Privacy by Design - With or Without Information Security

Influence of InfoSec on InfoPriv

Frank Dawson
frank dot dawson at nokia dot com

2013-01-23

NOKIA

Influence of InfoSec on InfoPriv

- ***You can have security without privacy but no privacy without security***

- Information privacy borrows heavily from InfoSec for organizational governance, concepts, processes and tools

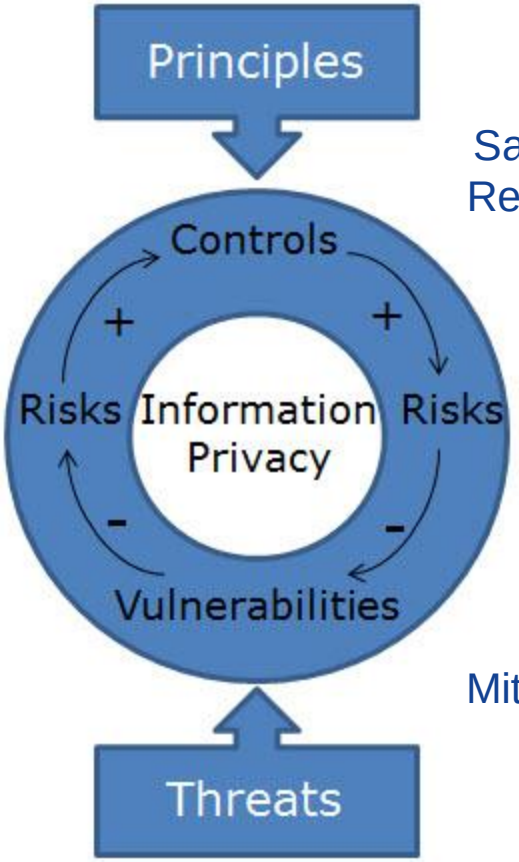
- InfoPriv differs in a number of key aspects:
  - More elaborate set of guiding principles
  - Goal is for consumer to have control over data
  - Risk Management is about harm to the individual

Privacy safeguarding framework

- Based on a cycle formed by ***principles*** (and supporting **safeguarding *requirements***), supported by technology ***safeguards*** or ***controls*** and dependent on iterative vigilance to assess and mitigate inevitable underlying ***threats*** from inherent ***vulnerabilities*** with ascertainable ***risks***

- Control types include Physical, Procedural, Technical, Legal and/or Regulatory

- Controls should be tied to underlying privacy principles and applicable privacy data lifecycle



Ref: US/DoC NIST SP-800-53 Appendix J Privacy Control Catalog

NOKIA

Privacy Engineering

- ***Privacy Engineering*** is emerging as a discipline based on accepted Information Privacy concepts, process and tools similar to those found in Information Security practices

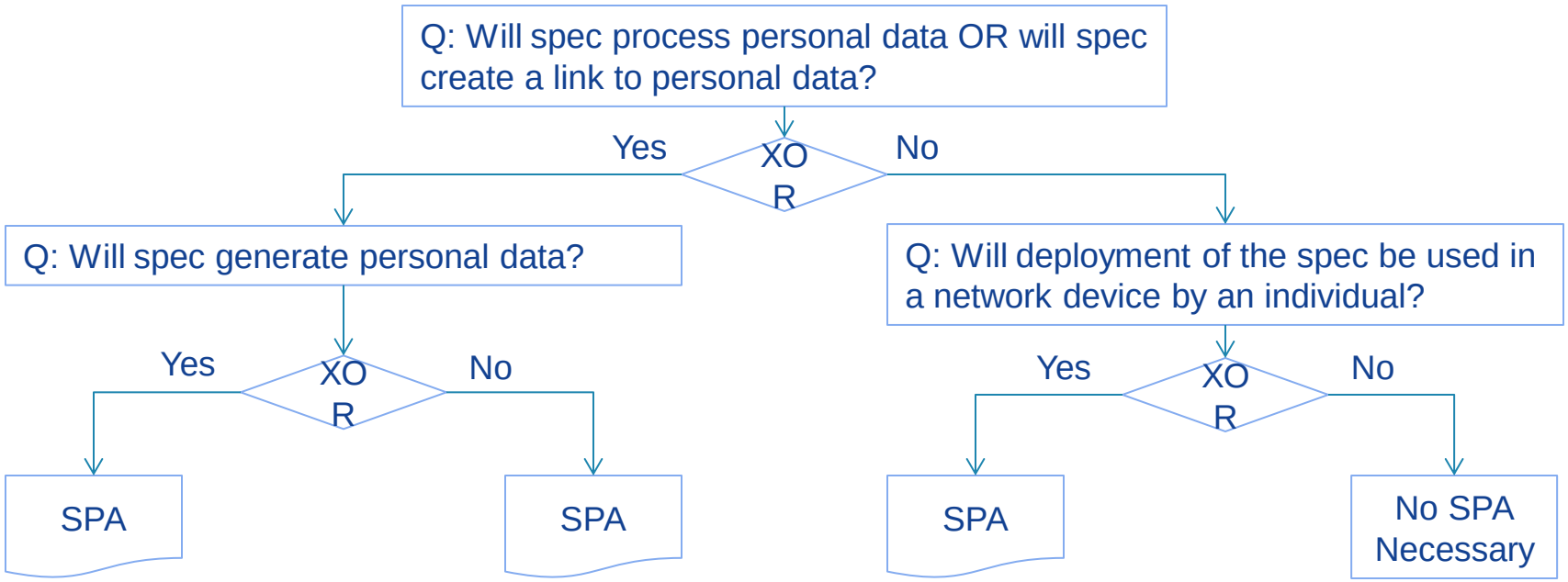
- Privacy Impact Assessment (PIA) continues as primary tool for assessing privacy impact of choices presented in the software development lifecycle

