Privacy Engineering Objectives and Risk Model - Discussion Deck

Objective-Based Design for Improving Privacy in Information Systems

Purpose and Scope

- This discussion deck describes initial draft components of privacy engineering developed from the output of NIST's first Privacy Engineering Workshop, April 9-10, 2014. It does not address a complete privacy risk management framework.
- The draft components include a definition for privacy engineering, a set of privacy engineering objectives and a system privacy risk model. This deck will be used to facilitate discussions at the second Privacy Engineering Workshop on September 15-16, 2014 in San Jose, CA.
- The privacy engineering objectives and risk model are primarily focused on mitigating risks arising from unanticipated consequences of normal system behavior. Risks to privacy arising from malicious actors or attacks can continue to be mitigated by following standard security principles.

Model Privacy Risk Management Framework

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

Privacy Engineering

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.

Key Terms

- **Privacy Engineering Objectives:** Outcome-based objectives that guide design requirements to achieve privacy-preserving information systems.
- **Data Lifecycle:** The data actions an information system performs.
- **Data Actions:** Normal information system operations that handle personal information.
- **Problematic Data Actions:** Problematic data actions occur when the data actions of an information system contravene the objectives of predictability, manageability, or confidentiality.
- **Context:** The circumstances surrounding a system's collection, generation, processing, disclosure and retention of personal information.

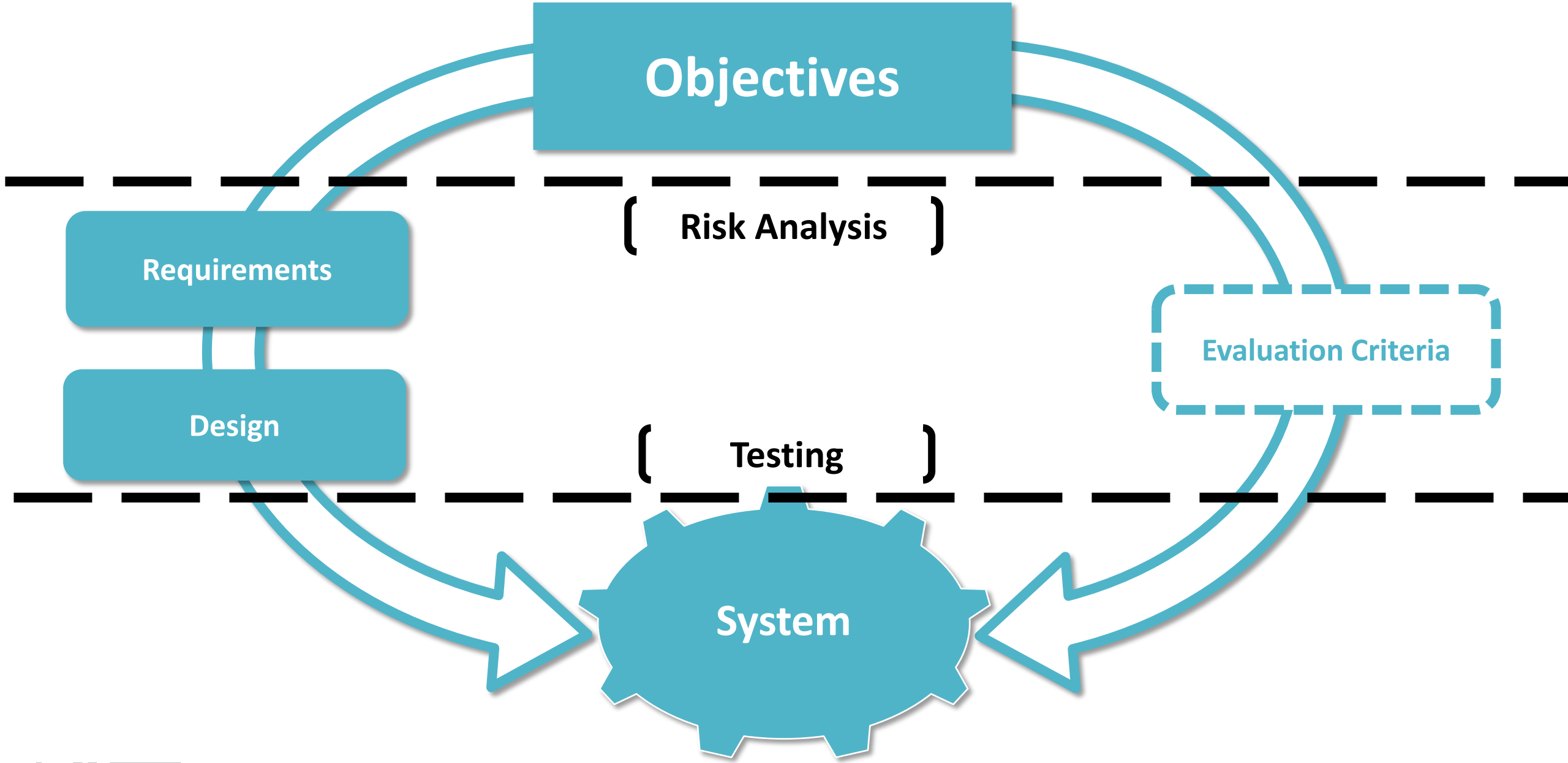
Key Terms (con't)

