# NIST Privacy Engineering:
## Risk Model and Assessment

NIST Information Security and Privacy Advisory Board
June 28, 2017

# Trustworthy Systems: Foundational to a Digital Society

## What makes systems trustworthy?

- Multiple attributes of trustworthiness include security, safety, reliability, etc.
- Privacy must be considered one of the attributes

## How can we know if systems are trustworthy?

- Repeatable and measurable approaches help provide a sufficient base of evidence
- Privacy needs a body of guidance for repeatable and measurable approaches similar to other attributes of trustworthiness

NIST

# Friction in Our Digital World

45% of online households reported that privacy or security concerns stopped them from:*

- Conducting financial transactions;
- Buying goods or services;
- Posting on social networks; or
- Expressing opinions on controversial or political issues via the Internet.

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

# Primary Federal Driver

OMB July 2016 update to Circular A-130:

- Agencies' obligations with respect to managing privacy risk and information resources extend beyond compliance with privacy laws, regulations, and policies
- Agencies must apply the NIST Risk Management Framework in their privacy programs

# Federal Security and Privacy Legal Foundations

## FISMA – Federal Information Security Management Act

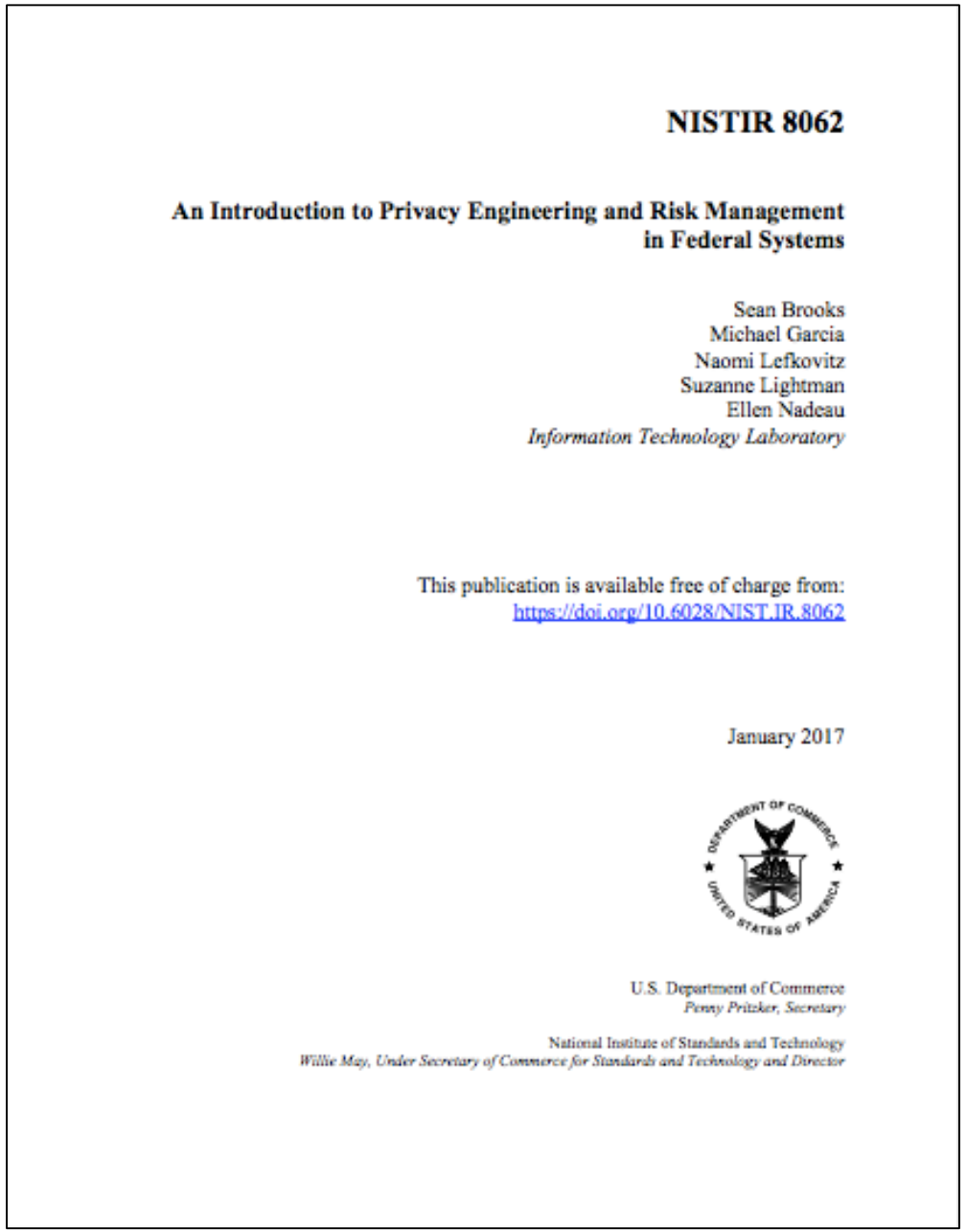
- Requires implementation of “information security protections commensurate with the risk and magnitude of the harm”

## The Privacy Act of 1974

- Establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies.

