Specification Privacy Assessment (SPA)

Frank Dawson (frank.dawson at nokia.com)
Nokia, CTO-CIC

2012-10-08

NOKIA

Purpose

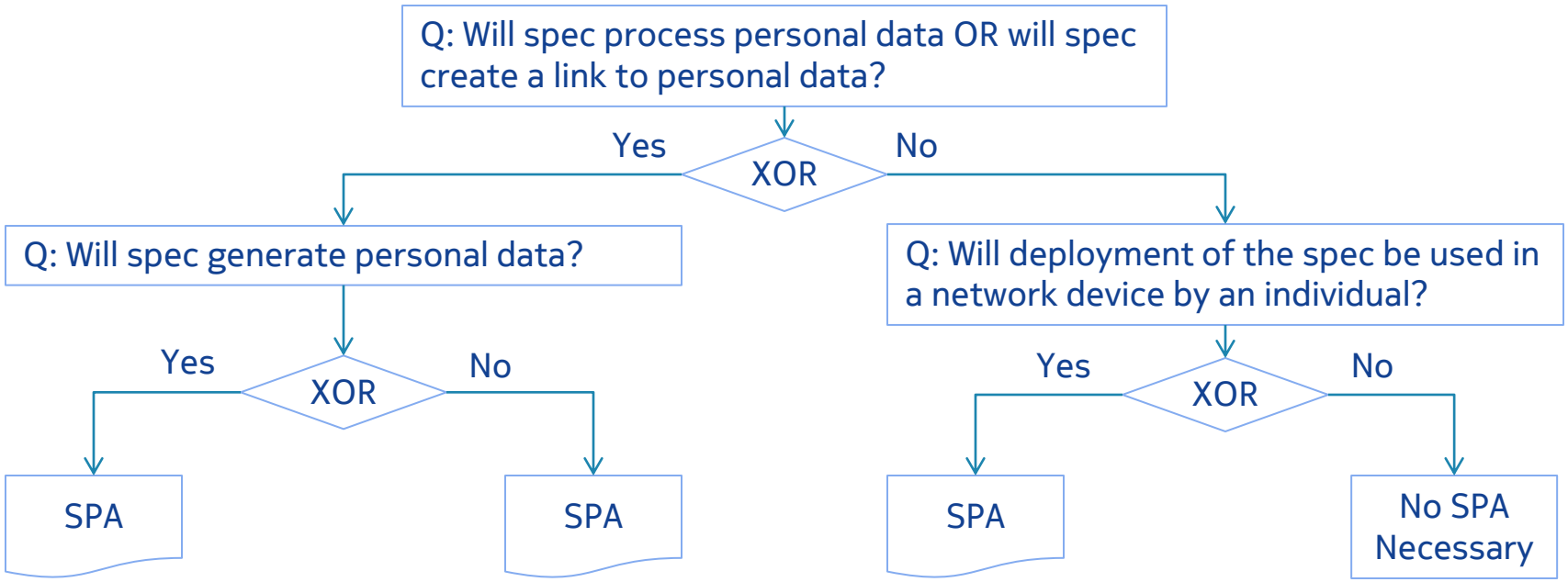
- Industry specifications make up the definition of the technology infrastructure for the internet and web that fuels the digital marketplace
- Integrity of this infrastructure is as strong as the weakest link in the technology network
- Information privacy or data protection is an increasingly important aspect of the digital marketplace and needs to be baked into the technical infrastructure
  - A process known as Privacy by Design
- Standards development organizations and industry fora have long recognized the need to include information security considerations in these specifications through application of a kind of security threat assessment
- It is time to also include Privacy Considerations sections within our internet and web technical specifications
- This will be accomplished by applying a Specification Privacy Assessment (SPA) methodology

Action items

1. Document the group's privacy commitment and endorse it at the highest level in the organization's management;
2. Identify a permanent group or an individual with the responsibility to oversee privacy implications of the organization's work items;
3. Include a section on "privacy considerations" in each of the organization's specifications and make it mandatory for all future specifications;
4. Review and update existing standards to include a "privacy considerations" section;
5. Begin to document the Best-Practices for Privacy Controls and publish them as Privacy Design Patterns, so that they can be shared across the industry.

