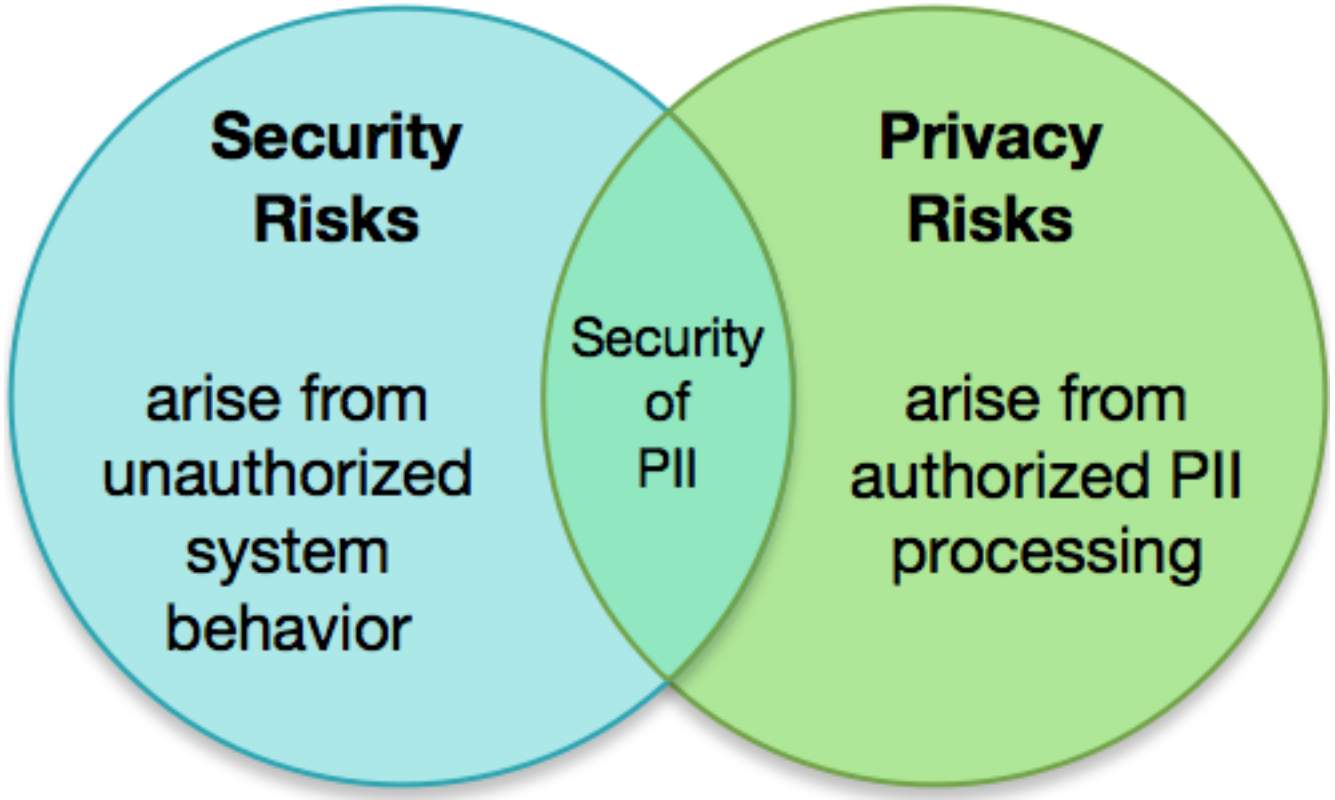
Privacy in Connected Vehicle Environments

Information Security and Privacy Relationship



- There is a clear recognition that confidentiality of PII plays an important role in the protection of privacy
- Individual privacy cannot be achieved solely by securing PII

Barriers to IoT Security/Privacy Market Factors

Market Access	Cheap processing readily available, such as: Arduino, Raspberry PI, Quark, many more
	An idea, a few dollars, and access to a maker space (with tools such as 3D printers) and service such as GoFundMe, Kickstarter, IndieGoGo, all can lead to quick prototypes
	These nascent entrepreneurs often lack security and privacy expertise or resources to implement security and privacy
First to market	Developers push for first to market or early to market in blooming market segment
	Focus on features and functionality first, tying user into ecosystem
	Massive price pressure (more so in consumer vs industrial), shaving fractions of pennies off of supply chain and hardware costs
Diversity	Vendors often use different hardware, software, APIs, third-party service providers, and patching mechanisms

NIST

DoT Smart Cities/Connected Vehicles Pilots

Where's the guidance on privacy for smart cities and CV deployments?