# NISTIR 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

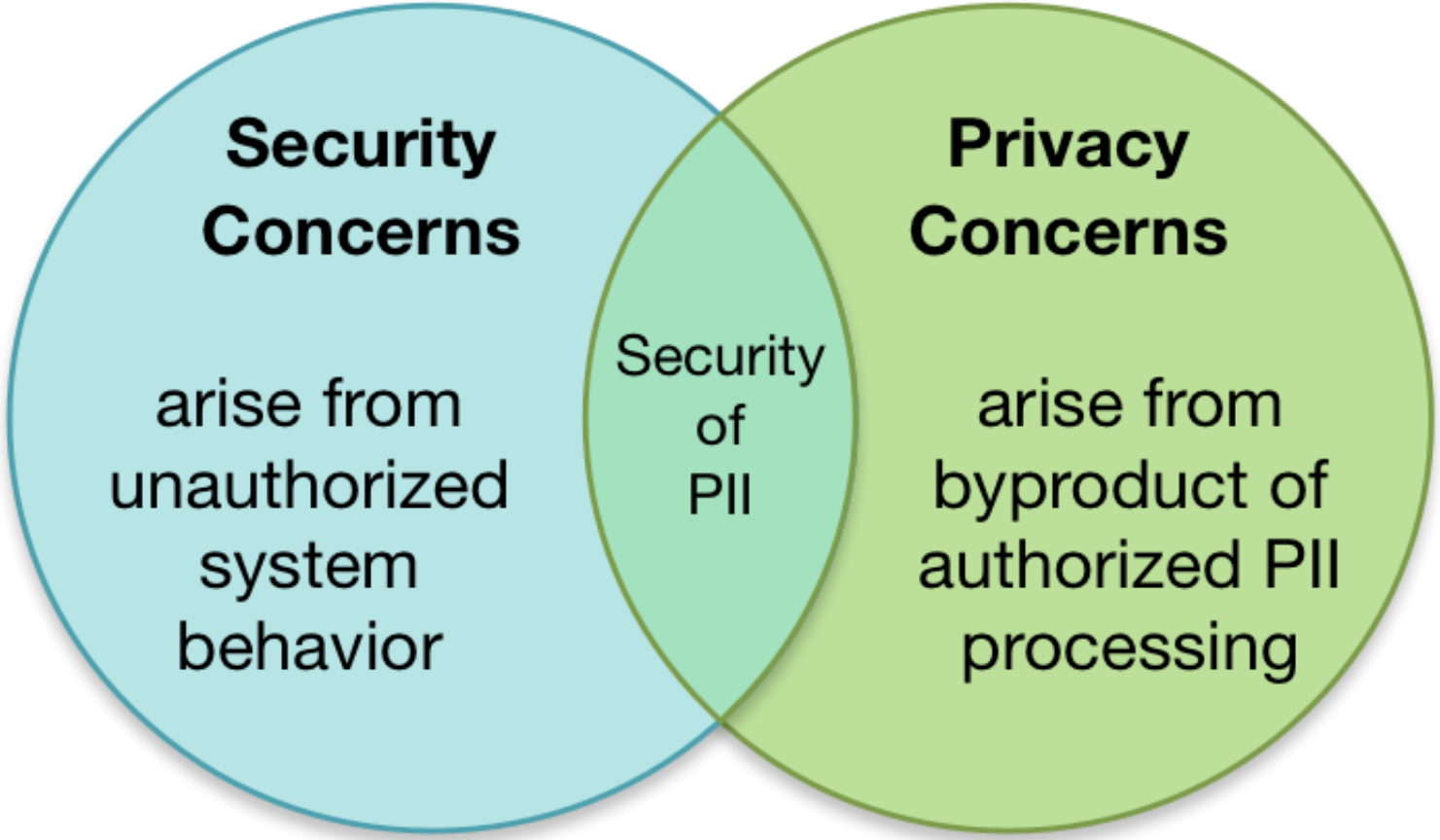
January 2017

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*

NIST

# Information Security and Privacy: Boundaries and Overlap



# Risk Model

Risk models define the *risk factors* to be assessed and the relationships among those factors.

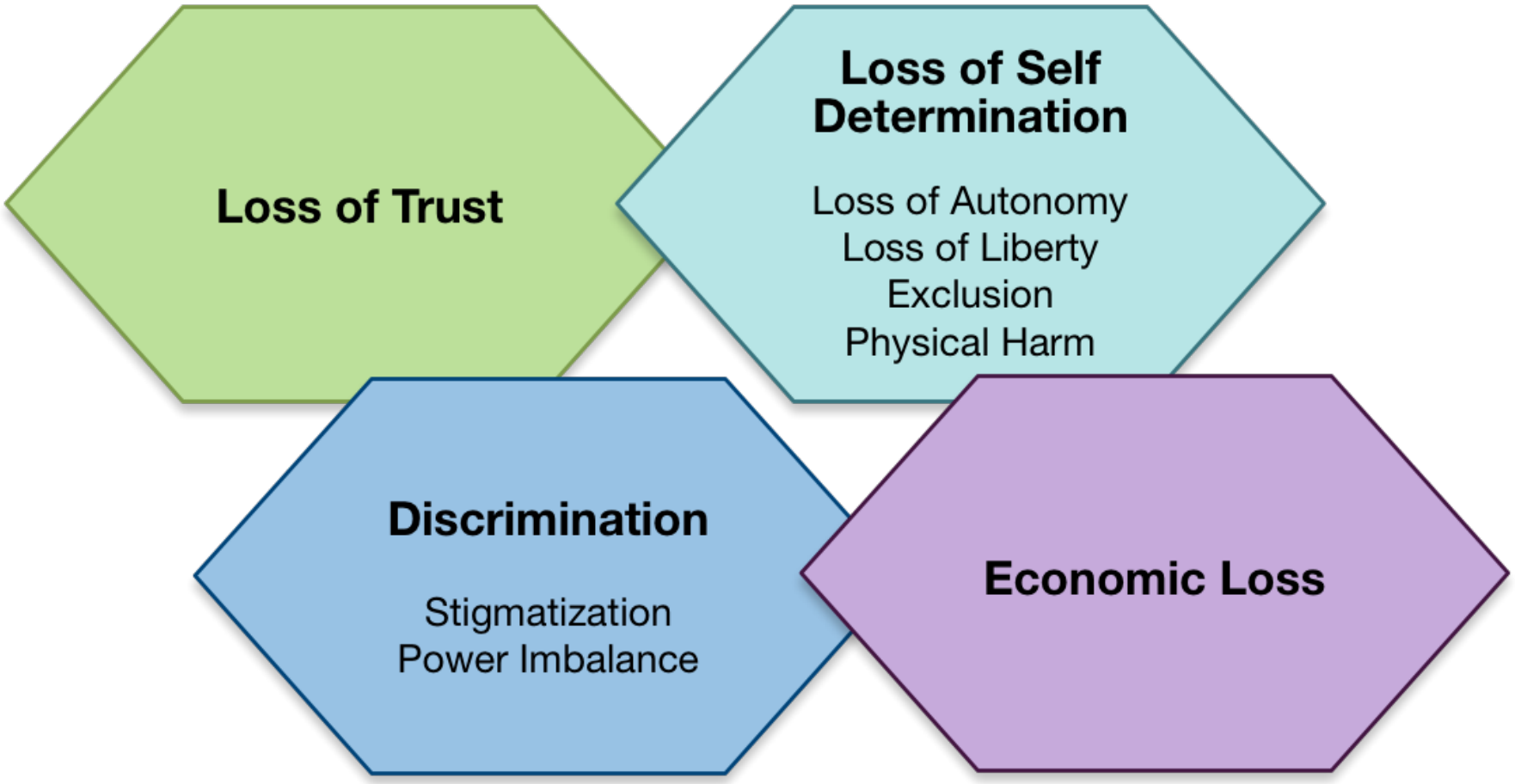
Risk factors are inputs to determining levels of risk.

# Security Risk Model

Risk factors:

