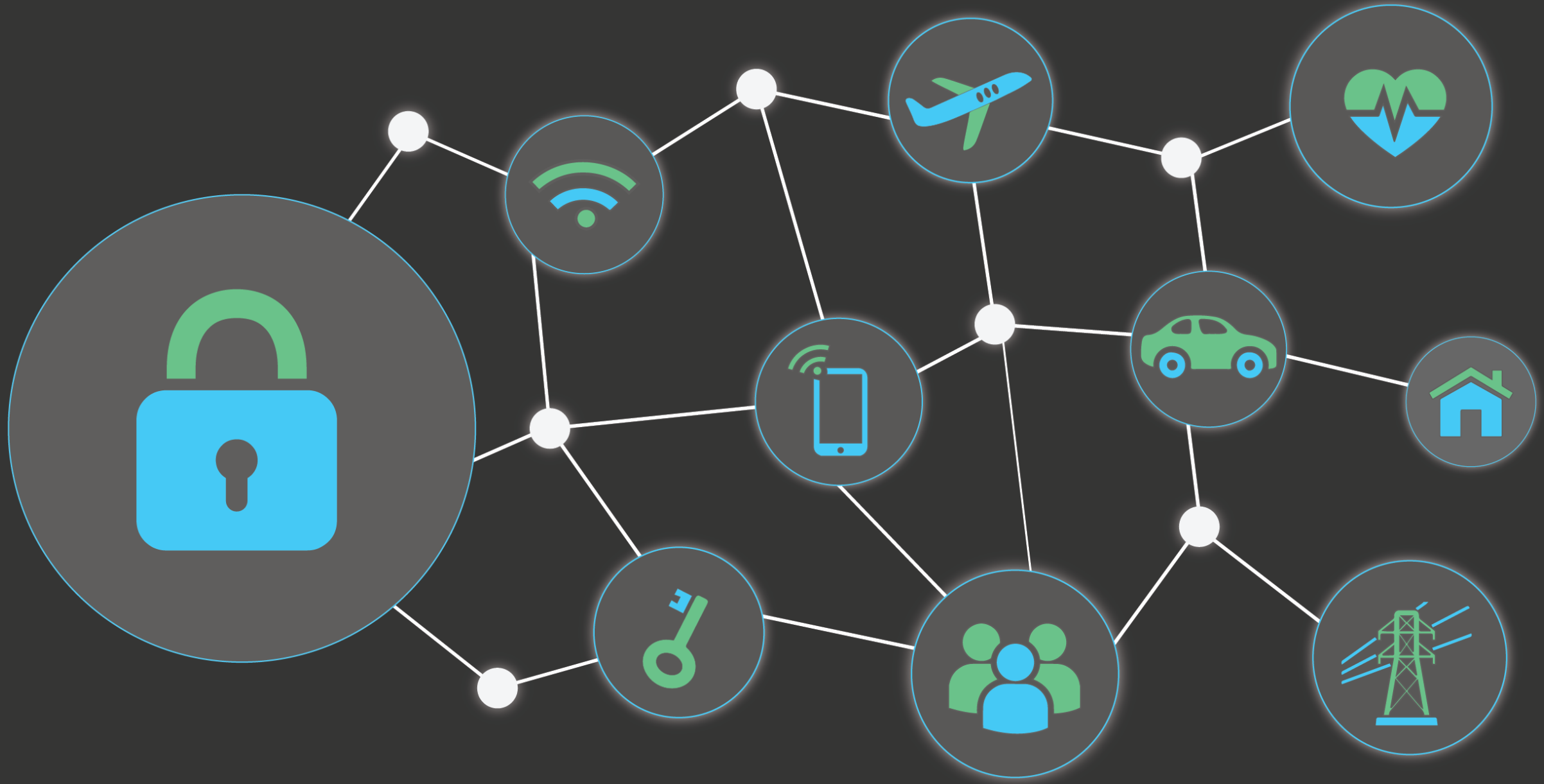


IoT Privacy & Security Risk

NIST Privacy Engineering & Cybersecurity for IoT Programs

March 29, 2018

NIST Cybersecurity for IoT Program

Cultivate trust in IoT & foster an environment that enables innovation on a global scale.