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



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

Specification Privacy Assessment (SPA)

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? 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? 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 specification *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 entities within the format, API or protocol specification that are control points for personal data,
  - Catalog the data collected, instances of data storage, type of processing, instances of data transfer (against the privacy data lifecycle);
  - Identify and list privacy threats;
  - Document current and proposed technical and organizational privacy safeguards/controls to mitigate identified threats,
  - Estimate the magnitude and likelihood of those risks;
  - Document proposed resolutions to risks, including privacy controls introduced by the specification to thwart the identified threats.

Background information

Could be material for use in group privacy training/awareness

NOKIA

Why is *privacy* important?

- ✓Authorities are doing joint-enforcement on major companies

  Example: Facebook

- ➢Canadian, US, Nordic, Irish regulators investigated complaints and found violations

- ✓Increasing public policy maker interest in mobile technologies

  Example: Positioning technologies

- ➢More and more laws globally

Enforcement Actions:

- € Fines
- € Penalties
- € Cost of remediation
- € Forced privacy program
- € 20 year external audit
- € Deletion of unlawfully collected data
- € Sales stops, recalls

NOKIA

Commonly referenced privacy principles

US FIPP

Notice/Awareness, Choice/Consent, Access/Participation, Integrity/Security, Enforcement/Redress (Self-regulation, Private remedies, Government enforcement)

OECD

Collection limitation, Data quality, Purpose specification, Use limitation, Security safeguards, Openness, Individual participation, Accountability

EU Directive 95/46/EC

Transparency, Legitimate purpose, Proportionality, Personal data, Processing, Data quality (Fair & legal, Purpose-limited, Relevant, Accurate, Time-limited), Legitimate data processing (Consent, Contract, Legal obligations, Vital interests, Public interest, Legitimate interests), Processing senstive information

EU-US Safeharbour

Notice, Choice, Onward transfer, Security, Data integrity, Access, Enforcement

Standards topics with privacy impact

- Internet protocols
- Internet and web formats
- Data schemas
- Web APIs
- Device APIs
- Web service definitions
- Browser plug-ins
- Proximity and connectivity standards for promoting data sharing, device coupling and service invocation
- Collaborative applications/services
- Device management services
- User experience and UI control
- Mobile applications and services

Common privacy threats

- Lack of consumer choice
- Lack of consumer control
- Unauthorized data collection – secret databases
- Unauthorized info access – data breach
- Unauthorized info sharing – covert transfers
- Unauthorized surveillance - spying
- Unauthorized profiling – tracking
- Data integrity loss – corrupted info
- Unauthorized solicitation – unwanted marketing
- Misrepresentation – Inaccurate characterization
- Lack of consumer redress – Inability to rectify errors
- Stolen value - fraud

Personal information

- Personal information relates to information about a natural person
- When the data can be associated with an individual, it is referred to as Personally Identifiable Information (PII)
- Criteria for linkability of data to an individual is a hot-topic within the privacy community
- *Sensitive PII* must be treated special
- Generally, if PII is of a racial, religious, political, sexual orientation, medical nature, it is characterized as Sensitive; but other categories should also be consisted
- Also commonly referred to as *Personal Data*

These are some of the things that should be considered when identifying the PII in your particular standard or architecture

Personal characteristics

Numbers or characters assigned to an individual

Descriptions of events

Descriptions of locations or places

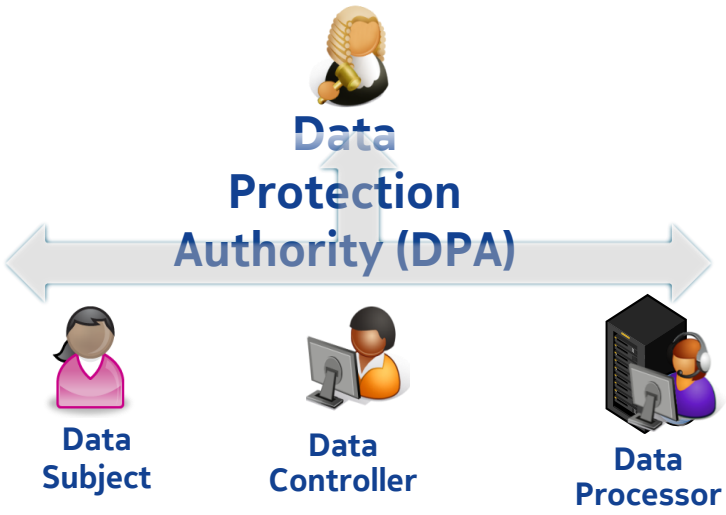
EU guidance on personal data

Personal Data as defined by the Directive 95/46/EC (Article 2) 'shall mean *any information relating to an identified or identifiable natural person* ('data subject'); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity'. Additionally, WP 136 and WP 175 (section 2.2) of Art. 29 Data Protection Working Party should be considered, which detail the concept of personal data and qualify a unique number as personal data if it is carried by a person.