Likelihood |Vulnerability | Threat | Impact

# Processing PII Can Create Problems for Individuals



# NIST Working Model for System Privacy Risk

**Privacy Risk Factors: Likelihood |Problematic Data Action |Impact**

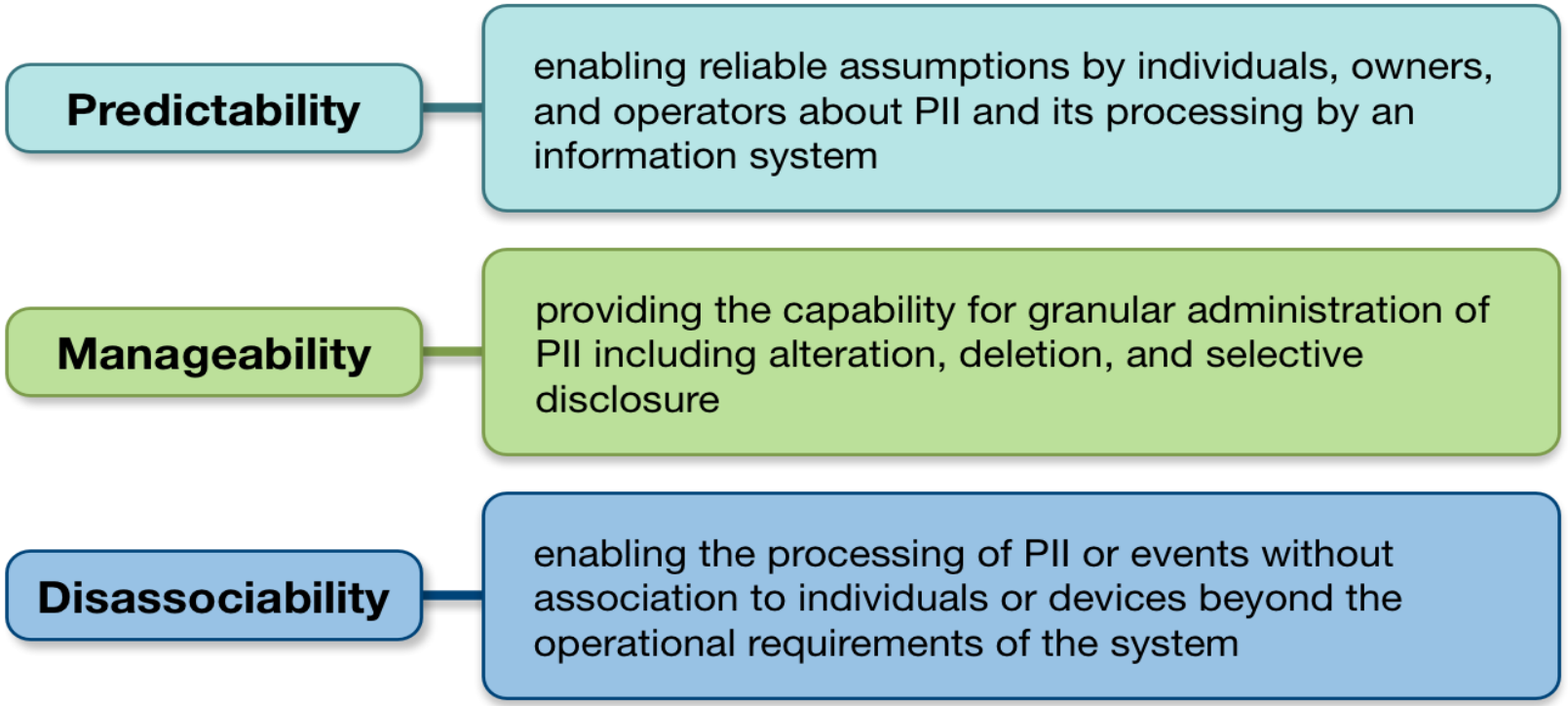
**Likelihood** is a contextual analysis that a data action is likely to create a problem for a representative set of individuals

**Impact** is an analysis of the costs should the problem occur

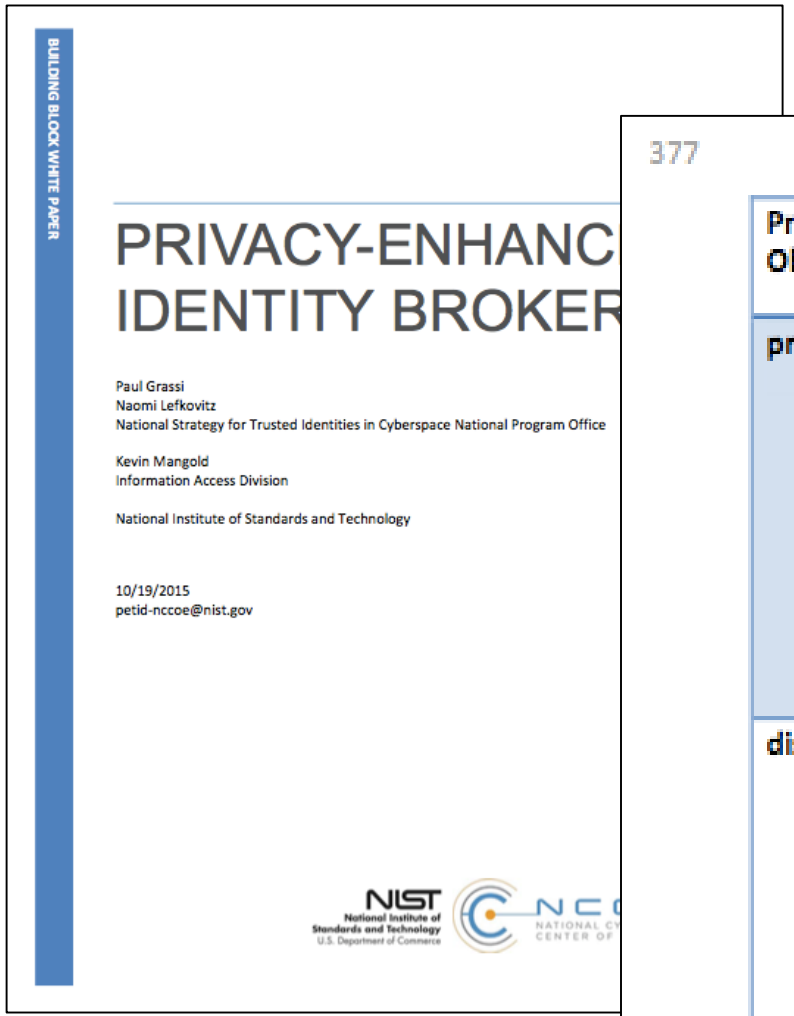
*Note: Contextual analysis is based on the data action performed by the system, the PII being processed, and a set of contextual considerations*