- Lessons-learned will form the basis of a catalog of Privacy Design Patterns to guide future Privacy Engineers

Privacy engineering – As applied to stds

Specification Privacy Assessment (SPA)

- Methodology for analyzing specification against applicable privacy impact, taking into account applicable privacy principles, associated privacy safeguarding requirements and assessing potential threats that require mitigation by introducting privacy safeguards/controls, based on risk assessment to harm caused by the technology to the consumer



NOKIA

Integration with spec creation process

- Kick-off – Best time to start is when the new work item has been created
  - Work item introduced, Privacy fundamentals explained, Privacy goals explained, SPA approach explained, Privacy Champ identified
- Collaboration – Specification taking shape through contributions
  - As group creates spec functionality, data flows analyzed and categorized, areas for Privacy Engineering are identified, Privacy requirements identified, Threats identified, Safeguards defined, Findings documented in SPA report for follow-up action
- Drafting
  - Privacy Considerations section reflects mitigation steps to address SPA findings
- Publication
  - Publication staff and Spec Editor verify Privacy Considerations compliance against SPA findings and update accordingly
- Support
  - Deployment of specification can lead to issue reporting that need address in timely manager with technical opinions and possible change requests for spec update

NOKIA

SPA process summary

1. Understand the specification in terms of the privacy data lifecycle.
2. Outline data flow between internal components defined by specification.
3. Outline data flow model between the internal components of specification and interactions of external components through associated format, interface or protocol used by the specification.
4. Does the specification collect, utilize, store, transfer, manage information that could identify a person? Does the standard collect, utilize, store, transfer, manage information that could identify a network connected device? Classify them (E.G., using a scheme such as proposed by ”PII 2.0”. ***Document these in the privacy considerations section of the specification***.
5. Identify applicable privacy principles and associated privacy safeguarding requirements.
6. Outline the threats created by the data flows and opportunities where a privacy control mechanism can be introduced to safeguard data protection. ***Document these in the privacy considerations section of the specification***.
7. Consider also, documenting, in the privacy considerations, specific approaches, beyond the privacy controls in #6, that will enhance privacy such as limits on collection, limits for retention, rules for secure transfer, rules for limiting identification or obsfuscation, for those deploying the specification or standard.

Outline of Privacy Considerations

- Every specifications should include a *Privacy Considerations* section that:
  - **Catalogs the personally identifiable information (PII)** collected, its classification, instances of data storage, type of processing, instances of data transfer (against the privacy data lifecycle);
  - **Identify and list privacy threats**;
  - **Identify appropriate privacy safeguards/controls** and context for mitigating identified threats,
  - **Identify recommendations** such as uses of privacy controls, by organization deploying the standard, that would additionally thwart the associated threats.

NOTE: A risk assessment (level of harm+probability of it) should be completed, as least, by the organization deploying the standard