About the Program

NIST's **Cybersecurity for IoT Program** develops & applies standards, guidelines, and related tools to improve the cybersecurity of connected devices and the environments in which they are deployed.

By collaborating with stakeholders across government, industry, international bodies, and academia, the program aims to cultivate trust and foster an environment that enables innovation on a global scale.

Security & Privacy Considerations for Federal Agencies

NIST is preparing a document on IoT security and privacy risk considerations for federal government. This effort is aimed at considering a practical approach to IoT security and privacy risk management.

Next steps

- Attending roundtables to gather industry feedback throughout the development process.
- Collecting input on discussion draft at iotsecurity@nist.gov

An Introduction to Managing IoT Cybersecurity & Privacy Risk

NIST is preparing a document to help federal agencies manage IoT cybersecurity and privacy risks. This guidance is aimed at considering a practical approach to IoT cybersecurity and privacy risk management.

The document will cover the following topics:

- Fundamental IoT concepts and terminology
- Typical differences in cybersecurity and privacy risk for IoT systems versus traditional IT systems
- Recommendations for addressing IoT cybersecurity and privacy risk enterprise-wide (e.g., policies, plans, strategies, processes)
- Considerations for selecting and using technical controls to mitigate IoT cybersecurity and privacy risk
- Worked examples to illustrate differences in managing IoT risk versus non-IoT risk
- Basic cybersecurity and privacy controls for manufacturers to consider providing in their IoT products

NIST Drivers for Privacy Engineering

Advancement of trustworthy systems

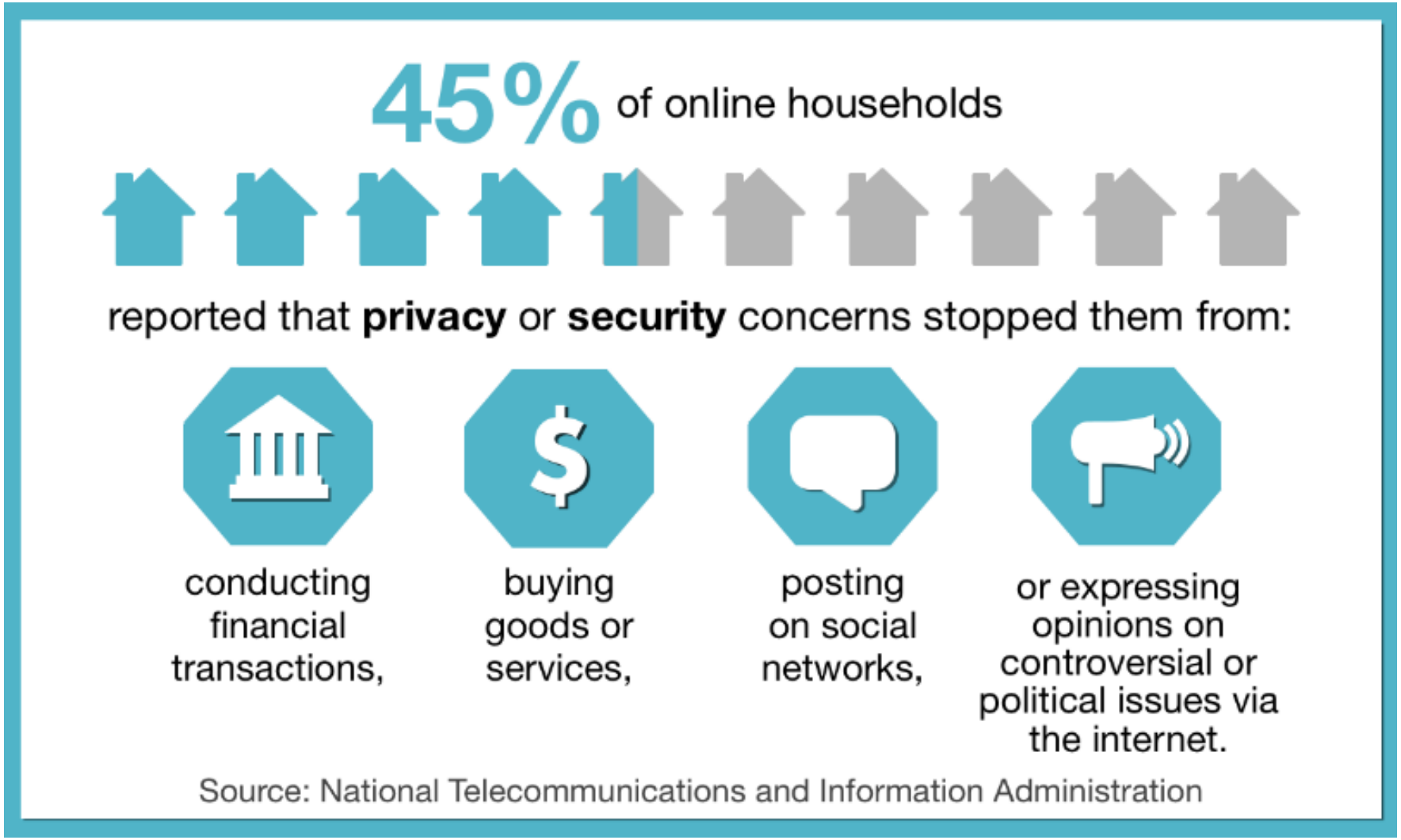
- Multiple attributes of trustworthiness include security, safety, reliability, etc.
- Privacy must be considered one of the attributes
- Privacy needs a body of guidance for repeatable and measurable approaches similar to other attributes

