W3C Workshop
DNT And Beyond

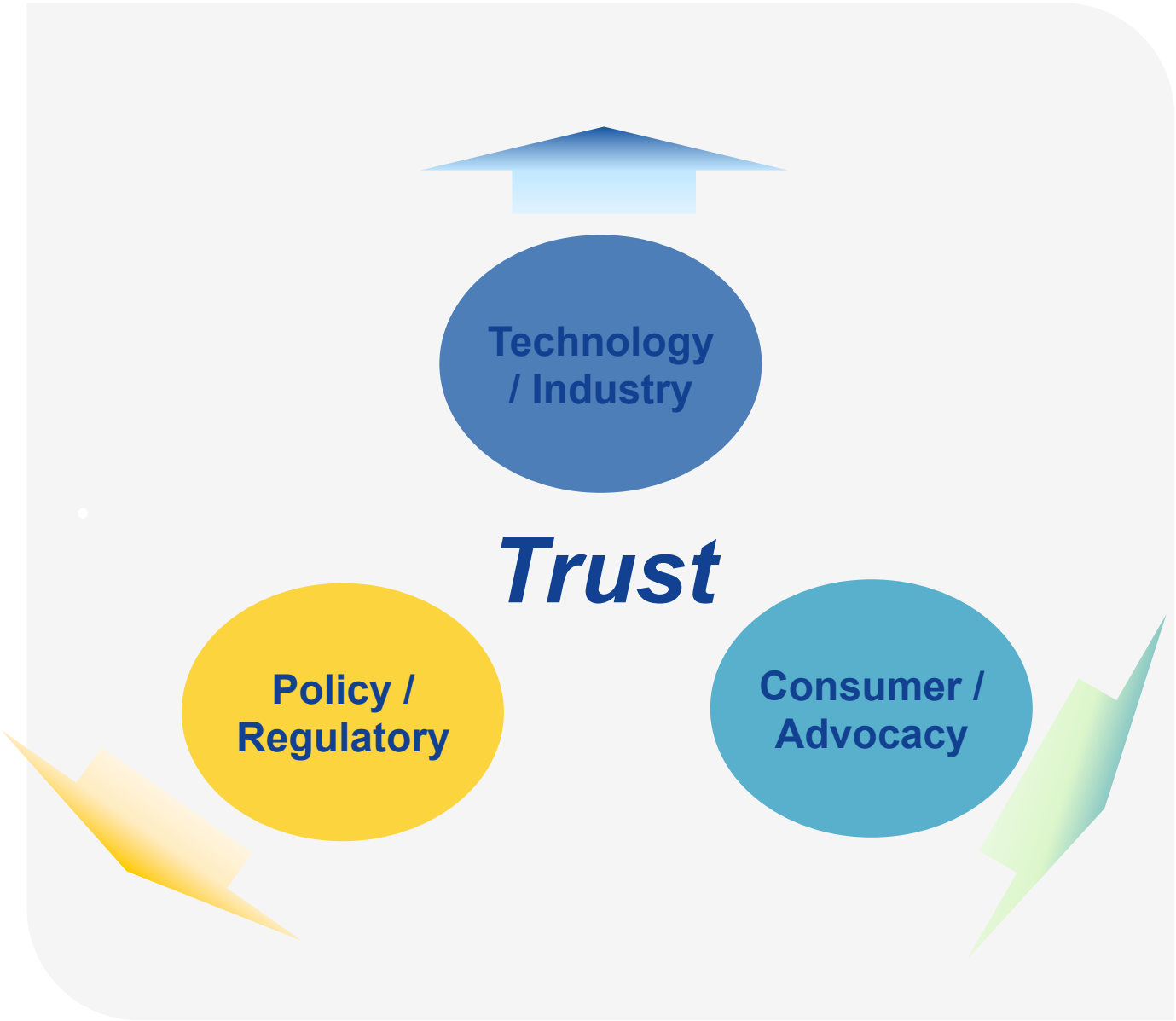
Future Directions Panel

Frank Dawson
frank dot dawson at nokia dot com

2012-11-27

NOKIA

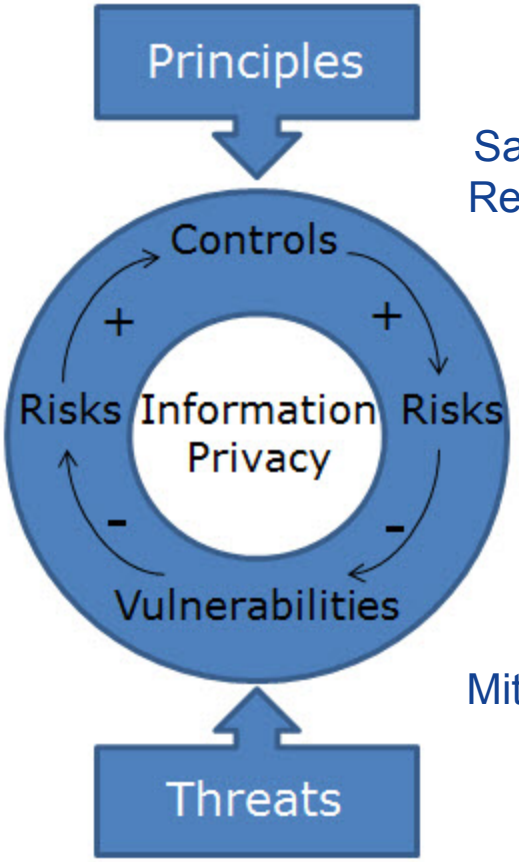
Triangle of Trust



NOKIA

Privacy safeguarding framework

- ***Privacy Engineering*** is emerging as a methodology based on accepted information privacy concepts similar to those found in informaiton security practices
- Based on a cycle formed by ***principles*** (and **safeguarding *requirements***), supported by technology ***safeguards*** or ***controls*** and dependent on iterative vigilance to mitigate inevitable underlying ***threats*** to inherent ***vulnerabilities*** with assertainable ***risks***
- Control types include Physical, Procedural, Technical, Legal and/or Regulatory



