Privacy Engineering Objectives and Risk Model

Objective-Based Design for Improving Privacy in Information Systems
NIST research has a broad impact

Facilitates trade and fair commerce

Improves public safety and security

Advances manufacturing and services

Improves quality, ensures uniformity
First Privacy Engineering Workshop

Purpose:
• Consider analogous models
  - Focus on objectives
• Identify distinctions

Key Outcomes:
• Communication gap
• Positive interest in a risk management model
Model Privacy Risk Management Framework

Policy
(Law, Regulation, FIPPs, etc.)

Risk Assessment

Requirements

System Evaluation

Privacy Engineering Components

Objectives
(Predictability, Manageability, Confidentiality)

Risk Model
(Personal Information + Data Actions + Context = System Privacy Risk)

Controls
(Derived from FIPPs, etc.)

Metrics

September Workshop
Key Terms

Privacy Engineering Objectives

Problematic Data Actions

Privacy Engineering

Data Lifecycle

Context

Data Actions

Privacy Harms
Privacy Engineering
Objectives

Outcome-based objectives that guide design requirements to achieve privacy-preserving information systems.
The Privacy Triad

- The objectives are characteristics of the system, not role-based.
- The objectives support policy
- Aligning the privacy and security overlap

**Predictability**
Enabling reliable assumptions about the rationale for the collection of personal information and the data actions to be taken with that personal information.

**Manageability**
Providing the capability for authorized modification of personal information, including alteration, deletion, or selective disclosure of personal information.

**Confidentiality**
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

(NIST SP 800-53, rev 4)
System Privacy Risk Model
Security Risk Equation

Security Risk = Vulnerability * Threat * Impact
System privacy risk is the risk of problematic data actions occurring

Personal Information Collected or Generated * Data Actions Performed on Personal Information * Context = System Privacy Risk
Context

“Context” means the circumstances surrounding a system’s collection, generation, processing, disclosure and retention of personal information.
Problematic Data Actions and Privacy Harms

Distinguish data actions that give rise to harms and actual harms

Validation of the objectives and the risk model

Problematic Data Actions

Privacy Harms
Privacy Engineering Definition

Privacy engineering is a collection of methods to support the mitigation of risks to individuals of loss of self-determination, loss of trust, discrimination and economic loss by providing predictability, manageability, and confidentiality of personal information within information systems.

Information Security: The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability.

[44 U.S.C., SEC. 3542]
# Illustrative Mapping of Privacy Engineering Objectives to Problematic Data Actions

<table>
<thead>
<tr>
<th>Data Lifecycle Phase</th>
<th>Normal Data Action</th>
<th>Problematic Data Action</th>
<th>Potential Harms</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Predictability</strong></td>
</tr>
<tr>
<td>Collection</td>
<td>Service Initiation</td>
<td>Induced Disclosure</td>
<td>Power Imbalance, Loss of Autonomy</td>
</tr>
<tr>
<td>Processing</td>
<td>Aggregation</td>
<td>Unanticipated Revelation</td>
<td>Stigmatization, Power Imbalance, Loss of Trust, Loss of Autonomy</td>
</tr>
<tr>
<td>Processing</td>
<td>System monitoring</td>
<td>Surveillance</td>
<td>Power Imbalance, Loss of Trust, Loss of Autonomy, Loss of Liberty</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Manageability</strong></td>
</tr>
<tr>
<td>Disclosure</td>
<td>Authorized Attribute Sharing</td>
<td>Distortion</td>
<td>Stigmatization, Power Imbalance, Loss of Liberty</td>
</tr>
<tr>
<td>Disposal</td>
<td>Normal Account Deletion</td>
<td>Unwarranted Restriction</td>
<td>Exclusion, Economic Loss, Loss of Trust</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td><strong>Confidentiality</strong></td>
</tr>
<tr>
<td>Use</td>
<td>Authorized Use</td>
<td>Appropriation</td>
<td>Loss of Trust, Economic Loss, Power Imbalance</td>
</tr>
<tr>
<td>Retention</td>
<td>Secure Storage</td>
<td>Insecurity</td>
<td>Economic Loss, Stigmatization</td>
</tr>
</tbody>
</table>
What's Next?

Webcast: 2:00pm, ET, October 2, 2014

Publish a NIST Interagency Report
• Public comment period between draft and final versions

Comments may be sent to privacyeng@nist.gov until October 15, 2014.