OMB Circular A-130 July 2016 update

- Manage privacy risk beyond compliance with privacy laws, regulations, and policies
- Apply the NIST Risk Management Framework to privacy programs

4

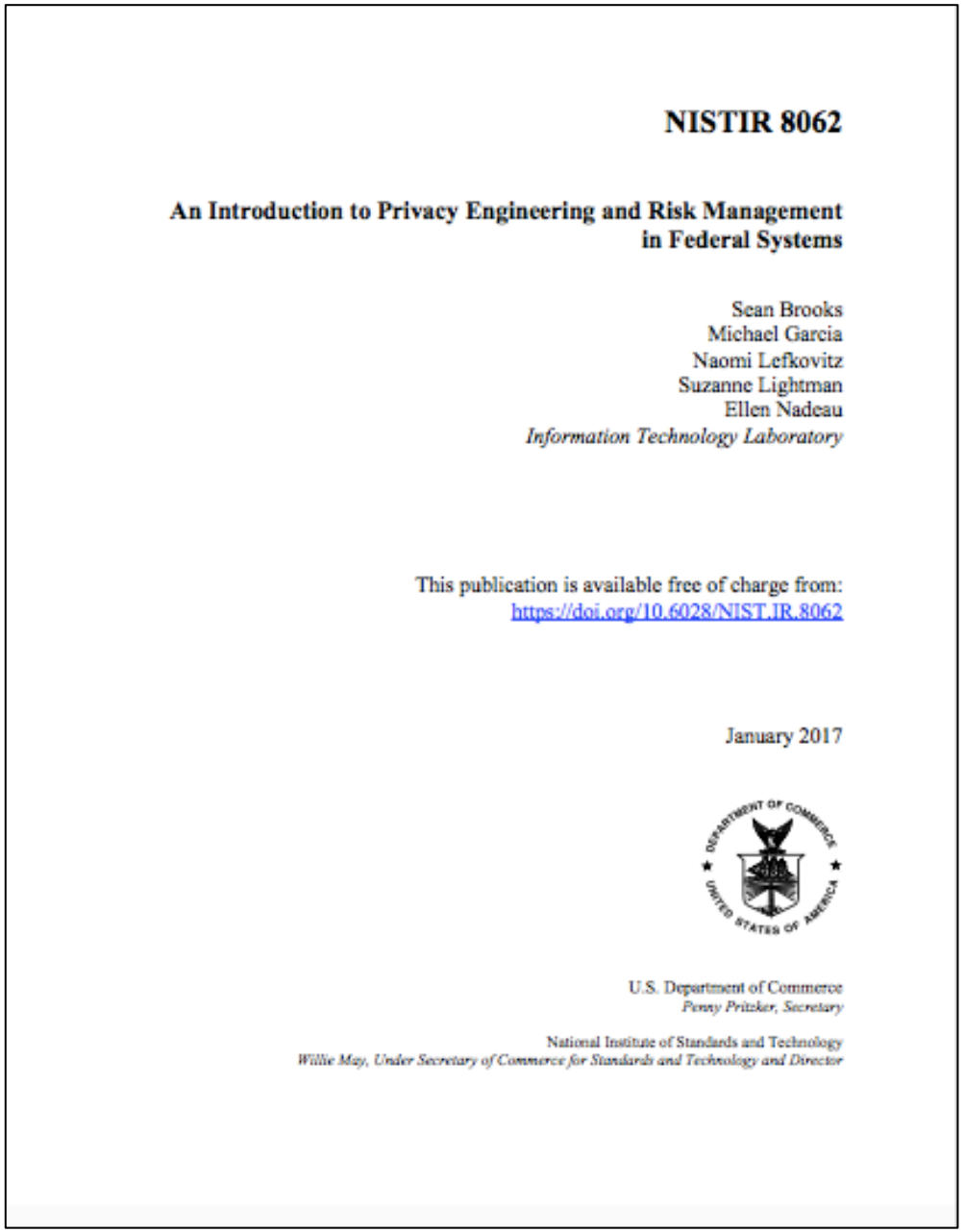
Friction in Our Digital World



July 2015 data collected for NTIA at https://www.ntia.doc.gov/blog/2016/first-look-internet-use-2015

NIST Internal Report 8062