Sensitive Personal Data is defined by the Directive 95/46/EC (Article 8) as any personal data that relates to (a) the racial or ethnic origin, the political opinions or the religious or philosophical beliefs of the data subject, (b) whether the data subject is a member of a trade union, (c) the physical or mental health or condition or sexual life of the data subject, (d) the commission or alleged commission of any offence by the data subject, or (e) any proceedings for an offence committed or alleged to have been committed by the data subject, the disposal of such proceedings or the sentence of any court in such proceedings. Additionally, it is recommended to consider the context, too, when determining the sensitivity of personal data. Data that is not sensitive in itself may become sensitive in a specific context.

Roles within the privacy framework

- DPA, Data Privacy Authority, Information Privacy Commissioner, etc is the independent legal authority for administering privacy rules within a country
- The consumer is the Data Subject
- The Data Controller is entity that determines purposes and means of processing consumer's personal data
- The Data Processor performs information processing on behalf of the Data Controller



Sometimes a reference is also made to a Third Party, which can be viewed as outside this privacy framework, but the responsibility of the Data Controller.

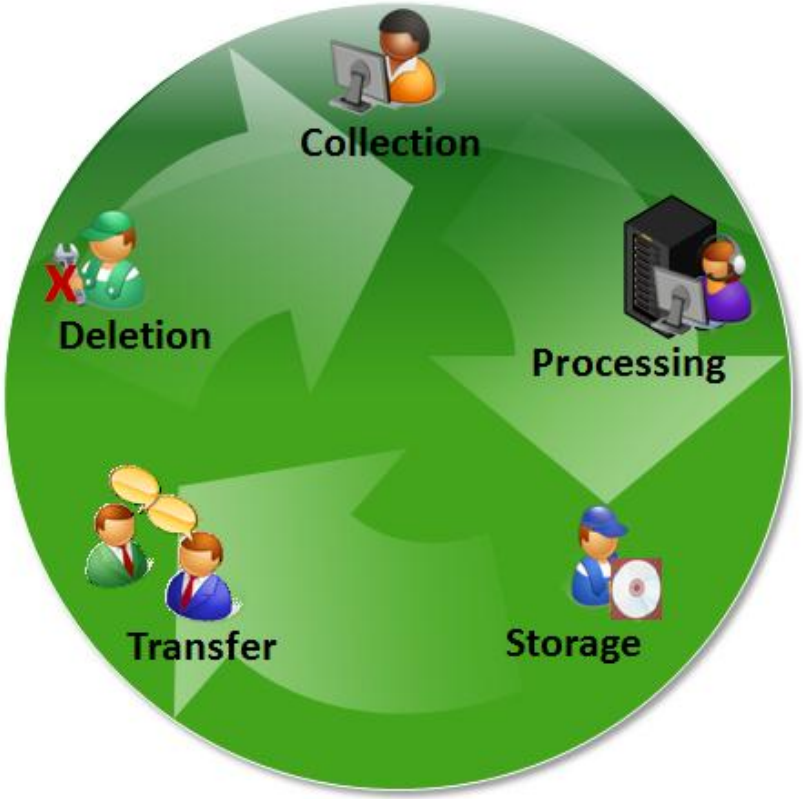
NOKIA

Nymity

- The Theory of Nymity applies to the degree of identification; varying along a spectrum from full identity of the consumer to other extreme of no linkability to the consumer, at all
- Combinations of few characteristics often combine in populations to uniquely or nearly uniquely identify some individuals; leading some privacy advocates to doubt universality of anonymity
- *k-anonymous coefficient* is often referred to as a quantative measure of the linkability of data to an individual and a measure of the level of anonymity
- Best to treat all PII with appropriate privacy controls, because over time, addition of context can compromise current level of anonymity

