Telecommunications and Information Exchange Between Systems

ISO/IEC JTC 1/SC 6

Document Number:	N13860
Date:	2009-02-10
Replaces:	
Document Type:	Liaison Organization Contribution
Document Title:	Liaison statement from JTC 1 SGSN to JTC 1/SC 6 on Sensor Networks issues explored on privacy replying to JTC 1 Nara Resolution 31
Document Source:	JTC 1 SGSN Sydney meeting
Project Number:	
Document Status:	Any comments on this document from SC 6 members should be submitted to SC 6 Secretariat by 24 April 2009.
Action ID:	COM
Due Date:	2009-04-24
No. of Pages:	7

ISO/IEC JTC1/SC6 Secretariat Ms. Jooran Lee, KSA (on behalf of KATS)

Korea Technology Center #701-7 Yeoksam-dong, Gangnam-gu, Seoul, 135-513, Republic of Korea ;

Telephone: +82 2 6009 4808 ; Facsimile: +82 2 6009 4819 ; Email : jooran@kisi.or.kr

ISO/IEC JTC 1
Study Group on Sensor Networks

Document Number:	SGSN N067
Date:	2009-02-04
Replace:	
Document Type:	Outgoing Liaison Statement
Document Title:	Sensor Networks issues explored on privacy replying to JTC 1 Nara Resolution 31
Document Source:	JTC 1 SGSN Sydney meeting
Document Status:	As per the JTC 1 SGSN Sydney Resolution 2, this Liaison Statement is submitted to SC6, SC17, SC24, SC27, SC29, SC36 and SC37 for comments by 29 April 2009.
Action ID:	ACT
Due Date;	
No. of Pages:	6

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)

Sensor Networks issues explored on privacy replying to JTC 1 Nara Resolution 31

“Based on the results of the Technology Watch session at the 23rd Plenary, JTC 1 instructs its Secretariat to distribute the presentation on “Creating Ubiquitous Services with Sensor networks” to the JTC 1 Study Group on Sensor Networks (SGSN), to give the SGSN the mandate to explore issues related to middleware and privacy in this context and to engage the appropriate SCs in JTC 1, e.g. SC 6 and SC 27, if concrete opportunities for work are identified.”

SGSN provided a first 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.
Those requiring guidance in respect of specific data protection and data privacy requirements in respect of ITS 'Probe' Data are referred to ISO 24100,"Basic principles for personal data protection in probe vehicle information services ".

SGSN would like to engage SC6, SC17, SC24, SC27, SC29, SC36 and SC37 in JTC1 to identify opportunities for joint work in respect to data privacy aspects and associated legislative requirements.

1. References

The following referenced documents are indispensable for the application of this document.
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
ISO 24100 Intelligent transport systems, Wide area communications, Basic principles for personal data protection in probe vehicle information services ".
ISO/IEC 17799 Information technology -- Security techniques -- Code of practice for information security management
ISO/IEC 18028 (series), Information technology -- Security techniques -- IT network security
ISO/IEC 18028-1, Information technology -- Security techniques -- IT network security -- Part 1: Network security management
ISO/IEC 18028-5, Information technology -- Security techniques -- IT network security -- Part 5: Securing communications across networks using virtual private networks, provides
ISO/IEC 27001, Information technology -- Security techniques -- Information security management systems --
Requirements
ISO/IEC 27002, Information technology -- Security techniques -- Code of practice for information security management
ISO/IEC 27005, Information technology -- Security techniques -- Information security risk management,
ISO/IEC 27006, Information technology -- Security techniques -- Requirements for bodies providing audit and certification of information security management systems,

2. Background

The requirement for this report is originated from discussions with ISO TC204 concerning the use of personal data in Intelligent Transport Systems. 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, and of course within National data protection legislation.
The subclauses of Recommendations are intended to provide a checklist of features to be consulted when developing a Standard or an implementation. The explanatory texts in the subclauses are directly extracted from the reference document, and this report does not attempt to make interpretation.
Where further information is required each subclause provides a direct reference to the original source.
In order to reach its recommendations, the developers of this report rely on three principal instruments which cover most of the world in their embrace.
These instruments are:
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
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
NOTE While the OECD guidelines and APEC Privacy Framework are policy instruments that are advisory in nature, the European Data Privacy Directive is mandatory in respect of EU countries.
Between them these instruments cover most countries of the world, who with the additional of further specific National Legislation, have signed to implement these basic principles of data privacy and protection of data held about individual persons. Although they vary in detail, the general principles are common, and originate from the OECD document c(80). The European deliverable has further specificity and protection requirements and is mandatory for EU member states.