An Introduction to Privacy Engineering and Risk Management in Federal Systems



NISTIR 8062

An Introduction to Privacy Engineering and Risk Management in Federal Systems

Sean Brooks
Michael Garcia
Naomi Lefkovitz
Suzanne Lightman
Ellen Nadeau
Information Technology Laboratory

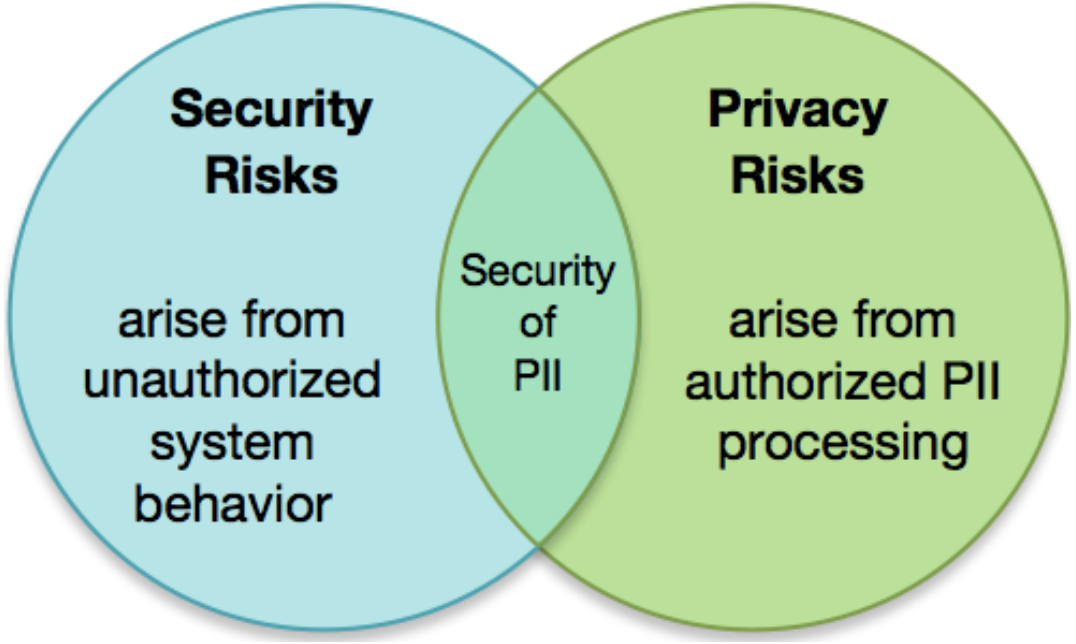
This publication is available free of charge from:
https://doi.org/10.6028/NIST.IR.8062

