ISO/IEC JTC 1 N9781

2009-09-19

Replaces:

ISO/IEC JTC 1
Information Technology

Document Type:	other (defined)
Document Title:	Sensor Networks issues explored on privacy replying to JTC 1 Nara Resolution 31
Document Source:	SGSN Secretariat
Project Number:	
Document Status:	This document is forwarded to JTC 1 National Bodies for review and consideration at the October 2009 JTC 1 Plenary meeting in Tel Aviv.
Action ID:	ACT
Due Date:	
No. of Pages:	5

Secretariat, ISO/IEC JTC 1, American National Standards Institute, 25 West 43rd Street, New York, NY 10036; Telephone: 1 212 642 4932; Facsimile: 1 212 840 2298; Email: lrajchel@ansi.org

ISO/IEC JTC 1
Study Group on Sensor Networks

Document Number:	SGSN N152
Date:	2009-08-21
Replace:	SGSN N135
Document Type:	Other Document (Defined)
Document Title:	Sensor Networks issues explored on privacy replying to JTC 1 Nara Resolution 31
Document Source:	SGSN Oslo meeting
Document Status:	As per the SGSN Oslo Resolution 2, privacy issues will be reported to JTC 1 (Regarding the JTC 1 Nara Resolution 31).
Action ID:	FYI
Due Date;	
No. of Pages:	4

SGSN Convenor: Dr. Yongjin Kim, Modacom Co., Ltd (Email: cap@modacom.co.kr)
SGSN Secretary: Ms. Jooran Lee, Korean Standards Association (Email: jooran@kisi.or.kr)

JTC 1/SGSN Oslo Resolution 2 – Privacy

SGSN approves Privacy issues replying to JTC 1 Nara Resolution 31 in SGSN Oslo-N06. And SGSN instructs its Secretary to forward it to JTC 1 Secretariat for consideration at the 2009 JTC 1 Plenary meeting in Tel Aviv.

<Proposed text JTC1>:
Improving safety, traffic management, environment quality etc. in ICT will require surveillance, control and management measures that will not always be compatible with freedom of the individual. National legislation is based on internationally recognised principles and imposes specific requirements on the collection and processing of personal data. Sensor Network Systems pose challenges to both the legislation and the principles and mechanisms established to safeguard the right to privacy.
It is extremely important to protect personal data from unauthorized access and misuse, and in many cases it is necessary to establish measures to protect privacy. Such measures must be taken seriously and incorporated into the development of new services right from the start. Solutions must be found that take account as far as possible of the right to privacy, consumer rights and the need for reliable data and statistics. When establishing whether a Sensor Network System is in conflict with protection of privacy, the following factors must be clarified:
- the purpose of the data collection and storage
- notification that the data is being registered
- how the registered data is being managed
When new systems are being introduced, a dialogue must be established with the competent authorities at an early stage. The authorities must also take proactive action with regard to legislation and guidelines that need to be reviewed in the context of new Sensor Network Systems.

SGSN reports on "Sensor networks issues explored on privacy replying to JTC 1 Nara Resolution 31". SGSN has received contributions from the following sub-committees in JTC 1/SC6, SC25, SC27, SC29, SC31, SC32, SC36 and SC37 in time for the 4th SGSN meeting in Oslo 29 June 2009. SGSN has summarized the contributions in SGSN N152. These contributions will make the basis for a recommendation in document SGSN N143 on Privacy to be used in Sensor Networks.

<Summary>
SGSN provided a second iteration in respect to data privacy aspects and associated legislative requirements when developing and revising Ubiquitous Services with Sensor Networks.
National laws shall always take precedence over International guidelines. Cases made to International courts are likely to give precedence to a combination of the OECD Recommendation and either the European Data Privacy Directive or APEC Privacy Framework as appropriate.

SGSN has engaged SC6, SC25, SC27, SC29, SC31, SC32, SC36 and SC37 in JTC1 to identify opportunities for joint work in respect to data privacy aspects and associated legislative requirements.

The requirement for this report is originated from contributions concerning the use of personal data in listed applications in Sensor Networks. The pressures for business case justification initially sustains such developments without a clear legal position, and it is necessary not only to consider the technical and engineering possibilities, but to ensure that they evolve within a framework of generally (internationally) accepted data protection principles, supporting National data protection legislation.