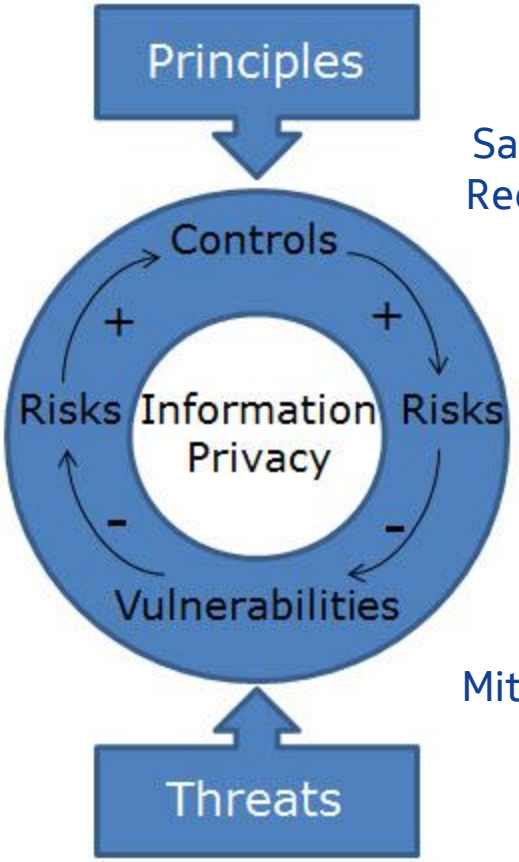
Privacy data lifecycle

- Also called the *Consumer Data Lifecycle* , it is a fundamental component of the privacy knowledge base
- Define the actions related to personal data within the privacy framework
- When analyzing the data flow in your specifications, you should also consider the complete lifecycle for the associated PII
- Within the EU, *collection*, itself is considered to be an act of *processing* !



Privacy controls

- ***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 ***requirements***), supported by technology ***controls*** and dependent on iterative vigilance to mitigate inevitable underlying ***threats*** to inherent ***vulnerabilities*** with assertainable ***risks***
- Controls types include Physical, Procedural, Technical, Legal and regulatory



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

NOKIA

Design principles that favor privacy

- Specification *Data Governance* plan
- Data minimization
- Data security (confidentiality, integrity, availability)
- Clarity of purpose for data collection, use, storage, transfer
- Limit retention of data
- Reduce the linkability of data with de-identification techniques
- Emphasis on complete product lifecycle
- Consumer centric defaults

Privacy by Design, Accountability

- PbD
  - Bake-in privacy into specifications from the beginning, rather than retro-fit to existing specifications
  - Privacy by Re-Design (PbRD) is inevitable for legacy specifications
  - 7-Foundation Principles
    1. Proactive not Reactive; Preventative not Remedial
    2. Privacy as the Default Setting
    3. Privacy Embedded into Design
    4. Full Functionality — Positive-Sum, not Zero-Sum
    5. End-to-End Security — Full Lifecycle Protection
    6. Visibility and Transparency — Keep it Open
    7. Respect for User Privacy — Keep it User-Centric
  - Is now globally included into regulations
- Accountability
  - Do What You Say _and_ Demonstrate It!
  - Aim to achieve more than just compliance
  - Is now globally included into regulations

Relationship of privacy to security

- **Information Security** (INFOSEC) can be viewed as *control over who may use a computer and information* stored in it
- **Information Privacy** (INFOPRIV) can be viewed as *control over disclosure of computer based information* and who gets access to it

- Therefore, there is a very dependent relationship
- *" You can have security without privacy but not privacy without security"*

- INFOPRIV can borrow greatly from the technology aspects of the more mature INFOSEC discipline
  - Threat analysis and mitigation, risk assessment
  - Control – Vunerability model
  - Implementation frameworks

Privacy design patterns

- Format for capturing and sharing design knowledge
- Describes a generic solution to a repeating problem
- Origins in architecture, application in 90s to O-O Design, in 2K to InfoSec and more recently InfoPriv
- Essential elements (POSA format) include:
  - Pattern name, Context, Problem, Solution, Consequences, Known Uses, Related Patterns
- Examples:
  - Informed notice, Explicit consent, Policy update, Visualizing interaction feedback & warnings
- RECOMMENDATION: Participate in creation of a pattern library for common solutions for privacy problems