January 2017

U.S. Department of Commerce
Penny Pritzker, Secretary

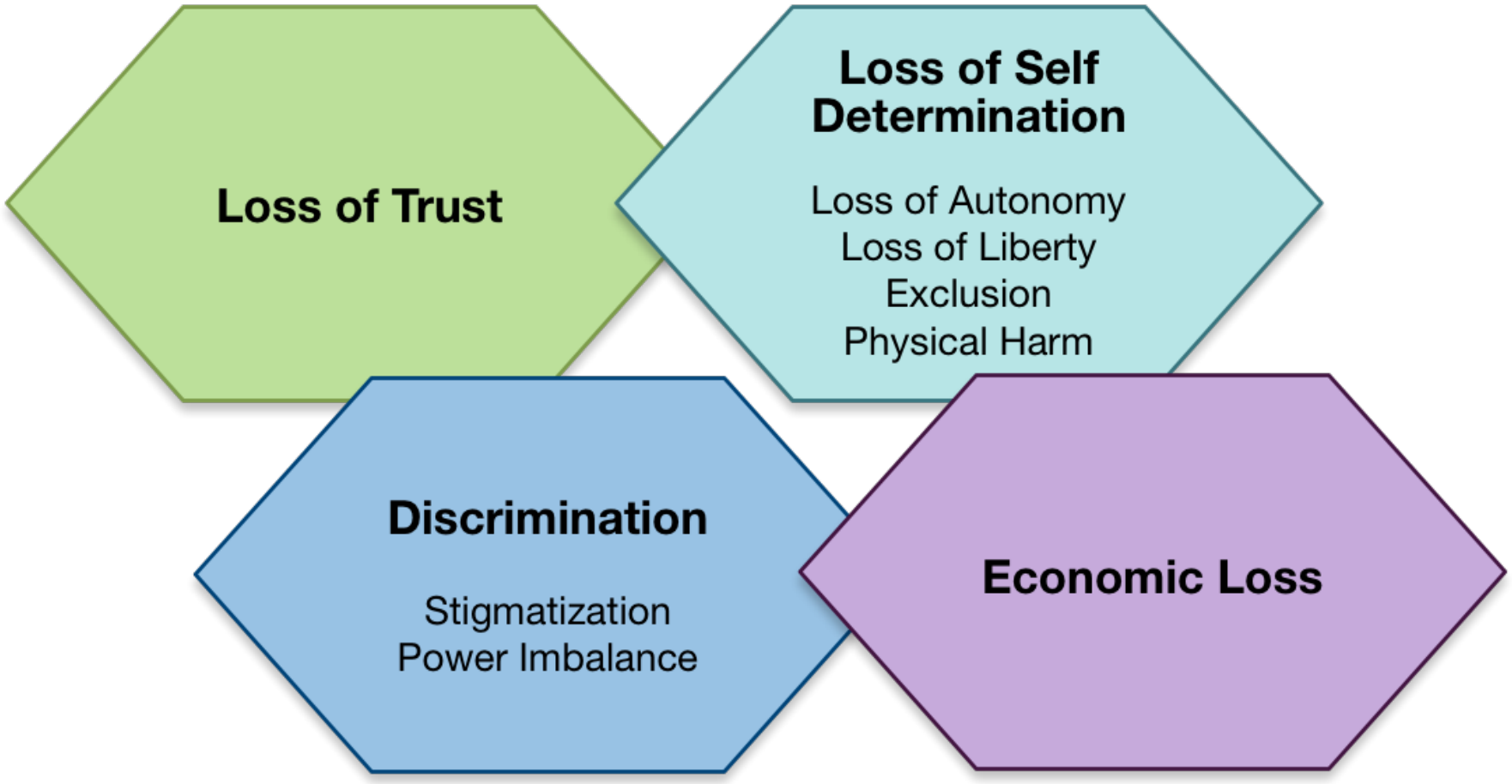
National Institute of Standards and Technology
Willie May, Under Secretary of Commerce for Standards and Technology and Director

NISTIR 8062: Information Security and Privacy Relationship



- There is a clear recognition that security of PII plays an important role in the protection of privacy
- Individual privacy cannot be achieved solely by securing PII
- Authorized processing: system operations that handle PII (collection –disposal) to enable the system to achieve mission/business objectives

Processing PII Can Create Problems for Individuals



NIST Privacy Risk Model

Privacy Risk Factors:
Likelihood |Problematic Data Action |Impact

Framing the Discussion

NIST Cybersecurity for IoT Program Principles

Outcome-Based Approach.

Risk-Based Understanding.