Working with Department of Transportation:

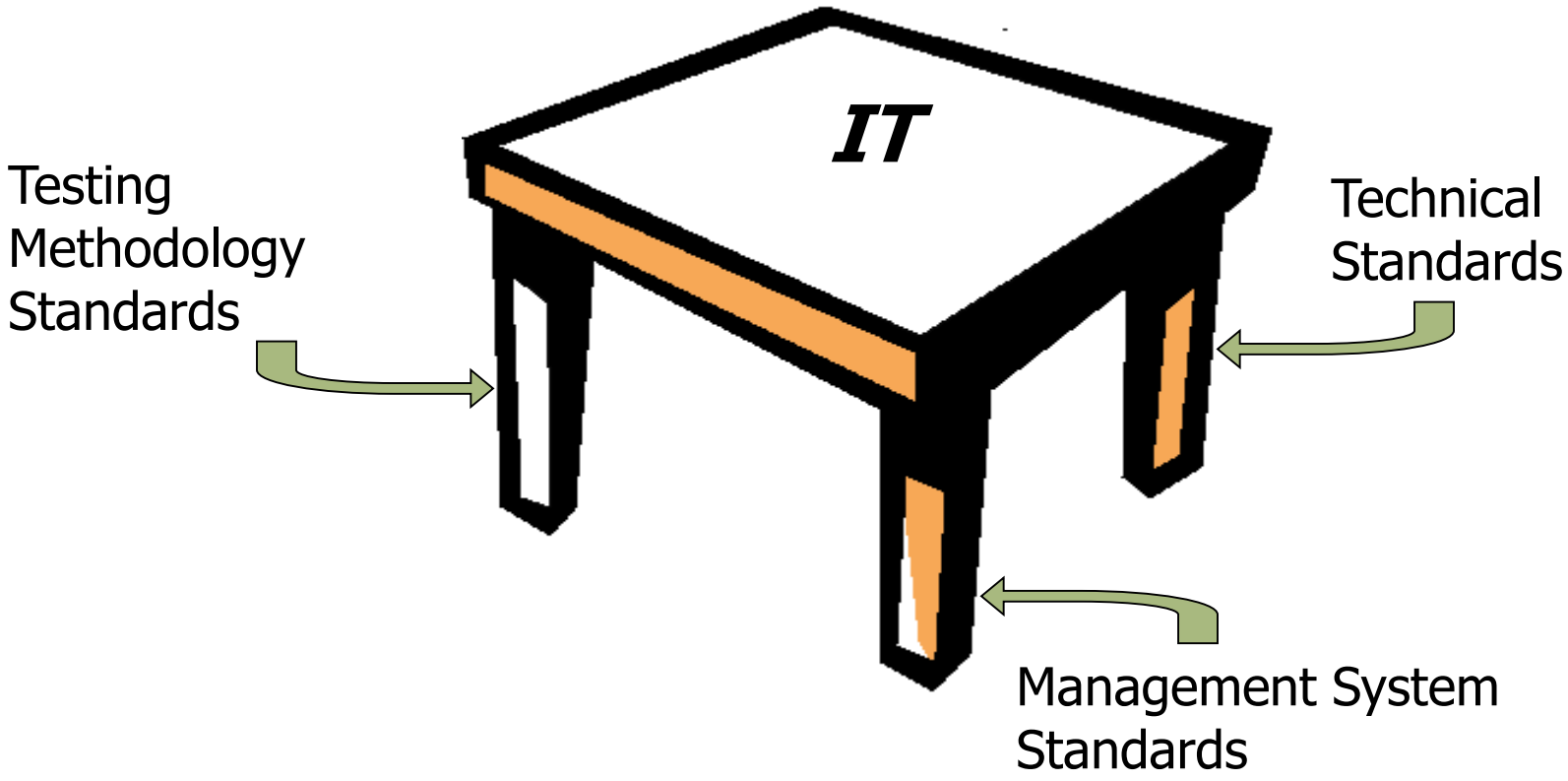
- Ann Arbor Connected Vehicle Test Environment
- Connected Vehicle Pilot Deployment Program
  - Cheyenne, WY
  - NYC, NY
  - Tampa, FL

Lessons Learned from the Pilots: Privacy Challenges in CV Environments

- System boundaries discussion, de-centralized data processing functions
- Re-identification risks, especially with combined information
- Limited user interfaces: how to inform individuals?

Standards

Categories of IT Standards



Examples

- ISO/IEC 27000-series, Information security management systems [management system standard]
- ISO/IEC 18033-3:2010, Information technology -- Security techniques -- Encryption algorithms -- Part 3: Block ciphers [technical standard]
- ISO/IEC 24759:2014, Information technology -- Security techniques -- Test requirements for cryptographic modules [testing methodology standard]

ISO/IEC 29100 FRAMEWORK FOR PROTECTION OF PII

- One of the foundational privacy management systems standards
- Includes
  - a risk management process component; and
  - a set of principles to adhere to (aligned with the Fair Information Practice Principles)
- No strong relationship between risk management and principles adherence

NIST

ISO/IEC 27001 INFORMATION SECURITY MGMT SYSTEMS

- Focus is on measurable security objectives – flexibility is allowed in achieving the outcome
- Risk management is linked to achievement of objectives
- Avoids prescriptive implementations

  A.10.1.1: A policy on the use of cryptographic controls for protection of information shall be developed and implemented

NIST

Next steps for privacy standards in smart mobility?

