Using Risk Management to Improve Privacy in Information Systems
Potential Problems for Individuals

- Loss of Trust
  - Stigmatization
  - Power Imbalance
- Loss of Self Determination
  - Discrimination
- Loss of Autonomy
  - Exclusion
  - Loss of Liberty
  - Physical Harm
- Economic Loss
NIST Risk Management Framework for Cybersecurity
The Right Tool for the Job

Many current privacy approaches are some mixture of governance principles, requirements and controls.

<table>
<thead>
<tr>
<th>USG FIPPs</th>
<th>NIST SP 800-53, Appendix J</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transparency</td>
<td>Authority and Purpose</td>
</tr>
<tr>
<td>Individual Participation</td>
<td>Security</td>
</tr>
<tr>
<td>Purpose Specification</td>
<td>Accountability, Audit, and Risk Management</td>
</tr>
<tr>
<td>Data Minimization</td>
<td>Data Quality and Integrity</td>
</tr>
<tr>
<td>Use Limitation</td>
<td>Data Minimization and Retention</td>
</tr>
<tr>
<td>Data Quality and Integrity</td>
<td>Data Quality and Integrity</td>
</tr>
<tr>
<td>Security</td>
<td>Security</td>
</tr>
<tr>
<td>Accountability and Auditing</td>
<td>Accountability and Redress</td>
</tr>
<tr>
<td></td>
<td>Security</td>
</tr>
<tr>
<td></td>
<td>Transparency</td>
</tr>
<tr>
<td></td>
<td>Use Limitation</td>
</tr>
</tbody>
</table>
NIST Process

Workshop 1
April 2014

Aug 2014
Draft Proposal for Objectives and Risk Model

Sep 2014
Workshop 2

2015
NISTIR
Draft Privacy Engineering Objectives

• Design characteristics or properties of the system
• Support policy
• Support control mapping

**Predictability** is enabling reliable assumptions by individuals, owners, and operators about personal information and its processing by an information system.

**Manageability** is providing the capability for granular administration of personal information including alteration, deletion, and selective disclosure.

**Obscurity** is enabling the processing of personal information or events without association to individuals or devices beyond the operational requirements of the system.
Security Risk Equation

Security Risk = Vulnerability * Threat * Impact
Draft Privacy Risk Equation

Privacy Risk = Likelihood of a Problematic Data Action * Impact of a Problematic Data Action

**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 for individuals occur.

*Note: Contextual analysis is based on the data action performed by the system, the personal information being processed, and a set of contextual considerations.*
Implementation
Implementing the Theory

- Frame Business Objectives
- Frame Org Privacy Governance
- Assess System Design
- Assess Privacy Risk
- Design Privacy Controls
- Monitor Change
Frame Business Objectives

Frame the business objectives for the system(s), including the organizational needs served.

• Describe the functionality of the system(s).
• Describe the business needs that the system(s) serve.
• Describe how the system will be marketed, with respect to any privacy-preserving functionality.
Frame Privacy Governance

Frame the organizational privacy governance by identifying privacy-related legal obligations, principles, organizational goals and other commitments.

- Legal Environment: Identify any privacy-related statutory, regulatory, contractual and/or other frameworks within which the system must operate.
- Identify any privacy-related principles or other commitments to which the organization adheres (FIPPs, Privacy by Design, etc.).
- Identify any privacy goals that are explicit or implicit in the organization’s vision and/or mission.
- Identify any privacy-related policies or statements within the organization, or business unit.
Assess System Design – Data Actions
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.

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

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

<table>
<thead>
<tr>
<th>Data Actions</th>
<th>Summary Issues</th>
<th>Problematic Data Actions</th>
<th>Potential Problems for Individuals</th>
<th>Likelihood</th>
</tr>
</thead>
</table>
| 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  
- Induced disclosure  
- Surveillance  
- Unanticipated Revelation | Stigmatization: Information is revealed about the individual that they would prefer not to disclose.  
Power Imbalance: People must provide extensive information, giving the acquirer an unfair advantage. | 7          |
| 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          |
Assess Privacy Risk

Problem Prioritization Heat Map

- Impact
- Likelihood

- Monitor Change
- Frame Business Objectives
- Design Privacy Controls
- Frame Org Privacy Governance
- Assess Privacy Risk
- Assess System Design

NIST
Resources

NIST Privacy Engineering Website:

Questions

Contact:
Naomi Lefkovitz
naomi.lefkovitz@nist.gov