3. Privacy requires security

Privacy in Ubiquitous Services with Sensor Networks (USN) has to be achieved, and this requires following 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 ITS 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.
Whenever appropriate, it is recommended to follow the guidelines defined for the Management of Information Security in accordance with the ISO 2700x family of Standards, with special reference to ISO 27002:2005. It is worth mentioning recommendations regarding the management of communications and operations or the measures taken in relation with the access control and privileges for authorized users.
There are a number of security related ISO Standards (including the ISO 2700x series) which may assist in the achievement of privacy, and guidance is needed here..

3.1 The investigative process

Some examples are provided in this clause, but examples are simply examples, they are used to highlight data protection and data privacy aspects where *existing law* must be taken in consideration in the design of systems and Standards. It is the intention of this report to encourage/inculcate an attitude of thinking as much as the specific recommendations implied by the EU, OECD and APEC deliverables.
Firstly, some significant example technical scenarios were studied in order to get an overview of the existing developmental situation. These are examples and do not purport to cover all USN scenarios. Parallel to this, legal areas within public law, civil law and data privacy law are considered.
The results are quite interesting and important in terms of legal implications, therefore the most important results are briefly summarised here for each scenario investigated:
For example, problems with data privacy laws may exist in many countries regarding the installation of traffic monitoring cameras which can identify individual vehicle characteristics. In terms of civil law, it is advisable to clearly stipulate responsibilities concerning liability issues in regard to control units.
The issue of floating car systems is also relevant to basic fundamentals, concerning the rights of the common person. It is the duty of the federal state to make sure that the rights of its citizens are not limited disproportionately. This problem, in regards to civil law, is again also reflected in labour laws. The employer must take the interests of his employees' protection into consideration. In some cases, the agreement of the workers' council is necessary.
Some parking schemes also raise concern because they save information related to mobile telephone numbers, license and registration numbers, bank accounts and names during the payment mode. It appears the present payment methods may not be in compliance with legal requirements for constitutional equality.
Regarding the area of traffic monitoring in public areas, it must be made certain that no unequal treatment is carried out. For example, cars that are equipped with monitoring chips should not be monitored more than cars without chips.
Constitutional rights of freedom of movement, is the most difficult in terms of legal data privacy considerations.
Another example may be with a temporary opening of a motorway emergency lane and entrance controls on motorway ramps. When monitoring the emergency lane in all areas, issues about the data security of video cameras are important.

Systems to reduce accident risks (intelligent speed adaptation, ISA; dynamic warnings, adaptive speed control, ACC, systems to avoid collisions) the level of accepted prudence is, in particular, in the opinion of the Austrian investigation, potentially problematic in terms of civil law.
On one hand, this report demonstrates the "need to catch up" in the sense of legal aspects, but on the other hand also highlights the legal inadmissibility of certain systems (at least within a European Member State). Nevertheless, this report is designed to make possible, as much as possible, the implementation of such systems and to help create legal clarity in the economic area in order to achieve the necessary and important developments towards intelligent infrastructure.
The recommendations in this report are based on identified existing legal positions for each case in order to ponder existing problems and to state needs for adaptation (*de lege lata*). A set of solutions (*de lege ferenda*) is discussed that aim to reduce or eliminate these problems. In doing so, the goal is always to enable the implementation of these systems to the greatest extent possible; nevertheless the limits of these technical developments should and will be shown (constitutional and/or international law). Furthermore, this report attempts to formulate basic principles from each aspect by establishing a - primarily legally motivated

– understanding of terms for intelligent infrastructure. Finally, based on these terms, the subjects are arranged based on their probable significance in legal order.

4 Recommendations

4.1 Basis of recommendations

This report proposes adherence to the following general principles for data protection and data privacy of data relating to personal information concerning individuals.
It is recommended that the conditions under which data shall be collected and held in support or provision of USN shall uphold all of the following principles :

4.2 Avoidance of harm

Shall recognize the interests of the individual to legitimate expectations of privacy, personal information protection and should be designed to prevent the misuse of such information. Further, acknowledging the risk that harm may result from such misuse of personal information, specific obligations shall take account of such risk, and remedial measures should be proportionate to the likelihood and severity of the harm threatened by the collection, use and transfer of personal information.
(APEC Privacy Framework Part iii)

4.3 Fairly and lawfully

All personal data shall be obtained and processed fairly and lawfully;
(APEC Privacy Framework Part iii, I,; EU Privacy Directive C3 Article 5; OECD Part 2, 7)