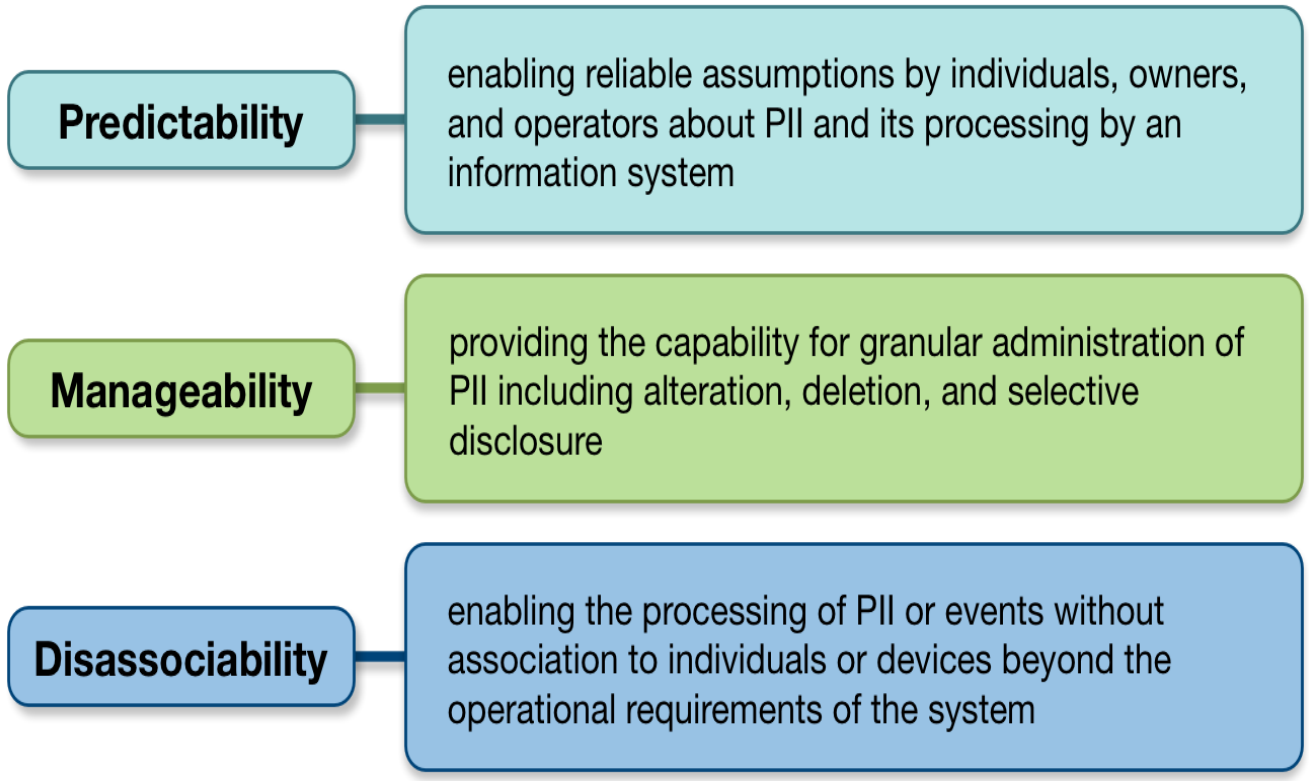
No One Size Fits All.

Ecosystem of Things.

Stakeholder Engagement.

NIST Privacy Engineering Objectives and an Outcome-based Approach for an IoT Ecosystem

System properties that support individuals' privacy



- How can the ecosystem enable reliable assumptions about data processing?
- How much manageability of data does this ecosystem need?
- How can data be dissociated from individuals or devices while still permitting functionality in the ecosystem?

12

Privacy Challenges in IoT

NIST Privacy Engineering Objective	Definition	IoT Data Actions	Potential Privacy-related Problems for Individuals
Predictability	Enabling reliable assumptions by individuals, owners, and operators about PII and its processing by a system.	It may be difficult for individuals to know what data devices are collecting about them and how the information will be processed after collection, especially if user interfaces are limited. De-centralized data-processing functions can contribute to complex automated systems and data flows IoT systems can act on human behavior directly. For example, traffic systems can influence or control where vehicles move. Environmental systems can influence behavior or movement in buildings.	When individuals lack awareness about what is happening in a system it can create problems around loss of self-determination: • Individuals may have difficulty participating in meaningful decisions about the use of their information • May create “chilling effects” on ordinary behavior and activity.