# NIST Privacy Engineering Objectives

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



# A Driver for System Capabilities



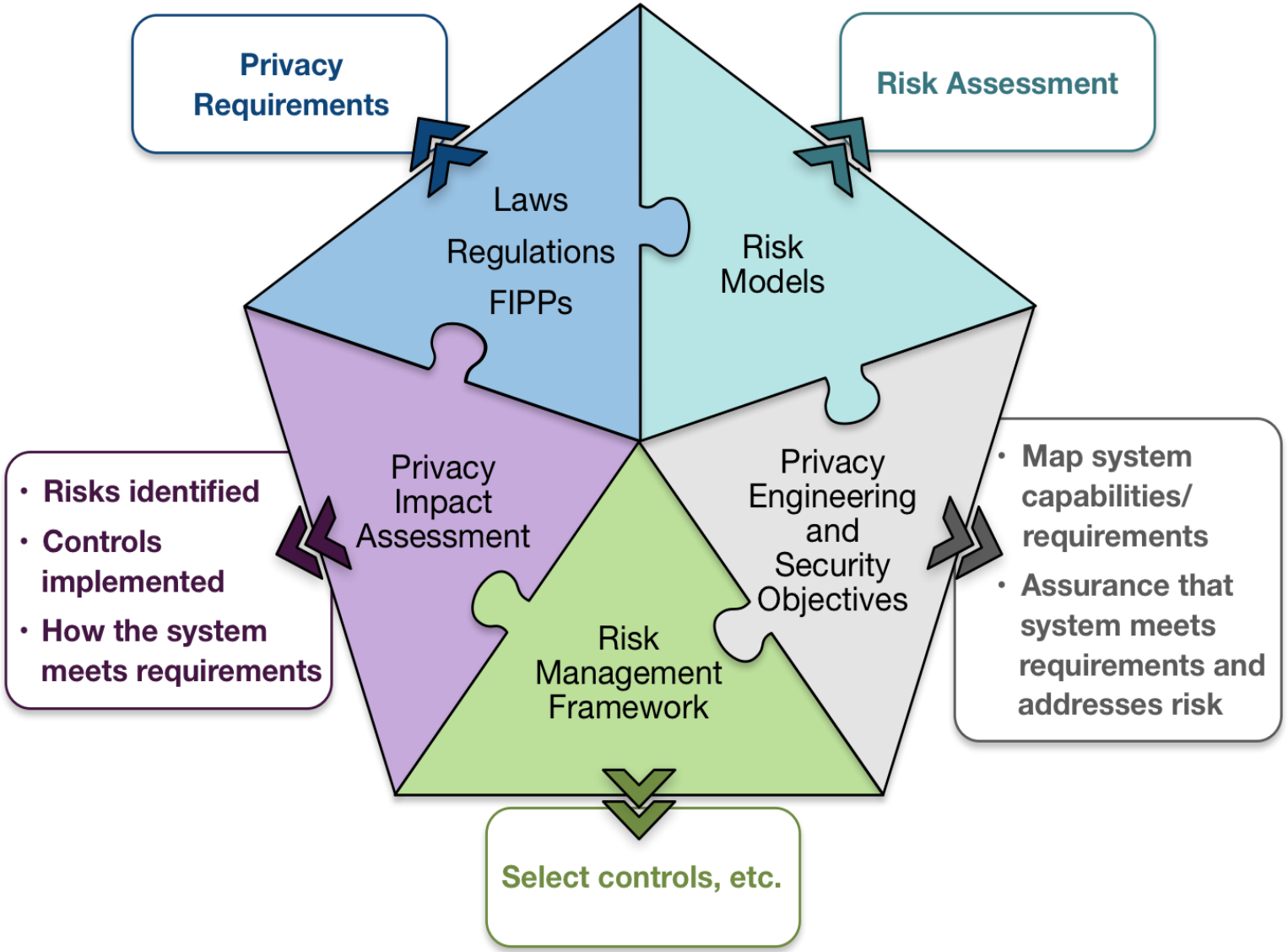

377

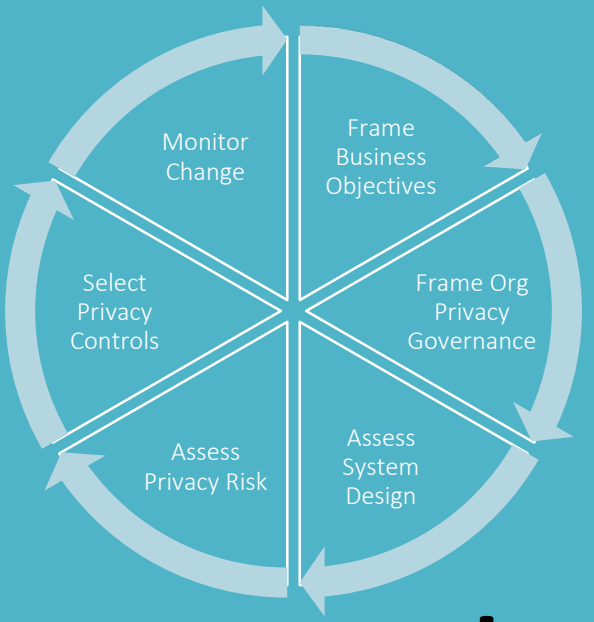
Table 4 - Privacy Objectives

| Privacy Engineering Objective | Example Capability(ies) |
|---|---|
| **predictability** | • Enables user, RP, IdP and identity broker assumptions that identity broker does not have access to user identity attributes.<br>• Enables user, RP, IdP and identity broker assumptions that IdP cannot process information about user's relationship with the RP.<br>• Enables user, RP, IdP and identity broker assumptions that RP cannot process information about user's relationship with the IdP. |
| **disassociability** | • The identity broker can transmit identity attributes from an IdP to an RP without being able to access them.<br>• The RP can accept an authentication assertion and identity attributes without associating a user to an IdP.<br>• The IdP can transmit an authentication assertion and identity attributes without associating a user to an RP. |

378

# Putting It All Together






# Privacy Risk Assessment Methodology

## Applying the Privacy Risk Model

# Primary Benefits

# Frame Business Objectives

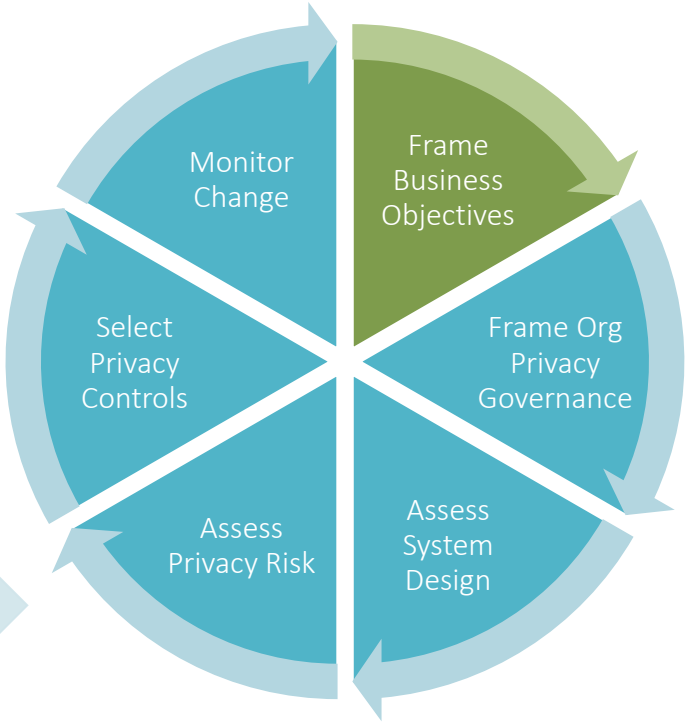
Describe the functionality of the system(s).

Describe the business needs that system(s) serve.

- Preserve benefits while mitigating privacy risk
- Establishes collaboration between business owners and privacy engineering

Describe how the system will be marketed, with respect to any privacy-preserving functionality.

- Privacy as competitive advantage
- Trace controls back to requirements



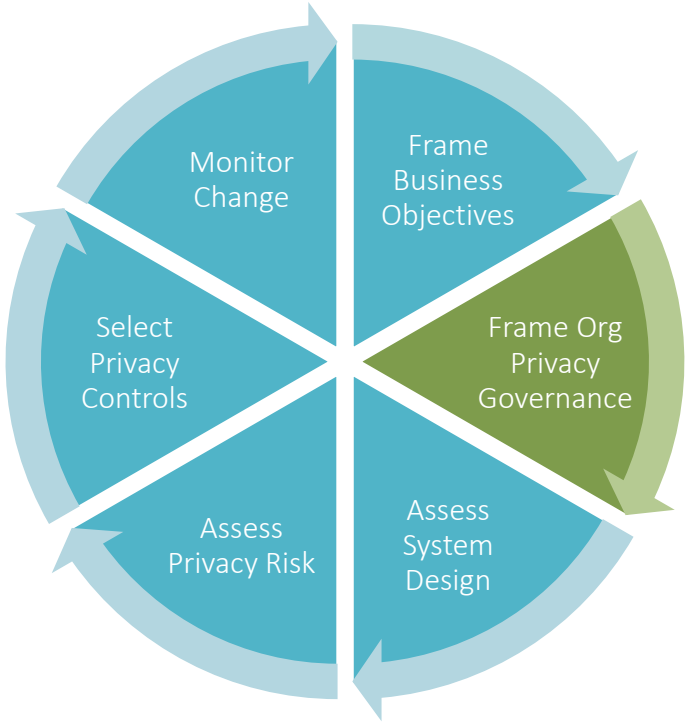
# Frame Privacy Governance

Identify any privacy-related statutory, regulatory, or contractual obligations.