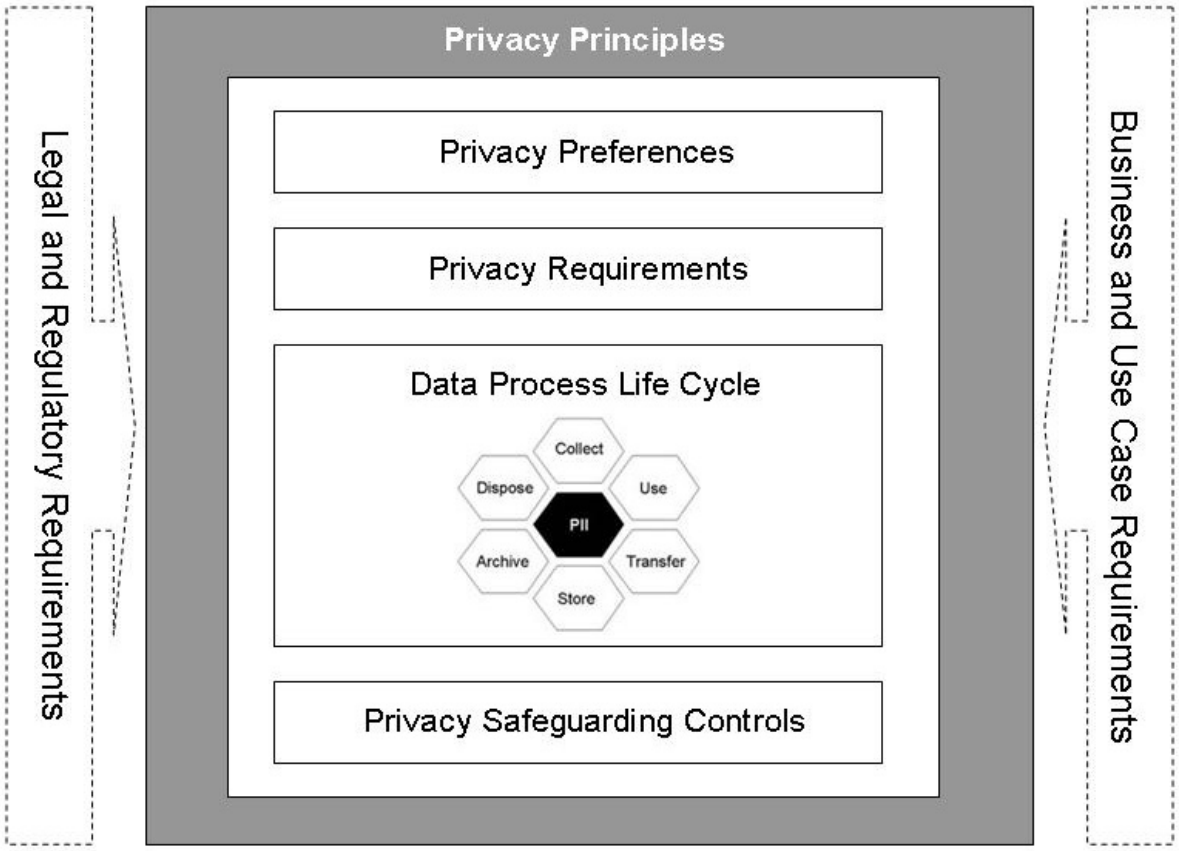
The following referenced documents are indispensable for the application of this document on Privacy:

European Data Privacy Directive Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995
European Privacy and electronic communications Directive Directive 2002/58/EC Of The European Parliament And Of The Council Of 12 July 2002
APEC Privacy Framework APEC#205-SO-01.2 wwww.apec.org
Recommendation Concerning And Guidelines Governing The Protection Of Privacy And Transborder Flows Of Personal Data O.E.C.D. Document C(80)58(Final), October 1, 1980

The Privacy Framework adopted by the Asia-Pacific Economic Cooperation (APEC),
The Privacy Framework developed by the International Security, Trust & Privacy Alliance (ISTPA), and
The `Montreux Declaration´ agreed by the International Conference of Data Protection and Privacy Commissioners.

Privacy in Ubiquitous Services with Sensor Networks (USN) has to be achieved, which requires attention on recognised and secure operations. Such means are not specified in this document but the following aspects will also need to be considered and some references are provided below where assistance can be found. Special concern needs to be given to the processing, transmission and storage of information, with authorized access for allowed users and potential information flows with external entities that may get involved. Moreover, in the overall context, it is often expected cooperation of different organizations that acquire the information in order to promote the exchange of data with the aim of improving functionalities regarding several USSN domains. In this case, the comprehension of other particular requirements and interfaces that are often under undefined responsibilities also need to be assessed in terms of security risks and possible attempts to privacy.

A basic framework representation has been contributed from SC27 resulting in ISO/IEC 29100 Privacy framework. This International Standard and its main elements relating to privacy and the processing of Personal Identifyable Information (PII) and communication technology is graphically shown in Figure 1 and described in the following text. For the development of this privacy framework, concepts, definitions and recommendations from other official sources have been taken into consideration. Those are namely the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, The Council of Europe Convention 108 for the Protection of Individuals with regard to Automatic Processing of Personal Data, The Privacy Framework adopted by the Asia-Pacific Economic Cooperation (APEC), the Privacy Framework developed by the International Security, Trust & Privacy Alliance (ISTPA), and the `Montreux Declaration´ agreed by the International Conference of Data Protection and Privacy Commissioners.



Initially, the data being processed is categorized as either PII or Non-PII. If the data is categorized as PII, the privacy framework shows the basic elements involved when personally identifiable information is exchanged between entities, depicted by the data processing life cycle, and the PII recipient as well as any potential third party need to ensure that required controls are in place for each of the data processes in order to protect PII and the PII principal's privacy.

Privacy preferences are always directly and subjectively linked to the PII principal. Privacy preferences depend on a number of factors that create certain levels of concern for the individual providing his/her PII in a specified context. The personal disposition of an individual towards privacy and what an individual considers sensitive personally identifiable information can depend on the person's understanding of the technology used, their social background, the sensitivity of the data provided, the person's past experience as well as socio-psychological factors.

Privacy requirements are defined by three main factors:
(1) legal and regulatory requirements for the safeguarding of the individual's privacy and the protection of his/her PII,
(2) the particular business and use case requirements, and
(3) individual privacy preferences of the PII principal as discussed in the preceding sub-clause.

A set of Privacy principles will be worked out in adherence to the general principles for data protection and data privacy of data relating to personal information concerning individuals.