Privacy Harms: Harms to individuals that result from problematic data actions. Harms can be grouped into four categories:

- **Loss of Self-Determination:** The loss of an individual's personal sovereignty or ability to freely make choices. This includes the harms of Loss of Autonomy, Exclusion, Loss of Liberty
- **Discrimination:** The unfair or unequal treatment of individuals. This includes the harms of Stigmatization and Power Imbalance.
- **Loss of Trust:** The breach of implicit or explicit expectations or agreements about the handling of personal information.
- **Economic Loss:** Economic loss can include direct financial losses as the result of identity theft, as well as the failure to receive fair value in a transaction involving personal information.

Privacy Engineering Objectives

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


Objectives
Risk Analysis
Requirements
Design
Evaluation Criteria
Testing
System

Predictability

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

Example Violation of Predictability			
Data Lifecycle Phase	**Normal Data Action**	**Problematic Data Action**	**Potential Harms**
Processing	Aggregation	Unanticipated Revelation	Stigmatization, Power Imbalance, Loss of Trust, Loss of Autonomy

Manageability

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

Example Violation of Manageability			
Data Lifecycle Phase	**Normal Data Action**	**Problematic Data Action**	**Potential Harms**
Disposal	Normal Account Deletion	Unwarranted Restriction	Exclusion, Economic Loss, Loss of Trust

Confidentiality

Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. *(NIST SP 800-53, rev 4)*

Example Violation of Confidentiality			
Data Lifecycle Phase	**Normal Data Action**	**Problematic Data Action**	**Potential Harms**
Retention	Secure Storage	Insecurity	Economic Loss, Stigmatization

