Privacy – From Principles to Technology Standards

Information Privacy is a critical success factor for the success of the emerging global digital market place[1]. Consumers will only shop in a market place that they trust. Technology standards will play an important role in progressing support for privacy in the information society accessing this market place[2][3]. Nokia supports Privacy by Design[4]. Privacy by Design is essential to assuring consumers that the underlying technology infrastructure of information society meets their privacy expectations.

Solving the privacy challenge requires multi-party efforts. Regulators and policy makers need to work on privacy principles and identify clear privacy objectives. Advocacy needs to raise awareness and help bring issues to public discussion. Industry and technology representatives need to identify best practices for translating privacy principles into concrete technology solutions and drive privacy objectives into underlying technology infrastructure of information society.

The role of technology standardization is essential for the above objective. Currently, many standards development organizations (SDO) and industry fora are working on technology standards and industry specifications for the information society infrastructure[5]. At the same time, the number of engineers with Privacy Engineering[6] skills is limited. To avoid fragmentation and to help build privacy engineering competency, SDOs and industry fora should:

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 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 they can be shared across the industry.

Some SDO and industry fora, such as ISO and IETF have formalized a central steering group or body of experts to address privacy related matters in their organizations. This approach means that privacy considerations are addressed in a timely and coordinated manner. Nokia supports this approach and believes it should be adopted commonly by all SDOs and industry fora.

---

[1] Kroes, N., Cloud Computing and Data protection reform, http://blogs.ec.europa.eu/neelie-kroes/cloud-data-protection, 2012.
[2] Cranor, L., The Role of Technology in Self-Regulatory Privacy Regimes, NTIA submission, http://lorrie.cranor.org/pubs/NTIA.html, 1996.
[3] IPO, Privacy Dividend, http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/Privacy_Dividend.pdf, 2010.
[4] Information & Privacy Commissioner, Ontario, Canada, Introduction to Privacy by Design, http://www.ipc.on.ca/english/Privacy/Introduction-to-PbD/, 2012.
[5] Ernst & Young, Privacy Trends 2012, http://www.ey.com/Publication/ vwLUAssets/Privacy_trends_2012/$FILE/ Privacy-trends-2012_AU1064.pdfpp 15-16, 2012.
[6] Privacy Engineering discipline is emerging as a university major study area. See University of Maryland reference at http://www.csee.umbc.edu/2012/04/privacy-engineering/.

A best-practice for businesses is the transparent articulation of their privacy vision. Similarly, SDOs and industry fora should specify the privacy mission for their standardization work. For example, this can be achieved by the management of these organizations explicitly committing to building privacy into their standards and specifications.

SDOs and industry fora need to assure that specifications published by the group include a common section on ***Privacy Considerations***, analogous to the Security Considerations section required in all IETF specifications[7] and is being proposed also by the Internet Architecture Board[8]. The process used to create the Privacy Considerations is analogous to that used in a Privacy Impact Assessment (PIA)[9]. The Privacy Considerations section should identify applicable privacy principles[10], describe possible control points that will allow for inserting privacy enabling technologies, document the personal data collected/used/stored/ transferred/ otherwise processed, identify vulnerabilities that could present a threat to privacy, specify what the risk of harm would be in these events, and document proposed mechanisms such as privacy controls[11] to mitigate the threats.

SDO and industry fora should review their portfolio of active projects. Each of the projects must be reviewed to assess the privacy impact that they might have. When a specification under development is identified as having a privacy impact, they must commit to adding a Privacy Considerations section prior to publication. As existing standards are considered for update or amendment, they too, should be edited to include a Privacy Considerations section.

Privacy is likely to become a major category of technology innovation[12]. Capturing leading and best practice solutions for privacy problems in the standards and specifications will promote the reuse of these solutions and enable growth of Privacy Engineering competency. Documenting these solutions as Privacy Design Patterns[13] using a standard template such as the POSA Template[14] would facilitate that.

Nokia is making these recommendations because of the importance of technology in solving the "privacy challenge" and the importance of open standards and industry specifications to build the required infrastructure. The proposed five recommendations have the potential to be instrumental in promoting SDOs and industry fora development of privacy friendly standards and specifications that leads to the proliferation of a global digital market place that assures consumer trust.

---

[7] RFC 3552, Guidelines for Writing RFC Text on Security Considerations, http://www.ietf.org/rfc/rfc3552.txt, IETF, 2003.
[8] IETF, Privacy Considerations for Internet Protocols, http://tools.ietf.org/html/draft-iab-privacy-considerations-02, 2012.
[9] See UK IPO, Privacy Impact Assessment Handbook, Version 2.0, http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/files/PIAhandbookV2.pdf, 2009.
[10] For example, the OECD Privacy Principles, http://oecdprivacy.org/, 1980.
[11] For example, NIST, Security and Privacy Controls for Federal Information Processing Systems and Organizations, http://csrc.nist.gov/publications/drafts/800-53-rev4/sp800-53-rev4-ipd.pdf, 2012.
[12] Golfarb, A. Tucker, C, Privacy and Innovation, http://www.nber.org/chapters/c12453.pdf, 2011.
[13] Hafiz,M.: A collection of privacy design patterns. Proc. 2006 Conference on Pattern Languages of Programs, ACM, NY, pp. 1-13. http://dl.acm.org/citation.cfm?id=1415472.1415481, 2006.
[14] F. Buschmann, R. Meunier, H. Rohnert,P. Sommerlad, and M. Stal. A System of Patterns:Pattern-Oriented Software Architecture. Wiley, 1996.