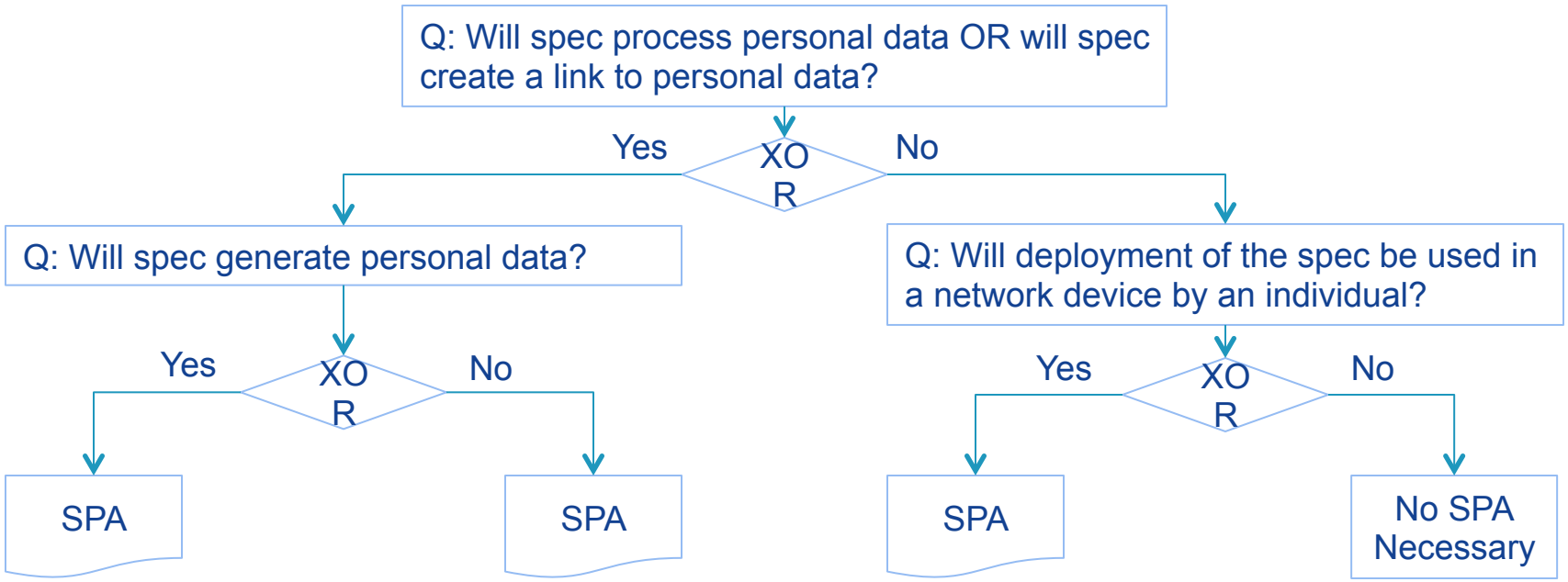
Ref: US/DoC NIST SP-800-53 Appendix J Privacy Control Catalog

NOKIA

Privacy engineering – tools of the trade

Specification Privacy Assessment (SPA)

- Methodology for analyzing specification against applicable privacy principles, taking into account associated privacy safeguarding requirements and assessing potential threats that requirement mitigation with introduction of privacy safeguards/controls, based on risk assessment to harm caused by technology to 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. Identify privacy principles and underlying privacy safeguarding requirements applicable to the scope of the specification.
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. Outline the threats created by these data flows for instances where a privacy control mechanism can be introduced to safeguard data protection. Document these in the privacy considerations section of the specification.
5. Does the specification collect, utilize, store, transfer, manage information that could identify a person? Classify and document these in the privacy considerations section of the specification.
6. Does the standard collect, utilize, store, transfer, manage information that could identify a network connected device? Classify and document these in the privacy considerations section of the specification.
7. Document in the privacy considerations section of the specification specific approaches, beyond the privacy controls in #4, that will enhance privacy such as limits on collection, limits for retention, rules for secure transfer, rules for limiting identification or obsfuscation.

Outline of Privacy Considerations

- Every specifications should include a *Privacy Considerations* section that details:
  - **Identify privacy principles and underlying privacy safeguarding requirements** that are applicable to the specification,
  - **Describe the data flow through entities that might provide control points** for personal data entities within the format, API or protocol,
  - **Catalog the data** collected, classification, instances of data storage, type of processing, instances of data transfer (against the privacy data lifecycle);
  - **Identify and list privacy threats**;
  - **Document privacy safeguards/controls** in technical specification and context for mitigating identified threats,
  - **Estimate risk of harm** (e.g., magnitude and likelihood);
  - **Document proposed risk mitigation actions**, including recommended uses of privacy controls introduced by the specification to thwart the associated threats.