Privacy Challenges in IoT

NIST Privacy Engineering Objective	Definition	IoT Data Actions	Potential Privacy-related Problems for Individuals
Manageability	Providing the capability for granular administration of PII including alteration, deletion, and selective disclosure.	The ubiquity of IoT sensors and devices in public and private environments can contribute to the aggregation and analysis of enormous amounts of data about individuals. Even non-identifying information can become identifying when combined with other information.	Information can be deeply sensitive and provide detailed insights into individuals' lives in ways that individuals did not anticipate and do not find beneficial. Decentralization can contribute to difficulty in ensuring the quality and management of data and could lead to inaccurate or damaging determinations about individuals or difficulty in providing redress.

Privacy Challenges in IoT

NIST Privacy Engineering Objective	Definition	IoT Data Actions	Potential Privacy-related Problems for Individuals
Disassociability	Enabling the processing of PII or events without association to individuals or devices beyond the operational requirements of the system.	Devices may collect information indiscriminately even when information about individuals is not necessary for the purpose of the system. Securing data is predominantly focused on data at rest in a system or data in motion between two known parties. Decentralizing data processing may be complicated by the low-power and low-processing capabilities required by many sensor use cases.	Processing identifying information even when not operationally necessary can increase the capability for tracking and profiling individuals. In a de-centralized system, encryption that relies on known parties/devices (as opposed to just trusted parties/devices) can create information-rich data trails about individuals.

Discussion

(1) Are there additional privacy risks pertinent to IoT?

NIST Cybersecurity for IoT Program Principles

Outcome-Based Approach.

Risk-Based Understanding.

No One Size Fits All.

Ecosystem of Things.

Stakeholder Engagement.

(2) Input on an outcome-based approach

(3) Input on a risk-based approach focused on the IoT ecosystem

(4) Would use cases be helpful?

Contact

@NISTcyber

privacyeng@nist.gov
iotsecurity@nist.gov

https://www.nist.gov/programs-projects/privacy-engineering
https://www.nist.gov/programs-projects/nist-cybersecurity-iot-program

Additional Resources

High-Level Overview of Planned Draft

While it is being drafted and is subject to change, the current outline includes:

- **Introduction**
  - Purpose and Scope
- **Major Cybersecurity and Privacy Risk Factors**
  - Diversity of IoT System Capabilities
  - Management and Maintenance of IoT Systems
  - IoT System Complexity
  - Built-In Cybersecurity and Privacy Controls
  - Potential Consequences of Compromise
- **Addressing the Risk Factors at the Enterprise Level**
  - Governance
  - Risk Management
  - Asset Management
  - Incident Handling
- **Addressing the Risk Factors for Individual IoT Systems**
  - Potential Issues with Achieving Cybersecurity and Privacy Outcomes
  - Compensating Controls
- **Worked Examples**
- **Cybersecurity and Privacy Control Considerations for IoT System Manufacturers**

NIST Cybersecurity for IoT Program Principles

Outcome-Based Approach.

We embrace the Cybersecurity Framework's outcome-based approach. We specify desired cybersecurity outcomes, not how to achieve those outcomes, which allows organizations to choose the best solution for each IoT device and/or their enterprise environment.

Risk-Based Understanding.

IoT capabilities, behaviors, deployment environments, and other characteristics can affect cybersecurity risk. Our approach to managing this risk is rooted in an understanding of how IoT can affect it.

No One Size Fits All.

Each organization has its own risk tolerance and mission needs, and no one set of controls will address the wide range of cross-industry and cross-vertical needs and use cases. There is no one-size-fits-all approach to managing IoT cybersecurity risk.

Ecosystem of Things.

Recognizing that no device exists in a vacuum, the Program takes an ecosystem approach to IoT cybersecurity. For many devices, much of the functionality happens outside the device—not all the security is on the device itself. As such, we look at the entire ecosystem, not just endpoints.

Stakeholder Engagement.

The Program works with a wide range of stakeholders to advance IoT cybersecurity. This includes collaborating with stakeholders to drive security, providing the necessary tools, guidance, standards, and resources.

Aligning the Circular A-130 FIPPs to the Privacy Engineering and Security Objectives

NISTIR 8062: Figure 8