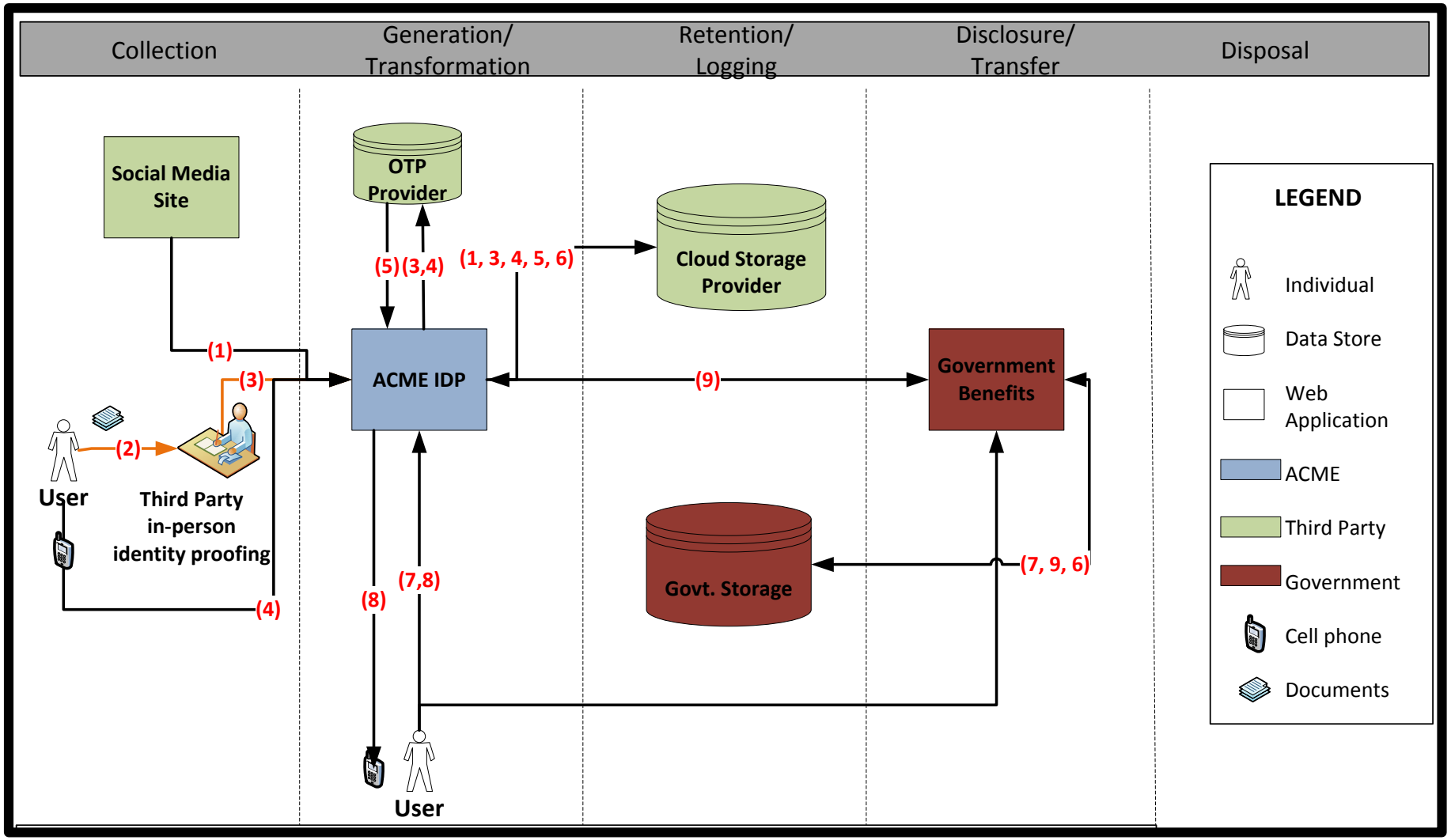
Identify any privacy-related principles to which the organization adheres (FIPPs, Privacy by Design, etc.).

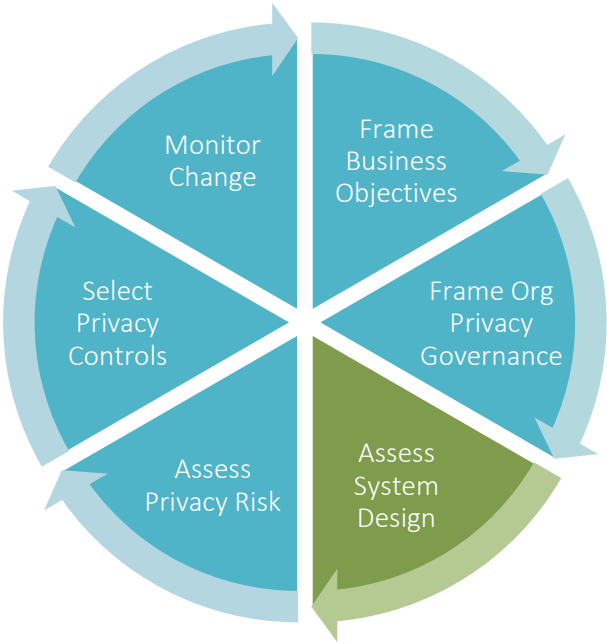
Identify any organizational privacy policies

- 1st question: Can we?
- 2nd question: Should we?



# Assess System Design – Data Map



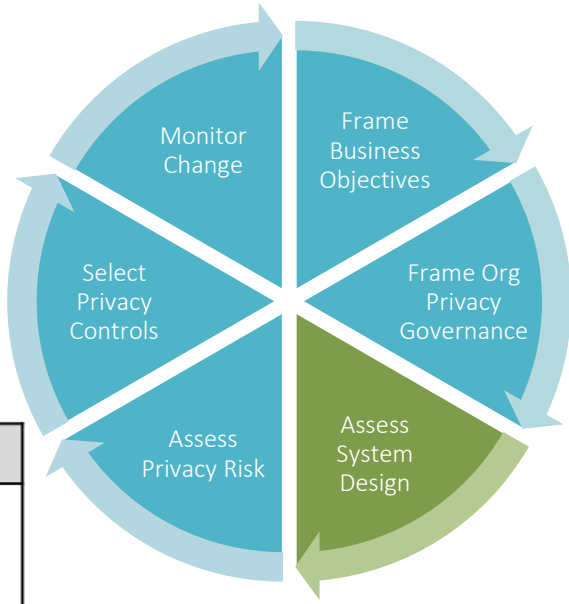




## Identify

When a business owner, an engineer, and a privacy pro sit at a table…

**Surprise! We're doing what with data?**

# Assess System Design - Context



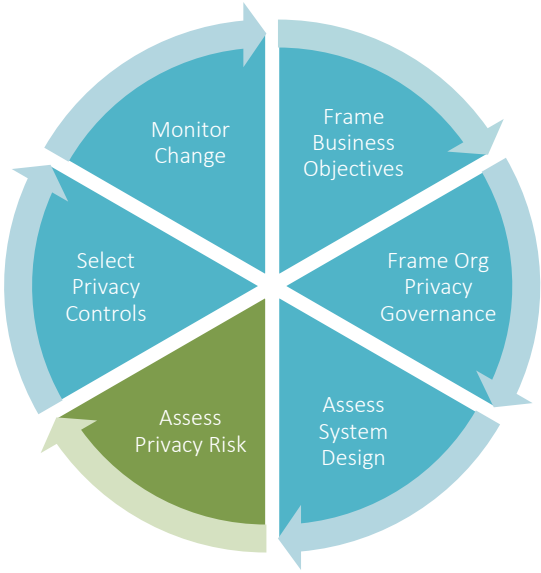

**Example:**

An individual wishes to use ACME IDP service to augment a social credential with identity proofing and a second authentication factor to create a stronger credential. This stronger credential will be used to access government benefits.