4.4 Specified, explicit and legitimate purposes

All personal data shall be collected for specified, explicit and legitimate purposes
(APEC Privacy Framework Part ii (Cl.13); Part iii (Cl. 1)

4.5 Explicit and legitimate and must be determined at the time of collection of the data

The purposes for which personal data are collected shall be determined at the time of the collection of the data and shall be explicit and legitimate at the time of collection of the data and use of the data limited to the fulfilment of those purposes (or such others as are not incompatible with those purposes specified); and the subsequent use shall be limited to the fulfilment of those purposes (or such others as are not incompatible with those purposes). All personal data collected shall be adequate, relevant and not excessive in relation to the purposes for which they are processed;
(EU Privacy Framework. 7.14.11 Cl 28, 56, 57; 7.19.5 (c) ; OECD Part 2. Cl.9)

4.6 Not further processed in a way incompatible with the purposes for which it was originally collected

All personal data shall not be further processed or used in a way incompatible with the purposes for which it was originally collected.
(EU Privacy Directive 7.14.1.1 Cl. 28,29; 7.19.5 (b); 7.40.1 (2); OECD Part 1 Cl 9, 24)

4.7 Not be disclosed without the consent of the data subject

Personal data shall not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Clause 4.4 except: (a); or (b).
a) **where the data subject has freely and unambiguously given his/her consent**
b) **by the authority of law of the Country**
c) processing is necessary for the performance of a contract to which the data subject is party or in order to take *steps at the request of the data subject* prior to entering into a contract; or
d) processing is necessary for compliance with a legal obligation to which the controller is subject; or
e) processing is necessary in order to protect the vital interests of the data subject; or
f) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in a third party to whom the data are disclosed; or
g) processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, *except where such interests are overridden* by the interests for fundamental rights and freedoms of the data subject defined above.
(EU Privacy Framework. Cl 28, Cl 30 & Section D11, Cl7.19.13 2(d); OECD Part 1. Cl.10; OECD Part 2. Cl.9; APEC Privacy Framework, Part iv Cl.29)

4.8 Adequate, relevant and not excessive in relation to the purposes for which they are collected

All personal data shall be adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed.
(EU Privacy Framework. Cl 28, Cl 30 & Section D11, Cl7.19.13 2(d); OECD Part 1. Cl.10; OECD Part 2. Cl.9; APEC Privacy Framework, Part iv Cl.29)

4.9 Accurate and, where necessary, kept up to date

All personal data shall be accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified.
(APEC Privacy Framework v1 Cl.21; EU Privacy Directive, Section 1. 7.19.5; OECD Part 1, Cl 8)

4.10 Identification of data subjects for no longer than is necessary for the purposes for which the data were collected

All personal data shall be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.
(APEC Privacy Framework ; EU Privacy Directive; OECD)

4.11 Restricted to those who have a demonstrable 'need to know'

Access to personal data shall be restricted to the minimum number of persons who have a demonstrable 'need to know'.
EXAMPLE in a situation where a law of the land has been allegedly infringed, an enforcement officer should have access only to information necessary to enforce, and not all information pertaining to the subject individual, his ownership of vehicles or other personal data. That information may for example only identify a vehicle and this data may be passed to a prosecution system. A national prosecution service, shall of course have need of access to much information concerning the accused person in order to effect a prosecution, but all of this information should not be available to all enforcement officers, and should not be made available without a justifiable need to know.
(OECD Para 1, 59)
The structure of systems and standards architecture for USSN shall be constructed to enable the use of data to be restricted to those who have a genuine need to know.

4.12 Clear and accessible

Personal information controllers shall provide clear and easily accessible statements about their practices and policies with respect to personal information that should include:
a) the fact that personal information is being collected;
b) the purposes for which personal information is being collected
c) the types of persons or organizations to whom personal information might be disclosed
d) the identity and location of the personal information controller, including information on how to contact them about their practices and handling of personal information.
(APEC Privacy Framework Part iii, Cl.15,20 ; EU Privacy Directive 7.9.1.2;)

4.13 Security safeguards

Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorised access, destruction, use, modification or disclosure of data.
(APEC Privacy Framework Part iii, Vii Cl.22 ; OECD Part 2. Cl.11)

4.14 Cumulative interpretation of multiple recommendations

In the development of USSN systems and standards, we are advised by legislators and lawyers that the recommendations cannot just be taken individually in isolation, but the combination of the recommendations may infer interpretations, this has significant implications. Lawyers often refer to this as 'cumulative interpretation'.