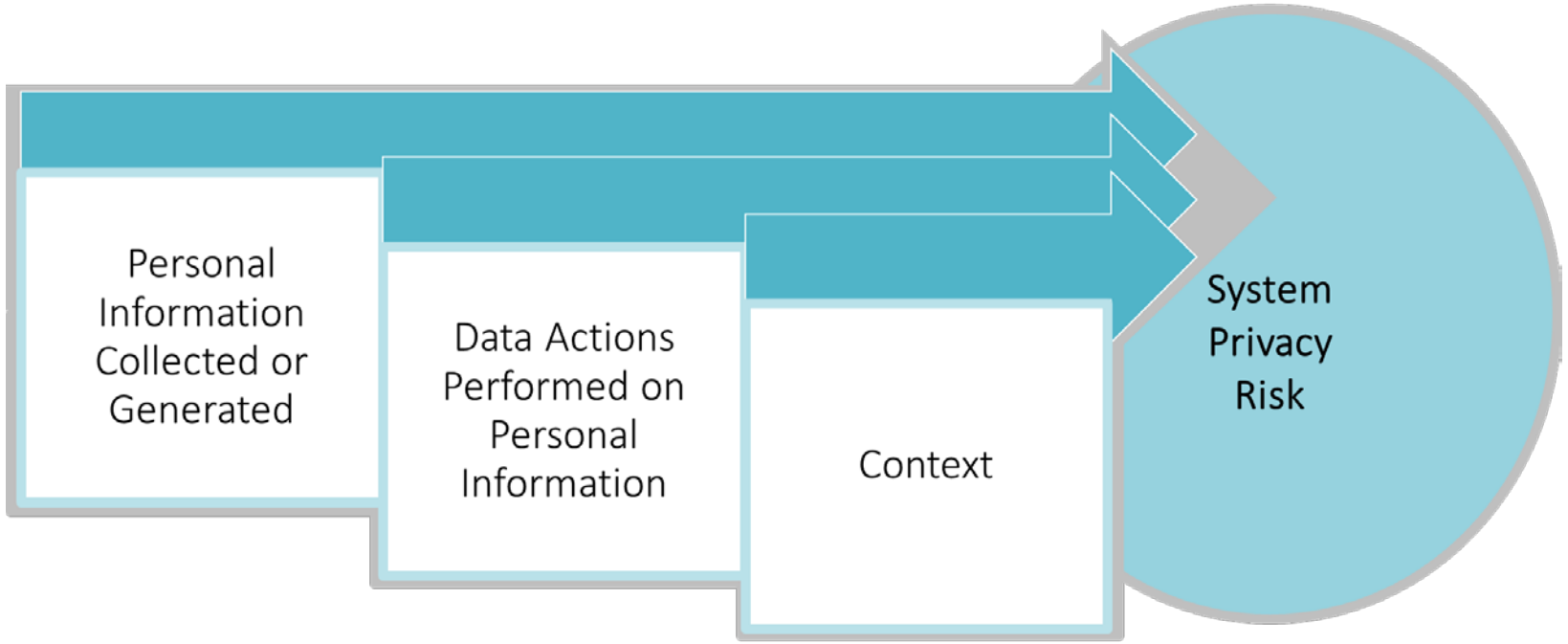
System Privacy Risk Model

Assessing System Privacy Risk

- To understand the magnitude of privacy risk within an information system, the proposed model focuses on the risk or likelihood of problematic data actions occurring that could result in privacy harm to individuals.
- A key distinction between privacy and security is that privacy harms may arise even though the system is performing data actions in accordance with its operational purpose. Moreover, these harms may be difficult to assess as they may occur externally to the system, and beyond the system owner's awareness.
- Thus, the risk model concentrates on the risk of data actions becoming problematic which the system owner or designer can better recognize and control.

System Privacy Risk Equation

System privacy risk is the risk of problematic data actions occurring



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

Context

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

Examples of Contextual Factors

- The relationship between individuals and the organization that controls the system
- The extent and frequency of direct interactions between an individual and the system
- The nature and history of those interactions
- The range of goods or services that the system offers, and such use by individuals
- The types of personal information that is foreseeably necessary for the system to process or generate in order to provide the goods or services
- The level of understanding that reasonable individuals would have of how the system processes the personal information that it contains
- Information known by the system about the privacy preferences of individuals
- The extent to which personal information under the control of the system is exposed to public view
- General user experience with information technologies

Problematic Data Actions

Problematic data actions occur when the data actions of an information system contravene the objectives of predictability, manageability, or confidentiality.

Appropriation: Personal information is used in ways that exceed an individual's expectation or authorization

Appropriation occurs when personal information is used in ways that an individual would object to or would have negotiated additional value for, absent an information asymmetry or other marketplace failure. Privacy harms that Appropriation can lead to include loss of trust, economic loss or power imbalance.

Distortion: The use or dissemination of inaccurate or misleadingly incomplete personal information

Distortion can present users in an inaccurate, unflattering or disparaging manner, opening the door for discrimination harms or loss of liberty.

Induced Disclosure: Pressure to divulge personal information

Induced disclosure can occur when users feel compelled to provide information disproportionate to the purpose or outcome of the transaction. Induced disclosure can include leveraging access or privilege to an essential (or perceived essential) service. It can lead to harms such as power imbalance or loss of autonomy.

Insecurity: Lapses in data security

Lapses in data security can result in a loss of trust, as well as exposing individuals to economic loss, and stigmatization.

Surveillance: Tracking or monitoring of personal information that is disproportionate to the purpose or outcome of the service

The difference between the data action of monitoring and the problematic data action of surveillance can be very narrow. Tracking user behavior, transactions or personal information may be conducted for operational purposes such as protection from cyber threats or to provide better services, but it becomes surveillance when it leads to harms such as power imbalance, loss of trust or loss of autonomy or liberty.