| Data Action | Personal Information | Specific Context | Summary Issues |
|---|---|---|---|
| Collection from the Social Media Site | - Self-Asserted Full Name<br>- Validated Email<br>-List of Friends<br>-Profile Photograph | - One-time action (per user) between social credential and ACME IDP, but establishes an ongoing relationship between user's social media presence and ACME IDP<br>- Social credential linking is visible to user<br>- Linking of social credential simplifies access to government benefits system<br>- User profile may contain information the user considers sensitive<br>- User profile may contain information from other users not participating in the system | - Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose<br>- Will users understand the eventual high-assurance credential is controlled by ACME and not by their social credential provider?<br>- How will perception of the social media organization's privacy practices impact users' willingness to consent to this data action?<br>- Will the user understand ACME will have |

| Example Contextual Factors |
|---|
| **Organizational** |
| *System includes both government benefits agency and commercial service providers* |
| *Multiple privacy policies governing system* |
| *Public perception: high expectation of privacy with government benefits agency, low expectation with social credential provider* |
| *Relationships: No pre-existing relationship with ACME IDP, regular interactions with government benefits agency, regular interactions with social credential provider* |
| **System** |
| *Personal information is not intended to be made public* |
| *New system, no history with affected individuals. Low similarity with existing systems/uses of social identity.* |
| *Four parties sharing personal information: one public institution, three private* |
| *ACME will use 3rd party cloud provider* |
| **User** |
| *High sensitivity about government benefits provided by system* |
| *Users exhibit various levels of technical sophistication* |
| *Potential user confusion regarding who "owns" the various segments of each system* |
| *20% of users use privacy settings at social provider* |

# Assess Privacy Risk

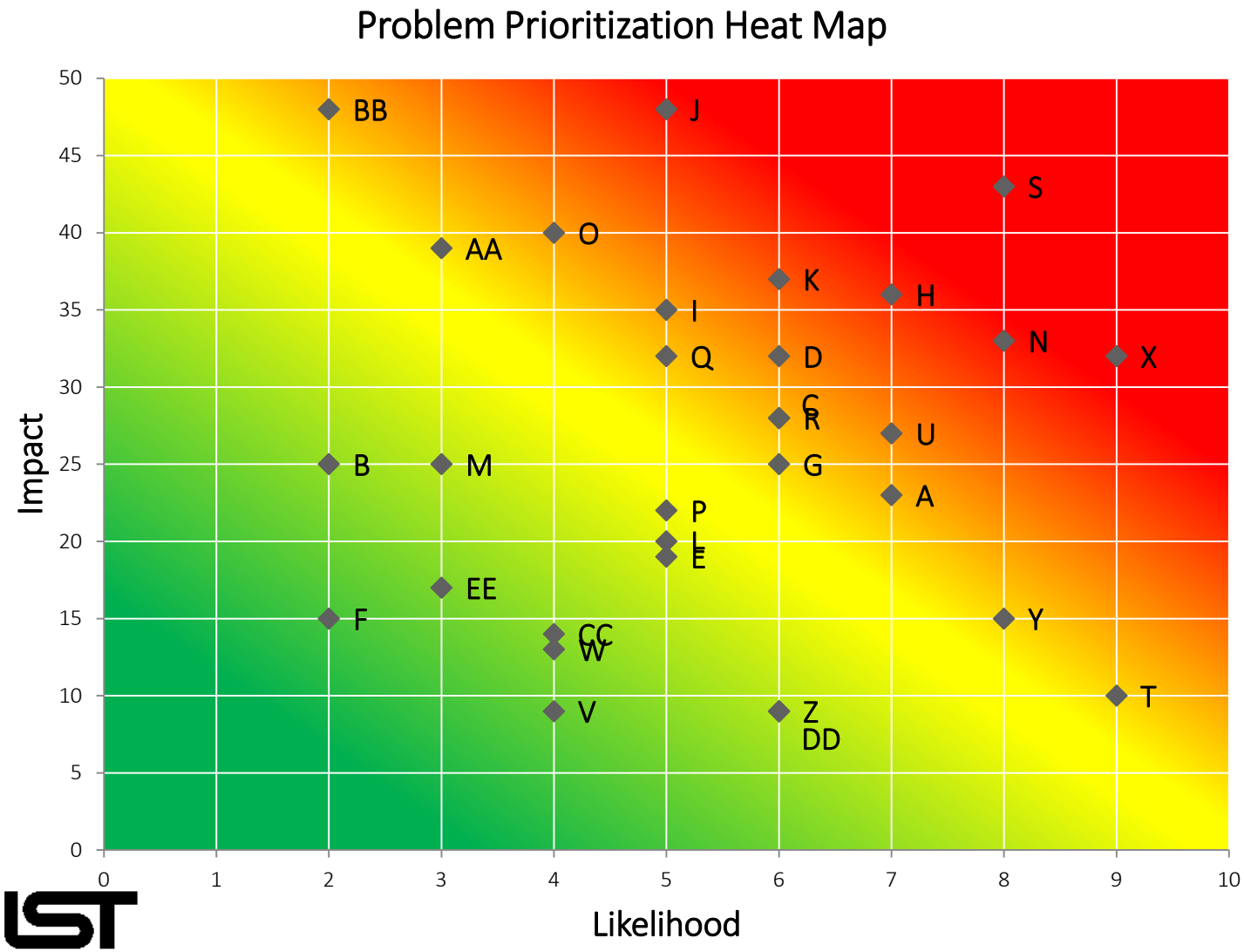


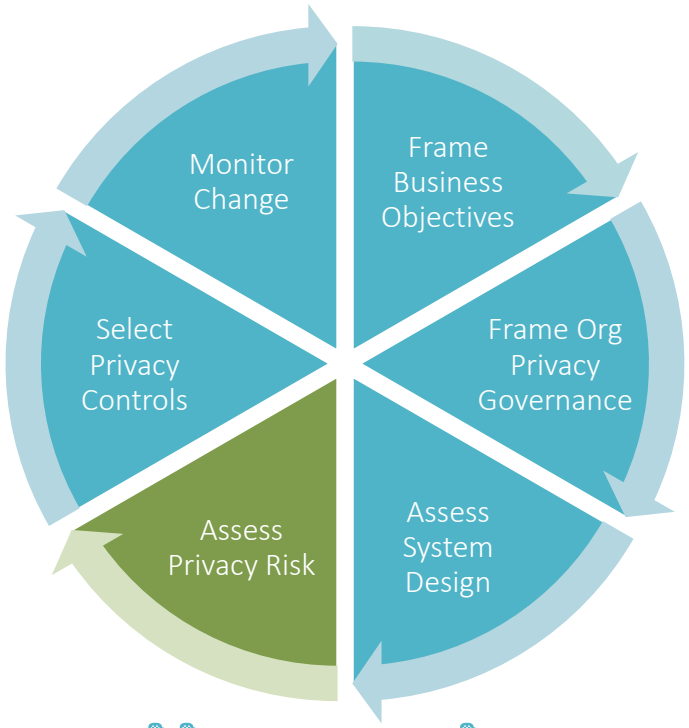

**SAMPLE TABLE**

| Data Actions | Summary Issues | Problematic Data Actions | Potential Problems for Individuals | Likelihood |
|---|---|---|---|---|
| | | | | |
| Collection from the Social Media Site | Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose. | -Appropriation<br>-Induced disclosure<br>-Surveillance<br>-Unanticipated Revelation | Stigmatization: Information is revealed about the individual that they would prefer not to disclose. | 7 |
| | | | Power Imbalance: People must provide extensive information, giving the acquirer an unfair advantage. | 2 |
| | Will users understand the eventual high-assurance credential is controlled by ACME and not by their social credential provider? | -This summary issue will be associated with another data action. | | NA |
| | How will percept<br>organization's priva<br>willingness to con | | | |