Resources

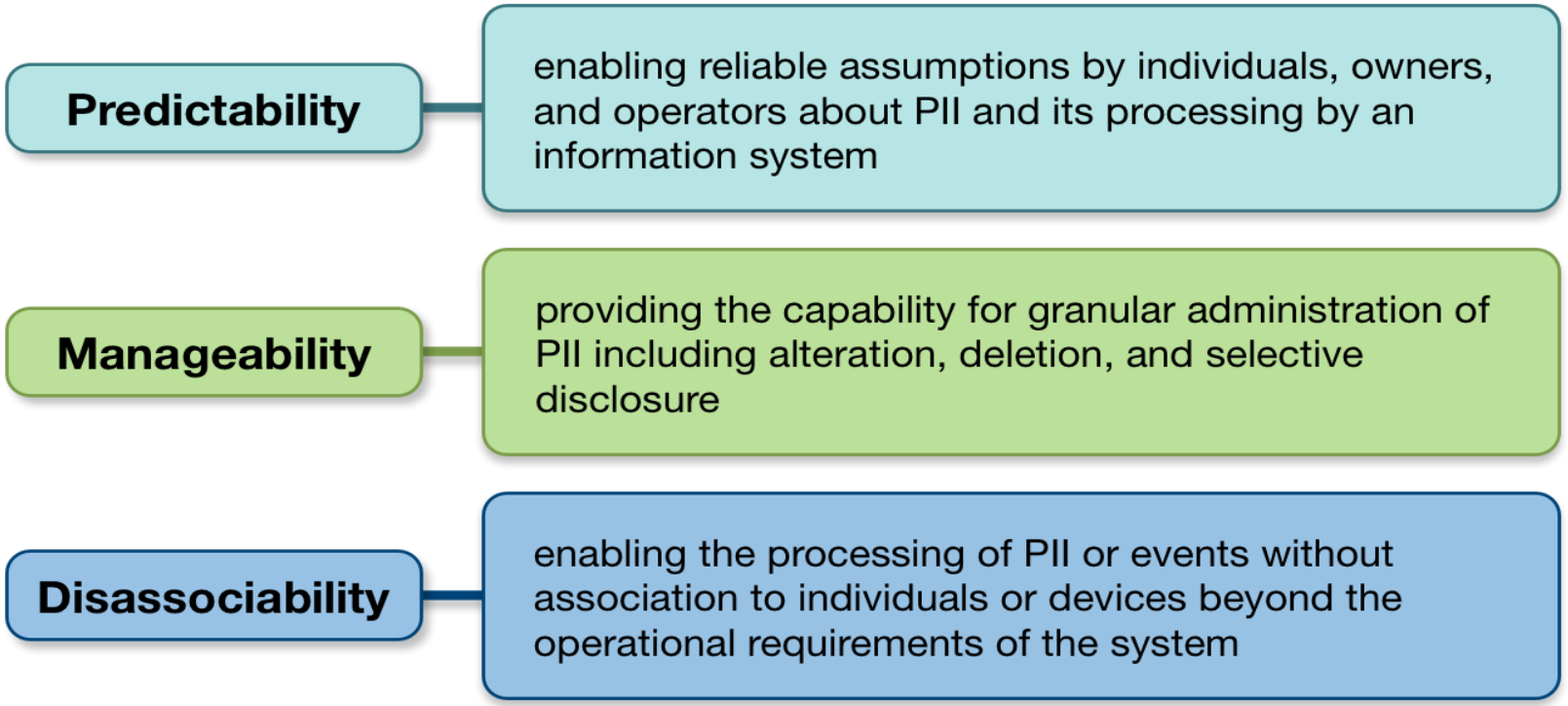
Ellen Nadeau
ellen.nadeau@nist.gov

NIST Privacy Engineering Website
https://www.nist.gov/programs-projects/privacy-engineering

Additional Resources

NIST Privacy Engineering Objectives

- Design characteristics or properties of the system
- Support policy through mapping of system capabilities
- Support control mapping



NIST Working Model for System Privacy Risk

Privacy Risk Factors: Likelihood |Problematic Data Action |Impact

Likelihood is a contextual analysis that a data action is likely to create a problem for a representative set of individuals

Impact is an analysis of the costs should the problem occur

Note: Contextual analysis is based on the data action performed by the system, the PII being processed, and a set of contextual considerations