Unanticipated Revelation: Non-contextual use of data reveals or exposes an individual or facets of an individual in unexpected ways

Unanticipated revelation can arise from aggregation and analysis of large and/or diverse data sets. Unanticipated revelation can give rise to stigmatization, power imbalance and loss of trust and autonomy.

Unwarranted Restriction: The improper denial of access or loss of privilege to personal information

Unwarranted restriction to personal information includes not only blocking tangible access to personal information, but also limiting awareness of the existence of the information within the system or the uses of such information. Such restriction of access to systems or personal information stored within that system can result in harms such as exclusion, economic loss and loss of trust.

Privacy Harms

Harms to individuals that result from problematic data actions.

Loss of Self-Determination

Loss of autonomy: Loss of autonomy includes needless changes in behavior, including self-imposed restrictions on freedom of expression or assembly.

Exclusion: Exclusion is the lack of knowledge about or access to personal information. When individuals do not know what information an entity collects or can make use of, or they do not have the opportunity to participate in such decision-making, it diminishes accountability as to whether the information is appropriate for the entity to possess or the information will be used in a fair or equitable manner.

Loss of Liberty: Improper exposure to arrest or detainment. Even in democratic societies, incomplete or inaccurate information can lead to arrest, or improper exposure or use of information can contribute to instances of abuse of governmental power. More life-threatening situations can arise in non-democratic societies.

Discrimination

Stigmatization: Personal information is linked to an actual identity in such a way as to create a stigma that can cause embarrassment and discrimination. Sensitive information such as health data or criminal records or merely accessing certain services such as food stamps or unemployment benefits may attach to individuals and be disclosed in unrelated contexts.

Power Imbalance: Acquisition of personal information which creates an inappropriate power imbalance, or takes unfair advantage of or abuses a power imbalance between acquirer and the individual. For example, collection of attributes or analysis of behavior or transactions about individuals can lead to various forms of discrimination or disparate impact, including differential pricing or redlining.

Loss of Trust

Loss of trust is the breach of implicit or explicit expectations or agreements about the handling of personal information. For example, the disclosure of personal or other sensitive data to an entity is accompanied by a number of expectations for how that data is used, secured, transmitted, shared, etc. Breaches can leave individuals leave individuals reluctant to engage in further transactions.

Economic Loss

Economic loss can include direct financial losses as the result of identity theft, as well as the failure to receive fair value in a transaction involving personal information.

Illustrative Mapping of Privacy Engineering Objectives to Problematic Data Actions

Data Lifecycle Phase	Normal Data Action	Problematic Data Action	Potential Harms
Predictability			
Collection	Service Initiation	Induced Disclosure	Power Imbalance, Loss of Autonomy
Processing	Aggregation	Unanticipated Revelation	Stigmatization, Power Imbalance, Loss of Trust, Loss of Autonomy
Processing	System monitoring	Surveillance	Power Imbalance, Loss of Trust, Loss of Autonomy, Loss of Liberty
Manageability			
Disclosure	Authorized Attribute Sharing	Distortion	Stigmatization, Power Imbalance, Loss of Liberty
Disposal	Normal Account Deletion	Unwarranted Restriction	Exclusion, Economic Loss, Loss of Trust
Confidentiality			
Use	Authorized Use	Appropriation	Loss of Trust, Economic Loss, Power Imbalance
Retention	Secure Storage	Insecurity	Economic Loss, Stigmatization

Discussion Questions

For discussion at the NIST Privacy Engineering Workshop on September 15-16, 2014:

- Privacy Engineering (slide 4): Is this definition helpful?
- Privacy Engineering Objectives (slides 8-10): Are these objectives actionable for organizations? Are there any gaps?
- System Privacy Risk Model (slide 13): Is it constructive to focus on mitigating problematic data actions?
- System Privacy Risk Equation (slide 14): Does this equation seem likely to be effective in identifying system privacy risks? If not, how should system privacy risk be identified?
- Context (slide 16): Are these the right factors? Are there others?
- Problematic Data Actions (slides 18-24): Are these actions functional? Are there additional ones that should be included?
- Harms (slides 26-29): Are these harms relevant? Are there additional ones that should be included?

Comments may also be sent to privacyeng@nist.gov until September 30, 2014.