| Data Actions | Summary Issues | Problematic Data Actions | Potential Problems for Individuals | Business Impact Factors | | | | | Total Business Impact (per Potential Problem) |
|---|---|---|---|---|---|---|---|---|---|
| | | | | Noncompliance Costs | Direct Business Costs | Reputational Costs | Internal Culture Costs | Other | |
| Collection from the Social Media Site | Full social credential profile access (including picture and list of friends) is not necessary for fulfilling operational purpose. | -Appropriation<br>-Induced disclosure<br>-Surveillance<br>-Unanticipated Revelation | Stigmatization | 7 | 6 | 6 | 4 | | 23 |
| | | | Power Imbalance | 7 | 6 | 8 | 4 | | 25 |
| | How will perception of the social media organization's privacy practices impact users' willingness to consent to this data action? | -Induced disclosure<br>-Surveillance | Loss of Trust | 7 | 6 | 8 | 7 | | 28 |

# Assess Privacy Risk



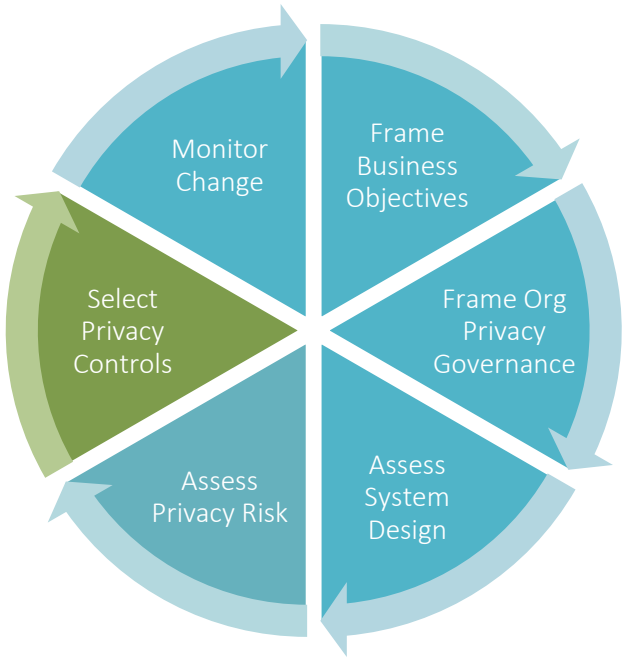




## Telling the Privacy Story

- Communicate with leadership
- Definable problems lead to actionable solutions

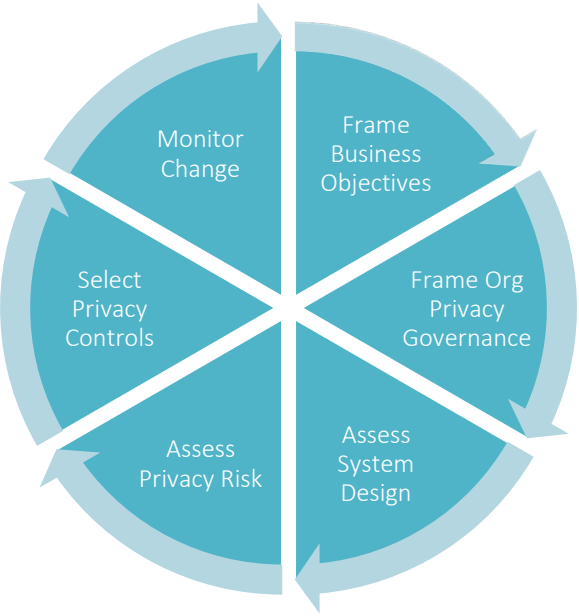
# Select Privacy Controls

| Data Actions | Potential Problems for Individuals | Potential Controls | Considerations |
|---|---|---|---|
| Collection from the Social Media Site | Stigmatization: Information is revealed about the individual that they would prefer not to disclose. | 1. Configure API to enable more granular retrieval of information, pull full name and email only; enable capability to pull profile photograph if future proofing requires it.<br>2. Inform users of collection.<br>3. Delete unneeded information after collection. | 1. Significantly reduces collection of information, possibly decreasing risk across the system. Would potentially lower risk of stigmatization, power imbalance, and loss of trust problems.<br>2. Users may be informed of specific information collected in this data action, but that may not improve risk across the system as they are unable to prevent the revelation of information.<br>3. Unclear how users will understand the process. Leverages appropriate disposal controls. Decreases risk of stigmatization, but not necessarily power imbalance or loss of trust. Compare potential failure rate for API |
| | Power Imbalance: People must provide extensive information, giving the acquirer an unfair advantage. | | |
| | Loss of Trust: Individuals lose trust in ACME due to a breach in expectations about the handling of personal information. | | |




| Data Actions | Potential Problems for Individuals | Selected Controls | Rationale | Residual Risks |
|---|---|---|---|---|
| Collection from the Social Media Site | Stigmatization: Information is revealed about the individual that they would prefer not to disclose. | 1. Change API call to only pull full name and email; consider change to pull profile photograph if future proofing requires it.<br>2. Inform users of information that is collected and why at time of collection. | 1. Significantly reduces collection of information, possibly decreasing risk across the system. Would potentially lower risk of stigmatization, power imbalance, and loss of trust problems.<br>2. Meets transparency requirement. Easy to implement. | |
| | Power Imbalance: People must provide extensive information, giving the acquirer an unfair advantage. | | | |
| | Loss of Trust: Individuals lose trust in ACME due to a breach in expectations about the handling of personal information. | | | |

