an organization

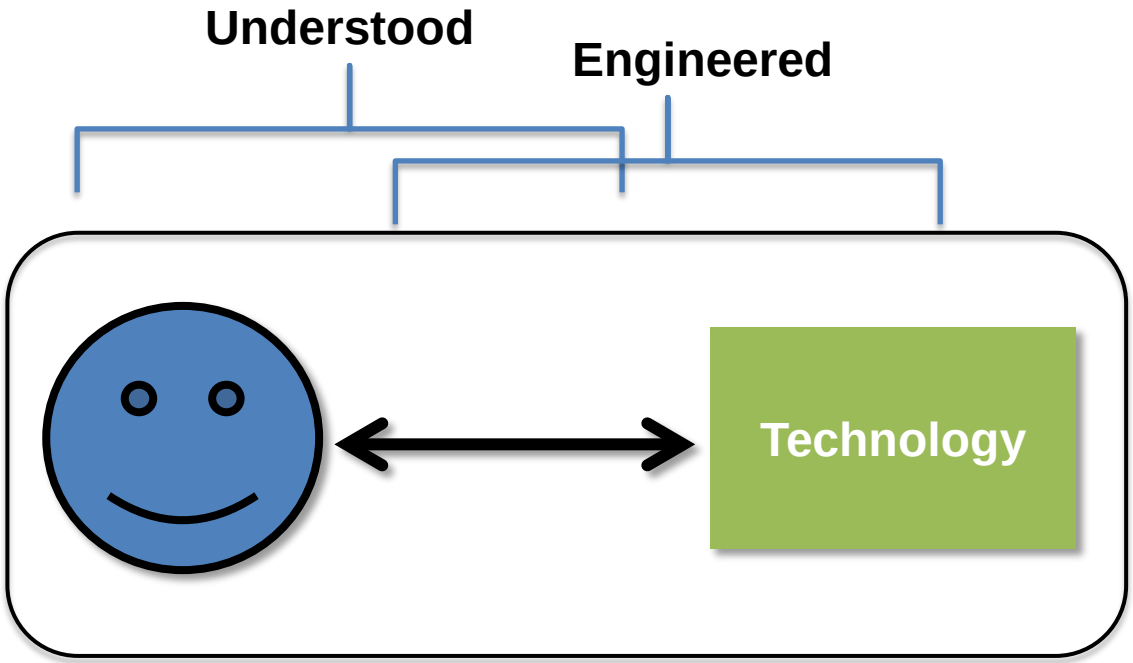


Today's Dynamic Environment



Source: World Economic Forum, *"Rethinking Personal Data: Strengthening Trust,"* May 2012

For effective privacy, systems must be understood, and be engineered to meet privacy requirements

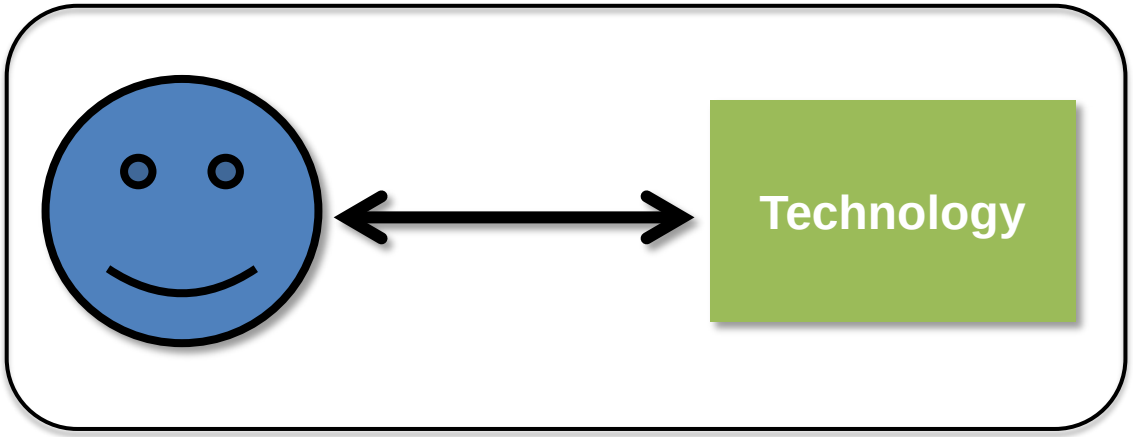


Goal of Privacy Engineering

- To develop reusable tools and practices to facilitate the creation and maintenance of systems with strong privacy postures.
- These reusable tools and practices:
  - Provide engineers with system design tools, terminology, and techniques that can be used to create systems that mitigate the risk of privacy harm.
  - Allow system owners and developers to proactively address privacy risks in a measured way within their overall risk management process.
  - Allow system owners to evaluate the privacy posture of existing systems.

Engineer for Individuals

A system is more than technology: it's the user and their interactions with the technology



Workshop Goals

- Define scope of problem
- Discuss possible approaches
- Consider appropriate terminology
- Next steps for building a privacy engineering model

Post Workshop

- Report out of the Workshop (basis for a NISTIR)
- Solicit comments
- Workshop 2
  - Refine the draft NISTIR
- Avoid pillow fights!