# Informed Risk Decisions




**The PRAM…**

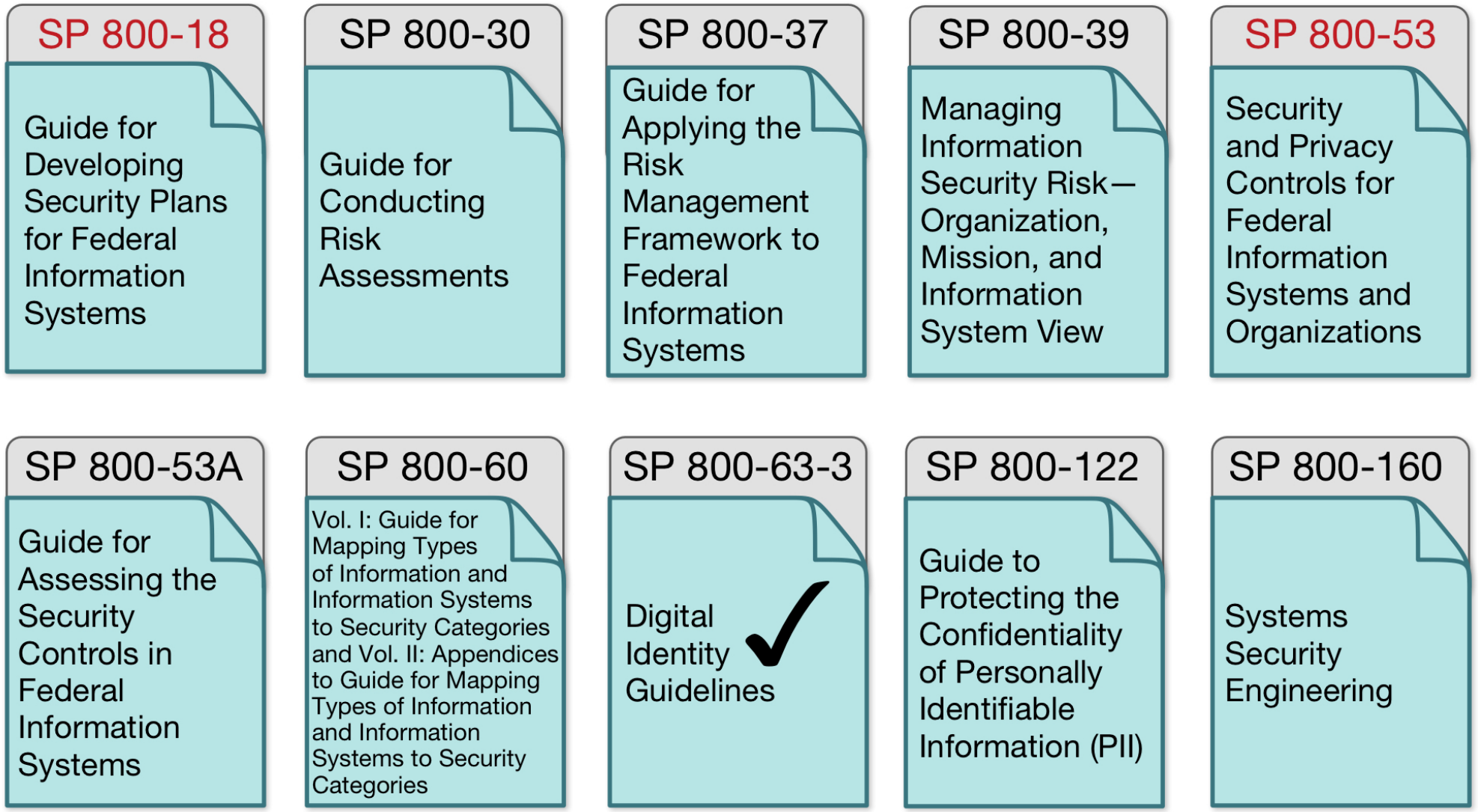
- Surfaces trade-offs
- Is at a level that all parties can understand
- Leads to *solutions*

**Mitigate | Avoid | Accept | Transfer**

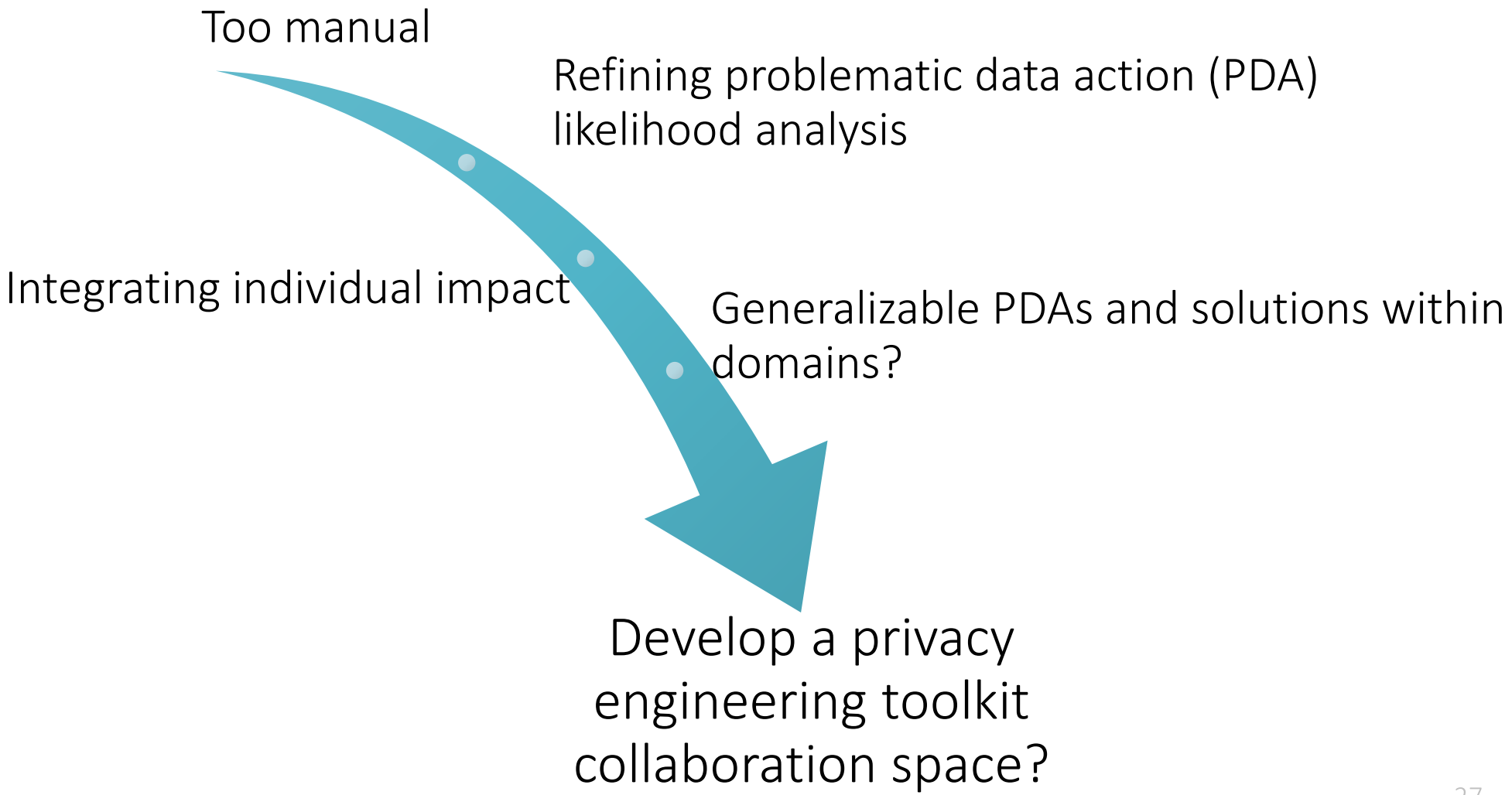
Whatever the decision,
it's *informed* by a reasoned process.

# Next Steps

# Guidance Roadmap



# Improving the PRAM



# Resources

Naomi Lefkovitz
Naomi.lefkovitz@nist.gov

Ellen Nadeau
Ellen.nadeau@nist.gov

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

NIST Internal Report 8062
https://doi.org/10.6028/NIST.IR.8062